International Centre for Chemical Safety and Security

National Aerospace University “Kharkiv Aviation Institute”

MANUAL
ON CYBERSECURITY, RELIABILITY AND RESILIENCE ASSURANCE
IN THE CRITICAL INDUSTRIES

Edited by

Vyacheslav Kharchenko, Adam Paturej, Oleksandr Potii

Warsaw-Kharkiv-2024

E. Babeshko, O. Illiashenko, V.Kharchenko, O.Morozova, A. Paturej, K. Paturej, E. Peña, O. Potii, Z. Rapacki. Manual on Cybersecurity, Reliability and Resilience Assurance in the Critical Industries / V. Kharchenko, A. Paturej, O. Potii (Editors). International Centre for Chemical Safety and Security, Warsaw, 2024. – 228 p.

This book is a unique and comprehensive guide to cybersecurity, reliability, and resilience in the critical industries. Developed by an international team of experts, it offers practical solutions grounded in real-world issues and threats faced by modern industrial environments. It emphasizes an innovative approach, reframing cybersecurity as an investment that drives operational excellence rather than a mere cost. With a focus on the convergence of information and operation technologies (IT and OT), physical and cyber environments, the book provides actionable strategies that align safety, security, and reliability. It combines scientific knowledge with industrial practices, integrating global standards, risk management, and advanced technologies like AI and IoT. The book presents an educational framework to develop key qualifications and training programs, preparing professionals for the evolving landscape of Industry 4.0. Through its multidisciplinary and practical approach, this publication serves as an essential roadmap for building a secure, resilient, and future-ready industrial infrastructure. This book is intended for engineers, managers and researchers in the area of critical industrial systems and infractructures, information and operation technologies, safety and reliability engineering. It can be usefull for MSc- and PhD-students on corresponding specialties, university lecturers and researchers.

Ref. – 89 items, figures – 47, tables – 14.

Reviewers:

Professor Nikolaos Bardis, Helenic Army Academy, Greece
Professor Andrzej Rucinski, New Hampshire University, USA
Professor Oleg Odarushchenko, Research and Production Company Radics, Ukraine

ISBN 978-83-973477-1-7

Contents

Figures

Tables

Introductory words

Robert Kosla, LT.COL. (R) - EMEA Chief Architect CYBER, Microsoft Security Enterprise Services (former Director Department of Cybersecurity, Ministry of Digital Affairs - Poland)

I would like to emphasize that the development of the "Manual on Cybersecurity, Reliability and Resilience Assurance in the Critical Industries" was one of the key priorities supported by the Industry 4.0 Cyber Security Team established by the Ministry of Digital Affairs, working within the Cyber Security Group. The team, working in parallel with the Cyber Security Certification and Supply Chain Security team, contributed to the document necessary to carry out effective activities in particular in ensuring the cyber security of Operational Technology, an area that has not been in the mainstream of European regulations such as the NIS Directive, but which is crucial to maintaining essential services by operators operating in particular in the sectors originally singled out in European and national regulations: energy, transportation, drinking water supply and distribution, and health care.

In parallel with the work on the Manual, work was carried out, supported by the Cyber Security Department of the Ministry of Digitization, on the formal approval of new professional qualifications covering Operational Technology, as well as work on the preparation of assumptions for cyber security certification criteria and programs dedicated to OT solutions.

Very important from a practical point of view was the reference in the Manual to ISO international standards and US NIST normative documents developed in cooperation with industry. This makes it possible to fully address the regulatory requirements for the maintenance of critical services and to propose scalable and standardized practical activities that must be performed by personnel managing and maintaining elements of critical industrial infrastructure. In addition, it was very important for the process of designing and maintaining critical services to refer to a security architecture tailored to the analysis of threats that may adversely affect industrial systems.

In addition, I would like to emphasize that the Handbook should serve as a basis for planning activities to increase the cyber resilience of critical industrial infrastructure against failures and targeted hybrid cyberattacks - conducted from outside and inside using multiple attack vectors and tools. Only such a comprehensive and holistic approach will make it possible to maintain the core functions of critical industrial systems necessary for a modern economy.

I express the hope that the Manual will be used as a de facto standard in the interaction between countries in the framework of transatlantic and European security and will be the basis for subsequent joint projects of a standardization-regulatory, operational-functional, as well as technological-scientific nature.

Brigadier general Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection of Ukraine

In today's increasingly interconnected world, the critical importance of robust cybersecurity and resilience cannot be overstated. This is particularly true in light of the intensified cyber threats targeting critical industries, exacerbated by the ongoing russian aggression against Ukraine. These attacks underscore the urgent need for coordinated efforts to safeguard vital infrastructure, ensuring the continuity of operations and the safety of our societies.

This Manual on Cybersecurity, Reliability, and Resilience Assurance in the Critical Industries represents a groundbreaking collaboration between Ukrainian and Polish cybersecurity professionals. United by shared values and a common purpose, these experts have crafted a resource that is both innovative and practical, addressing the specific challenges faced by chemical and energy carriers industries. The book offers actionable tools and insights designed to bolster information security, integrate operational technologies, and navigate the evolving risks of the so-called Industry 4.0.

Beyond providing technical guidance, this publication reframes cybersecurity as a strategic investment, one that enhances operational excellence while aligning with global standards and cutting-edge technologies like artificial intelligence and the Internet of Things. By bridging the gap between scientific knowledge and industrial practice, it empowers professionals to build secure, resilient infrastructures for the future.

The creation of this manual would not have been possible without the dedication of its co-authors, editors, and the publisher. Special recognition is owed to Mr. Krzysztof Paturej, President of the Board at the International Centre for Chemical Safety and Security (ICCSS). His visionary leadership and strong commitment were instrumental in bringing this publication into life.

With gratitude and admiration for all contributors, this book is offered as a testament to international cooperation and a vital resource for strengthening cybersecurity in critical industries. Together, we stand resilient.

Scientific editors

	Prof. Vyacheslav Kharchenko Prof. Vyacheslav Kharchenko is a Doctor of Technical Sciences and a Head of the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine. He leads the Centre for Safety Infrastructure-Oriented Research and Analysis at RPC Radiy. Prof. Vyacheslav Kharchenko is a member of ICCSS Global Team. As an Honor Inventor of Ukraine, Prof. Kharchenko has been instrumental in advancing the fields of industrial cybersecurity, safety, and reliability. He has supervised the development of 12 national and branch standards focusing on Nuclear Power Plant (NPP) Instrumentation and Control (I&C) systems and aerospace system reliability and safety. Additionally, he has led 14 national projects and coordinated 11 EU-funded projects under TEMPUS, Erasmus+, FP-7, H2020 and other programs, addressing dependable computing, infrastructure safety and security, green and sustainable IT-engineering, the Internet of Things (IoT) and intelligent autonomous systems. Prof. Kharchenko's pioneering work has significantly shaped the integration of cybersecurity and reliability in industrial settings, emphasizing resilience and the importance of a secure-by-design approach to ensure operational continuity in critical infrastructures.
	Mr. Adam Paturej Mr. Adam Paturej is the Business Director of the International Centre for Chemical Safety and Security (ICCSS) and the Director for the ICCSS Cybersecurity Program. A leader in developing key qualifications and competencies for industrial cybersecurity, he played a crucial role in establishing the three leading qualifications that laid the groundwork for the ICCSS's approach to cybersecurity and reliability. As an inventor of unique training programs, Mr. Adam Paturej has contributed to promoting the concept that cybersecurity is an investment in safety and efficiency. His experience in financial management, project coordination, and development of international safety programs underscores his dedication to fostering a secure and reliable industrial environment. His strategic vision has been instrumental in creating education and training pathways that prepare industry professionals to meet the evolving demands of cybersecurity in the industrial sector.

Prof. Oleksandr Potii

Prof. Oleksandr Potii is Brigadier General, Doctor of Technical Sciences. He is Chairman of the State Service of Special Communication and Information Protection of Ukraine. At his previous position, as a Deputy Head of the State Servicee was responsible for a range of important areas, including critical infrastructure protection, IT standardisation and certification, cyber defence, and cyber workforce development. His work emphasized the importance of integrating cybersecurity and reliability across various industrial sectors, advocating for a comprehensive approach to secure digital transformation. Oleksandr Potii has more than 25 years of experience in military service, and 20 years of academic experience. Before joining the State Service, he has hold different technical and administrative positions at important educational institutions, such as Kharkiv National University of Radio Electronics and National Aerospace University "KhAI" Prof. Potii is an expert on information protection standards, on the development of personnel potential in the field of cyberdefense, and on the protection of critical information infrastructure, information security and cryptography.

Author's list

Dr. Eugene Babeshko

Dr. Eugene Babeshko, PhD, is an Associate Professor at the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine. He is recognized as one of the leading scientists in the functional safety assessment and assurance of industrial control systems. He is a safety expert at the Kharkiv Regional Centre for Industry 4.0 and a senior researcher at the Centre for Safety Infrastructure-Oriented Research and Analysis. His primary activities include supporting the verification, licensing, and certification of control systems for nuclear engineering and other critical industries. Dr. Babeshko's work contributes significantly to the advancement of industrial cybersecurity and the development of resilient safety mechanisms that align with international standards and regulations.

	Dr. Oleg Illiashenko Dr Oleg Illiashenko, PhD, is an Associate Professor at the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine, a Researcher at the Institute of Informatics and Telematics of the National Research Council (IIT-CNR), Pisa, Italy. As one of the leading scientists in the cybersecurity assurance of cyber-physical systems, he specializes in formal methods for embedded systems. Dr. Illiashenko is an industrial cybersecurity expert at the Kharkiv Regional Centre Industry 4.0. He heads the cybersecurity division of TC185 "Industrial Automation" and contributes through TC 185's collaboration with the Ukrainian RTC for Standardization, Certification, and Quality. His research focuses on developing robust cybersecurity measures for industrial settings, ensuring resilience, implementing secure-by-design principles, safety and security co-engineering and advancing cybersecurity education.
	Prof. Olga Morozova Prof. Olga Morozova is a Doctor of Technical Sciences and a Full Professor at the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "KhAI", Kharkiv, Ukraine. She is recognized as one of the leading scientists in the AI systems, safety of IoT systems. Prof. Morozova is a developer and responsible executor of the projects dedicated to dependable mobile systems for monitoring of critical objects. Her R&D interests are related to industrial IoT-based logistic, transport and monitoring systems, application of AI and Digital Twins to insure safety and resilience, information platforms for cooperation of university and IT-business in education and innovation.
	Mr. Krzysztof Paturej Ambassador Krzysztof Paturej is the President of the International Centre for Chemical Safety and Security (ICCSS) in Warsaw, Poland. As a former diplomat and senior official at the Organisation for the Prohibition of Chemical Weapons (OPCW), he has been at the forefront of developing integrated solutions for chemical safety, environmental and cybersecurity. He is a visionary who was among the first experts to highlight the risks of cyber-attacks on chemical plants. His initiatives led to the establishment of the ICCSS, which offers innovative strategies for enhancing the security and resilience of the industry. Ambassador Paturej's holistic approach to cybersecurity encompasses societal resilience, emphasizing the need to protect the chemical supply chain from cyber threats. He is actively involved in international collaborations with the UN, EU, NATO, and other global organizations, promoting a comprehensive framework for industrial cybersecurity, reliability, and safety.

	Mr. Emil Peña Mr. Emil Peña serves as the Executive Director of the Global Energy Safety Institute. He is dedicated to transitioning NASA's space program knowledge and technologies into the energy sector, encompassing oil, gas, utilities, and renewables. With a rich history of leadership, Mr. Peña has held executive roles at the National Corrosion Center at Rice University and the U.S. Department of Energy, where he oversaw oil and gas programs. Dr. Emil Peña is a member of ICCSS Global Team. He advocates for an innovative approach to cybersecurity as an investment rather than a cost, highlighting the financial advantages of integrating cybersecurity and reliability into risk management practices. His experience spans research in material science, environmental systems, and infrastructure protection, making him a key voice in developing industry-wide cybersecurity strategies that offer tangible benefits, such as reduced insurance premiums and enhanced operational efficiency.
	Dr. Zdzisław Rapacki Dr. Zdzisław Rapacki is an expert in cybersecurity education, serving as ICCSS international director and Trainer in Chemical Safety and Security. A former ambassador of Poland to the United Nations Office in Geneva, Dr. Rapacki has a wealth of experience in diplomacy, disarmament, and economic and social transitions. Currently, he lectures at the Academy of Finance and Business Vistula and at Collegium Civitas. His input in cybersecurity education is profound, advocating for inclusive, practitioner-focused training programs that blend practical experience with theoretical knowledge. Dr. Rapacki's approach emphasizes the development of core competencies needed to address contemporary cybersecurity challenges, aligning with the need for structured training programs discussed in the manual.

Acknowledgments

This Manual on Cybersecurity, Reliability and Resilience Assurance in the Critical Industries represents a significant advancement in the field of industrial security. Through collaborative efforts spanning Poland, Ukraine, and the United States, along with contributions from numerous international partners, it establishes an innovative framework for industrial security and safety management.

The development of this manual has been made through the visionary leadership and support of the International Centre for Chemical Safety and Security (ICCSS) and the National Aerospace University "Kharkiv Aviation Institute" (KhAI). Their partnership has been instrumental in bringing together diverse expertise and perspectives to create this comprehensive resource.

We extend our profound gratitude to Prof. Oleksandr Potii for his invaluable contributions made during the ongoing Russian military aggression against Ukraine. His insights, drawn from Ukraine's experience in defending against sustained cyber warfare and attacks, have provided crucial practical lessons that significantly enhance this manual's relevance for cybersecurity governance and critical infrastructure protection.

Special appreciation is extended to Mr. Robert Kosla, former Director of Cybersecurity Department at the Ministry of Digital Affairs of the Republic of Poland, for his inspirational role in establishing the international collaboration and providing valuable insights on national and European regulatory frameworks.

This manual has particularly benefited from real-world experiences in cybersecurity defense, notably during the ongoing Russian military aggression against Ukraine. The practical insights gained from defending against sustained cyber warfare have significantly enhanced the manual's relevance and applicability. The contributions of numerous practitioners who continue to defend against cyber attacks have proven invaluable in developing robust cybersecurity strategies.

The technical reviewers from Poland, Ukraine, the United States, and other European countries deserve special recognition. Their diverse perspectives and rigorous analysis have enhanced the manual's technical accuracy and global applicability. Their expertise across various aspects of industrial cybersecurity, from operational technology to risk management, has ensured comprehensive coverage and practical value.

Sincere appreciation goes to the editorial and production team for their dedication in transforming complex technical content into an accessible and practical resource. Their attention to detail and commitment to clarity have significantly enhanced the manual's utility.

The development of this manual would not have been possible without the input of numerous professionals in the critical industry sectors who shared their experiences and challenges. Their practical insights have been crucial in ensuring that the manual effectively addresses real-world needs while advancing the understanding of cybersecurity as a strategic investment rather than merely a cost.

This manual demonstrates how embedding cybersecurity, reliability, and resilience assurance into core operational practices yields substantial returns through prevented downtime, reduced catastrophic failure risks, and enhanced operational efficiency. The approach outlined herein, including its potential impact on insurance premiums, creates compelling financial incentives for implementing comprehensive security strategies.

In the increasingly complex digital landscape facing critical industries, this manual stands as a testament to the power of international collaboration in advancing industrial security practices. It is hoped that it will serve as a valuable resource for all professionals working to secure and strengthen critical infrastructure through strategic investment in cybersecurity measures.

Preface

In an era where the digital transformation of industrial processes has become the norm, the convergence of Information Technology (IT), Operational Technology (OT), and Environmental Technology (ET) presents both remarkable opportunities and unprecedented challenges. As industries, particularly in the chemical and energy sectors, embrace these technological advances, the risk landscape has expanded in complexity. Cybersecurity and reliability are no longer mere operational concerns; they have become essential pillars for ensuring safety, regulatory compliance, and business continuity. This publication, *"Manual on Cybersecurity, Reliability, and Resilience Assurance in the Critical Industries,"* addresses this multifaceted reality head-on, offering a unique, integrated framework for building a secure, reliable, and resilient industrial future.

This Manual results from an exceptional collaboration between the International Centre for Chemical Safety and Security (ICCSS) and the National Aerospace University "Kharkiv Aviation Institute" (KhAI). Both organizations are global leaders in the fields of cybersecurity, safety, and infrastructure resilience. The ICCSS, the initiator and coordinator of this project, led the efforts to integrate crucial aspects of digitalization, risk measurement, and the development of competencies and training programs for reliability and cybersecurity management. National Aerospace University "KhAI" spearheaded the scientific and academic aspects, providing critical methodologies and practical solutions essential to this publication. KhAI's extensive experience in infrastructure safety, advanced computing, and formal methods for embedded system assurance has been invaluable in crafting the comprehensive approach detailed in this Manual. Together, ICCSS and KhAI present a well-rounded perspective that bridges policy, industry practices, and education.

The creation of this Manual represents a truly unique collaborative effort, bringing together authors from Poland, Ukraine, and the United States. This diverse team combines expertise from academia, industry, civil society, and independent experts, enriching the publication with a holistic blend of knowledge. Their collective insights provide a practical roadmap grounded in real-world challenges, ensuring that this Manual not only mitigates risks but also transforms cybersecurity into a strategic investment for industrial operators.

This publication's core strength lies in its practical, real-world applicability. It is not simply a collection of theoretical ideas; it is a roadmap grounded in the actual challenges faced by industrial operators, insurers, policymakers, and educators. The authors—drawn from a diverse international team—bring together insights from multiple disciplines to address the rapidly evolving digital landscape. Their combined expertise ensures that this Manual is not just about mitigating risks but also about transforming cybersecurity into a strategic investment that drives operational excellence.

The Manual offers an innovative approach by treating cybersecurity not as a cost but as a vital investment that provides tangible financial and operational benefits. One of its unique features is the detailed roadmap for linking cybersecurity and reliability practices to reduced insurance premiums, encouraging a proactive mindset among industry stakeholders. In addition, the Manual emphasizes a comprehensive educational framework, laying out core competencies and qualifications necessary for building a skilled workforce capable of navigating the complexities of industrial cybersecurity in the age of Industry 4.0.

Through this publication, we seek to contribute to the development of an international protocol on industrial cybersecurity and reliability. This protocol aims to establish global standards, enhance confidence-building measures, and increase awareness of cyber threats in industrial environments. By fostering international cooperation, it will create a unified approach that aligns industry practices, regulatory frameworks, and educational programs, ensuring that cybersecurity becomes an integral part of global industrial operations.

The authors collectively affirm ICCSS's rights to this Manual, ensuring its continued evolution and relevance. This commitment protects the concepts of cybersecurity, reliability, and resilience outlined within, maintaining their integrity as global standards for industrial operations. The ideas presented here are not merely theoretical constructs; they are meant to shape policies, educational programs, and industry practices, laying the groundwork for a secure, resilient, and future-ready industrial landscape.

It’s important to note that the Manual has been prepared drawing upon the foundational principles and requirements outlined in earlier versions of normative regulatory documents, specifically the IEC 61508 and IEC 62443 families of standards. These standards provided a robust framework that has guided the development of this Manual. The subsequent updates to these standards, as referenced in the Manual’s bibliography, have not only retained the core concepts but also expanded upon them to address evolving industry needs. By integrating insights from both the original and updated versions, the Manual ensures alignment with the latest best practices and regulatory expectations.

Work on the manual lasted several years. These years were quite difficult. On the one hand, the pandemic, and especially Russia's large-scale war against Ukraine, has emphasized the importance of ensuring the security and resilience of industrial systems and critical infrastructures.

On the other hand, new technological challenges were formed. They are associated with the introduction of artificial intelligence of other modern technologies accompanied by the new security deficits. Some methods of their analysis and solutions for reducing the risks of danger in the monitoring systems of critical objects, the development of smart cities, and unmanned intelligent mobile systems are provided in the publications at the end of the book. They need additional discussion and further development.

In conclusion, this book offers more than just solutions—it presents a comprehensive, future-oriented framework that integrates safety, security, reliability, and resilience into one cohesive model. We invite you to delve into its pages, not just as a reader but as an active participant in advancing the global approach to cybersecurity and reliability in the chemical and energy industries. Together, we can turn challenges into opportunities and ensure a secure, prosperous future in an increasingly interconnected world.

Executive Summary

General

This Manual presents a comprehensive and integrated approach to cybersecurity, reliability, and resilience in the chemical and energy carriers industries. In an era defined by rapid digital transformation and the convergence of Information Technology (IT), Operational Technology (OT), and Environmental Technology (ET), these sectors face increasingly complex risks. The Manual envisions a future where cybersecurity is not merely an IT concern but a core component of operational reliability and safety. It provides a holistic methodology to embed cybersecurity into all levels of industrial operations, offering strategies, educational frameworks, and policy recommendations designed to build a resilient industrial infrastructure capable of withstanding modern threats.

The Manual outlines a unique, multi-disciplinary approach that integrates functional safety, risk management, advanced technologies like AI and IoT, and a well-rounded education model to develop the necessary competencies. It emphasizes the need for a proactive stance on cybersecurity, advocating for "big" safety and security models that address both digital and physical aspects of industrial environments. This vision calls for dynamic collaboration among industry professionals, regulators, and educators to create a workforce equipped to secure critical assets and systems. The subsequent chapters detail a comprehensive roadmap to achieve this vision.

Cybersecurity as an investment, not a cost

A key principle of this integrated approach is reframing cybersecurity from being a mere cost to a strategic investment. By embedding cybersecurity and reliability into core operational practices, organizations can prevent costly downtime, mitigate the risk of catastrophic failures, and enhance overall operational efficiency. This proactive approach leads to reduced incidents, minimizing financial losses related to cyber-attacks, compliance breaches, and equipment failures. Additionally, adopting robust cybersecurity measures can result in lower insurance premiums, as insurers increasingly favor assets with advanced cybersecurity and reliability postures. Therefore, investing in cybersecurity not only strengthens the resilience of industrial operations but also creates financial incentives that drive long-term value and operational sustainability. This mindset shift encourages organizations to view cybersecurity as a vital component of their overall business strategy, yielding significant returns in terms of risk reduction, improved market competitiveness, and operational excellence.

Structure

Chapter 1: Introduction

The Manual opens by exploring the convergence of IT, OT, and ET within industrial systems, emphasizing the need for a unified cybersecurity and reliability framework. It introduces the concept of "(Big) Safety and Security," a model that integrates safety, security, and environmental management into a single operational strategy. The chapter highlights the growing complexities of cybersecurity challenges in digitalized industrial environments and the imperative for a holistic approach that aligns safety protocols with digital security measures.

Chapter 2: Methodology for Integrated Cybersecurity and Safety Management

Chapter 2 introduces an integrated IT-OT-ET management system tailored for industrial environments. It provides a detailed methodology for implementing a comprehensive enterprise management system that covers physical, informational, and cybernetic components. This chapter stresses the importance of harmonizing cybersecurity and safety standards, such as IEC 61508 and IEC 62443, to reduce operational risks. It also addresses regulatory compliance, verification processes, and the need for continuous improvement in security practices to align with technological advancements.

Chapter 3: Security (Information, Cyber, Physical) for Resilience

Chapter 3 focuses on establishing a cybersecurity governance framework tailored to industrial operations. It details the elements required for a robust cybersecurity strategy, including risk assessments, threat intelligence, and security architecture design. The chapter provides an in-depth analysis of cybersecurity operations, including active defense, incident response, vulnerability management, and recovery procedures. It emphasizes the critical role of cybersecurity in ensuring resilience and the need for executive management involvement in overseeing cybersecurity policies.

Chapter 4: Functional Safety Regulation, Assessment and Insurance

The Manual delves into the functional safety lifecycle, outlining how to develop, implement, and manage safety-critical systems within industrial facilities. Chapter 3 discusses international standards like IEC 61508 and IEC 61511, providing guidance on functional safety audits, assessments, and best practices. The chapter highlights methodologies such as Failure Mode and Effects Analysis (FMEA) to ensure the reliability of safety systems and underscores the significance of integrating safety certification processes into the operational lifecycle.

Chapter 5: Risk Management and Security Audits for OT Systems and Processes

Risk management in OT systems is explored in Chapter 5, which outlines standards and best practices for conducting security audits in industrial environments. The chapter discusses how to adapt risk assessments to the unique challenges of OT systems, addressing aspects like infrastructure reliability and the transformation toward Industry 4.0. A case study on a cyber-attack in an industrial setting illustrates the importance of robust security measures, highlighting key considerations in safeguarding OT assets from potential threats.

Chapter 6: Digitalization of Energy Assets for Measuring Risk – Roadmap for Insurance

Chapter 6 discusses how the digitalization of energy assets has revolutionized risk measurement and insurance. It presents a comprehensive roadmap for integrating operational and physical asset data into risk assessment algorithms. Key topics include enhanced data collection using sensors, AI-driven predictive maintenance, anomaly detection, and data encryption to improve asset ratings. The chapter further explores how advanced analytics and real-time monitoring can lead to dynamic pricing models for insurance, offering incentives for assets that prioritize cybersecurity and reliability.

Chapter 7: Developing Competencies and Training in Industrial Cybersecurity and Reliability

A critical aspect of ensuring cybersecurity and reliability in industrial settings is developing professional competencies. Chapter 7 outlines the evolving landscape of industrial cybersecurity and the need for structured training programs. The chapter introduces three key qualifications developed by the International Centre for Chemical Safety and Security (ICCSS):

1. Shaping Reliability and Cybersecurity Policy in Industry
2. Management of Reliability and Cybersecurity in the Scope of Devices and Technology in Industry
3. Management of Reliability and Cybersecurity in Industry

Each qualification emphasizes the development of essential skills, including risk assessment, incident response planning, compliance management, and secure system design. The chapter stresses that a well-trained workforce is central to the successful implementation of cybersecurity strategies, aligning educational programs with regulatory requirements such as the NIS 2 Directive.

Chapter 8: Innovative Insurance Models Based on Cybersecurity and Reliability

The Manual concludes with an innovative approach to insurance models, emphasizing the financial benefits of incorporating cybersecurity and reliability into risk assessment. It discusses the transition to dynamic pricing models, such as usage-based and parametric insurance, which reward energy asset operators that adopt advanced cybersecurity practices. The chapter provides recommendations for insurers to develop risk-scoring models that incorporate cybersecurity metrics, offering premium discounts for compliance with cybersecurity standards. For energy asset operators, it advises investing in multi-layered defense strategies, predictive maintenance, and secure-by-design principles to enhance their insurability.

Chapter 9: Cyber and AI Risks for CBRN Related Facilities: Navigating Security in an Era of Democratized Knowledge

Chapter focuses on the specific cyber and AI risks facing Chemical, Biological, Radiological, and Nuclear (CBRN) facilities. It identifies potential threats, such as automated cyber-attacks, manipulation of safety systems, AI-driven disinformation, and synthetic biology misuse. The chapter proposes protection strategies, including real-time monitoring, defense-in-depth approaches, secure data management, and AI-enhanced threat detection. It also recommends policy development, international collaboration, and countering AI-driven disinformation to safeguard these critical facilities effectively.

Chapter 10: Industrial Reliability, Cybersecurity, and Resilience Education: Concept

Chapter proposes a comprehensive educational model for building expertise in industrial cybersecurity and reliability. It introduces the "(Big) Safety and Security Model" to teach students the interdependent nature of safety and security in industrial environments. The model includes elements like safety-cybersecurity interdependence, defense-in-depth strategies, risk management, and human-machine interaction security. The chapter further describes the concept of "safety and security spaces," highlighting the need for protecting physical, virtual, data processing, and human-machine interaction zones. The curriculum integrates multidisciplinary and practical skills development, focusing on secure-by-design principles, AI applications, and ethical considerations.

Final remarks

This Manual outlines a unique and comprehensive approach to cybersecurity and reliability in industrial settings. By integrating safety, security, and reliability into a cohesive framework, it offers a vision for building resilient and secure industrial systems. The Manual's multi-disciplinary strategy encompasses regulatory compliance, risk management, advanced technological solutions, and competency development. It promotes a proactive approach, advocating for education, collaboration, and the adoption of innovative insurance models to align financial incentives with best practices in cybersecurity and reliability.

This approach aims to equip the chemical and energy sectors with the tools and knowledge needed to navigate the complexities of the digital age, ensuring operational continuity, regulatory compliance, and a strong defense against evolving cyber threats. The Manual serves as a roadmap for building a future-proof industrial landscape where safety, security, and reliability form the cornerstone of risk management and operational excellence.

1 INTRODUCTION

1.1 Global Cyber Security, Reliability and Resilience Challenges

As of 2024, the landscape of cyber threats for industrial facilities continues to undergo a significant transformation. The proliferation of sophisticated hacking tools, once limited to state-level actors, has now become accessible at a broader public level. This democratization of advanced cyber capabilities has led to a drastic escalation in the risk and frequency of cyber incidents, with recent events demonstrating the tangible impact of what were once theoretical threats. Manufacturers and industrial operators have faced substantial financial losses, with damages running into billions of dollars, highlighting the criticality of robust cybersecurity measures.

The 2024 World Economic Forum's Global Risks Report highlights the escalating challenges in cybersecurity amidst rapid technological advances. It underscores a growing "cyber equity gap" where organizations that lack resources struggle to defend against increasingly sophisticated threats, including the misuse of generative AI and quantum computing. The report calls for global collaboration to strengthen cyber-resilience, emphasizing the need for equitable access to defensive technologies and skilled talent. Enhanced cooperation is critical as the interconnected nature of cybersecurity risks makes even robustly protected organizations vulnerable. The Report highlights energy as a critical area amidst growing challenges in sustainability and resource security. It underscores the importance of accelerating the transition to renewable energy carriers and technologies, as fossil fuel reliance increasingly conflicts with climate goals and geopolitical stability. The report points out risks associated with energy infrastructure vulnerabilities, such as cyber threats, supply chain disruptions, and the geopolitical competition over critical materials like rare earth elements essential for clean energy technologies. The report emphasizes the need for coordinated international efforts to secure energy systems while maintaining affordability and sustainability to mitigate these risks in the next decade. This involves fostering innovation, diversifying energy sources, and strengthening regulatory frameworks to ensure both economic stability and environmental responsibility.

The Microsoft Digital Defense Report 2024 addresses the cybersecurity of energy carriers and critical infrastructure with a focus on resilience against sophisticated cyber threats, particularly from nation-state actors and ransomware groups. It highlights the growing risk of ransomware attacks, often facilitated by phishing or exploiting unmanaged devices. These attacks can disrupt energy systems by targeting operational technology (OT) environments that control physical processes, such as electricity grids or oil pipelines. Microsoft emphasizes the importance of securing both IT and OT systems through Zero Trust frameworks, which assume breach scenarios and continuously verify all network access.The report also warns about the increasing sophistication of Distributed Denial-of-Service (DDoS) attacks, including those targeting the energy sector. Newer threats like application-layer DDoS attacks and loop attacks exploit vulnerabilities in core protocols, posing significant risks to energy carriers. To counter these, Microsoft recommends combining DDoS mitigation techniques, such as web application firewalls and periodic simulations, to enhance defenses. Additionally, Microsoft stresses the role of AI-powered tools for proactive defense, enabling quicker detection of anomalies and more robust responses. These tools are critical in preventing disruptions in energy supply chains by addressing vulnerabilities before attackers exploit them.

The industrial sector, in particular, has seen this evolving threat landscape coincide with the advent of the digital era. The integration of production processes with advanced data analytics, a key component of Industry 4.0 / 5.0, offers numerous benefits in terms of efficiency and innovation. However, it also introduces new vulnerabilities as interconnected systems provide more entry points for cyberattacks.

The integration of Operational Technology (OT) with Information Technology (IT) systems adds complexity to cybersecurity efforts in the industrial domain. This convergence necessitates a reevaluation of traditional cybersecurity approaches, emphasizing the need for more sophisticated and integrated strategies to safeguard critical infrastructure.

Investing in cybersecurity measures has become a strategic imperative for industrial operations. It is no longer seen as a mere cost but as an essential investment to safeguard operations, protect intellectual property, and maintain a competitive edge. This shift in perspective is driven by the understanding that the potential losses due to cyber incidents can far exceed the costs of implementing robust security measures.

Furthermore, cybersecurity and reliability are crucial for building trust and credibility with customers and stakeholders. In an era marked by frequent data breaches, investing in robust cybersecurity measures is also an investment in brand protection and customer trust.

The development of a skilled workforce capable of managing these emerging risks is paramount. Comprehensive training programs and the development of professional competencies in cybersecurity are vital for creating a resilient industrial sector. Initiatives like the Integrated Qualification System in Poland, which aims to standardize skills and knowledge in the cybersecurity field, are indicative of a global recognition of this need.

Qualifications such as "Shaping Reliability and Cybersecurity Policy in Industry," "Management of Reliability and Cybersecurity for Industrial Devices," and "Managing Reliability and Cybersecurity in the Industrial Sector," developed by the International Centre for Chemical Safety and Security (ICCSS), exemplify targeted efforts to enhance the cybersecurity posture of industrial operations. These qualifications provide a structured approach for building necessary capabilities within the workforce, ensuring professionals are equipped to handle the complex challenges presented by Industry 4.0.

The integration of these qualifications into professional training programs marks a significant shift in the industry's approach to cybersecurity. Moving from reactive measures to a more proactive and strategic stance, these programs integrate cybersecurity into the fabric of industrial operations, underscoring its importance in the overall business strategy.

In conclusion, the risk landscape for cyber incidents in industrial facilities, as of 2023, is characterized by rapidly evolving threats driven by the widespread availability of advanced hacking tools and the integration of digital technologies. Addressing these risks requires a multifaceted approach that includes investing in cybersecurity measures, developing professional competencies, and implementing effective management strategies. Embracing these strategies allows industries not only to protect themselves against current threats but also to build a foundation for resilience and adaptability in the face of future challenges. This proactive approach to cybersecurity is a strategic investment in the future of industrial operations, ensuring their sustainability, competitiveness, and growth in the digital age.

1.2 Two Sides of Information Technologies in Human and industry cyber security, reliability and resilience

The realm of industrial cybersecurity extends beyond the technical and into the human and procedural domains. There is a need to explore the integral role humans play in cybersecurity management, the necessary skills and knowledge they must possess, and the procedural frameworks that underpin effective cybersecurity practices in the industrial sector, drawing insights from the official announcement regarding human and procedural resources.

The Human Element in Cybersecurity

The human aspect of cybersecurity is often considered the most variable and challenging to manage. Employees can either be the strongest link in cybersecurity or its weakest point. The complexity and sophistication of cyber threats mean that every individual in the organization, from top management to operational staff, plays a crucial role in maintaining security.

1. Awareness and Training: Central to managing the human aspect of cybersecurity is creating a culture of awareness and continuous learning. Regular training sessions are essential to keep staff updated on the latest cyber threats and the best practices for preventing and responding to them. Training should be tailored to different roles within the organization, ensuring that everyone understands their responsibilities in maintaining cybersecurity.
2. Behavioral Aspects: Understanding the behavioral aspects of cybersecurity involves recognizing how human actions (or inactions) can impact security. This includes addressing common behaviors such as password management, response to phishing attacks, and adherence to security protocols.
3. Empowering Employees: Empowering employees to take an active role in cybersecurity involves encouraging them to report suspicious activities and providing them with the tools and knowledge to identify potential threats.

Skills and Knowledge for Cybersecurity Professionals

For those directly responsible for cybersecurity in the industrial sector, a more specialized set of skills and knowledge is required. The official announcement from the Polish Minister of Digital Affairs highlights several key competencies:

1. Technical Expertise: A deep understanding of both IT and OT systems, their vulnerabilities, and how they can be secured against cyber threats.
2. Risk Management: The ability to conduct comprehensive risk assessments and develop strategies to mitigate identified risks.
3. Legal and Regulatory Knowledge: Familiarity with relevant cybersecurity laws, standards, and regulations to ensure compliance and understand the legal implications of cyber incidents.
4. Incident Response and Recovery: Skills in developing and implementing incident response plans and recovery procedures after a cybersecurity breach.
5. Communication Skills: The ability to communicate complex cybersecurity concepts clearly and effectively to various stakeholders, including non-technical staff, management, and external parties.

Procedural Frameworks in Cybersecurity

Procedural frameworks provide the structured approach necessary for effective cybersecurity management. These frameworks encompass policies, procedures, and protocols that guide how cybersecurity is managed within the organization:

1. Cybersecurity Policies: Developing comprehensive cybersecurity policies is foundational. These policies should cover aspects such as access control, data protection, and incident response. They must be regularly reviewed and updated to reflect the evolving cybersecurity landscape.
2. Standard Operating Procedures (SOPs): SOPs provide detailed instructions on carrying out specific cybersecurity tasks. This can include procedures for installing updates, managing user access, and responding to security incidents.
3. Compliance and Auditing: Regular audits are crucial to ensure that cybersecurity practices comply with internal policies and external regulatory requirements. Audits help identify gaps in security measures and guide improvements.
4. Continuity Planning: Cybersecurity is an integral part of business continuity planning. Organizations must have plans in place to ensure that critical functions can continue during and after a cyber incident.
5. Collaboration and Communication: Effective cybersecurity management requires collaboration across different departments and, in some cases, with external organizations. Clear and consistent communication is key to ensuring that all parties are aligned in their cybersecurity efforts.

Challenges and Opportunities

Managing the human and procedural aspects of industrial cybersecurity presents several challenges. These include keeping up with the rapidly evolving threat landscape, managing the diverse skill sets required, and ensuring that procedures are followed consistently. However, these challenges also present opportunities for innovation and improvement. For instance, advancements in cybersecurity training methods, such as gamification, can make learning more engaging and effective.

1.3 Reliability, Safety, Security and Resilience

Recent cyberattacks on industrial control systems (ICS) have highlighted the growing threat to critical infrastructure and manufacturing. According to a 2023 report by Dragos, a leading industrial cybersecurity firm, 80% of their incident response engagements involved ransomware attacks on industrial organizations. The manufacturing sector was the most targeted, accounting for 30% of attacks, followed by food and beverage at 22% and oil and gas at 15%.

One of the most significant recent incidents was the Colonial Pipeline ransomware attack in May 2021. This attack on the largest fuel pipeline in the United States led to widespread fuel shortages and highlighted the vulnerability of critical infrastructure to cyber threats. The company paid a $4.4 million ransom, though some was later recovered by authorities.

The convergence of Information Technology (IT) and Operational Technology (OT) in industrial settings has expanded the attack surface for cybercriminals. The rise of Industrial

Internet of Things (IIoT) devices and the push towards Industry 4.0 have further complicated the security landscape. According to a 2022 Trend Micro report, 89% of manufacturing organizations experienced cyberattacks on their smart factories in the previous 12 months.

Industrial Automation and Control Systems (IACS) remain particularly vulnerable. These systems, which include Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) systems, are often the backbone of critical infrastructure and industrial processes. The Cybersecurity and Infrastructure Security Agency (CISA) reported a 110% increase in vulnerabilities discovered in industrial control systems from 2020 to 2021.

To address these growing threats, several standards and frameworks have been developed:

1. IEC 62443: This international standard for industrial cybersecurity has gained widespread adoption. It provides a comprehensive framework for securing industrial control systems across various sectors.
2. NIST Cybersecurity Framework: While not specific to industrial systems, this framework provides a flexible approach to managing cybersecurity risk that many industrial organizations have adapted.
3. ISA/IEC 62443: This series of standards, developed jointly by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), provides detailed guidance on implementing secure industrial automation and control systems.

The concept of Defense-in-Depth has become crucial in industrial cybersecurity. This strategy involves implementing multiple layers of security controls to protect against various types of threats. According to a 2022 ABI Research report, spending on industrial cybersecurity solutions is expected to grow from $10 billion in 2021 to $23 billion by 2026, reflecting the increasing emphasis on robust security measures.

As the threat landscape evolves, so do the priorities in industrial cybersecurity. While confidentiality, integrity, and availability remain important, the order of priority in industrial systems often differs from traditional IT environments. In IACS, availability is typically the top priority, followed by integrity and then confidentiality. This is because maintaining continuous operations is often critical in industrial settings, where downtime can have severe consequences.

The challenges in securing industrial systems are compounded by several factors:

1. Legacy systems: Many industrial organizations still rely on outdated systems that were not designed with modern cybersecurity threats in mind.
2. Skill gap: There's a significant shortage of professionals with expertise in both IT and OT security. IBM's 2023 Cyber Resilient Organization Study found that 34% of organizations cite lack of skilled personnel as a major obstacle to achieving cyber resilience.
3. Increasing complexity: As industrial systems become more interconnected and reliant on digital technologies, the complexity of securing them increases.
4. Geopolitical factors: State-sponsored cyberattacks on critical infrastructure have become a growing concern. The 2023 Global Risks Report by the World Economic Forum ranked cybersecurity failure as one of the top ten risks facing the world in the next decade.

To address these challenges, industrial organizations are increasingly adopting advanced technologies such as AI and machine learning for threat detection and response. They are also implementing stricter access controls, network segmentation, and continuous monitoring practices.

As we move forward, the integration of cybersecurity into the fabric of industrial operations will be crucial. This includes not only technological solutions but also a focus on building a culture of security awareness among employees at all levels of industrial organizations. The future of industrial cybersecurity lies in creating resilient systems that can not only defend against attacks but also quickly recover and adapt in the face of evolving threats.

1.4 Industry 4.0/5.0 Context

The rapid digitalization of industry and the reinforcing influence of telecommunication technologies, providing high-speed data transmission and direct customer engagement, have brought new challenges for enterprises with the implementation of Industry 4.0 technologies. These developments have reinforced the importance of cybersecurity for global supply and value chains.

As we transition towards Industry 5.0, which emphasizes human-centric and sustainable approaches, the cybersecurity landscape continues to evolve, presenting both challenges and opportunities for the chemical and energy carriers industries.

1.5 Time for Ensuring Resilience by Complexing Safety and Security

In this Manual, security is conceptualized as a multi-faceted domain encompassing physical, cyber, and information components, while safety is addressed through functional, ecological, and human-centric aspects. This holistic approach is designed to address the complex interdependencies within critical infrastructure sectors, including but not limited to chemical and energy industries, in the context of Industry 4.0 and beyond.

The rapid advancement of digital technologies, including artificial intelligence (AI), Internet of Things (IoT), and 5G networks, is fundamentally transforming industrial landscapes. This digital revolution, while offering unprecedented opportunities for efficiency and innovation, also introduces new vulnerabilities and challenges. The concept of resilience in this evolving context extends beyond traditional notions of risk management to encompass adaptive capacity, operational continuity, and rapid recovery in the face of both known and unforeseen threats.

The increasing complexity of cyber-physical systems in critical domains, particularly in Chemical, Biological, Radiological, and Nuclear (CBRN) facilities, amplifies the potential consequences of security breaches or safety failures. Recent incidents, such as the Colonial Pipeline ransomware attack in 2021, underscore the far-reaching impacts of cyber disruptions on critical infrastructure and highlight the urgent need for robust, integrated security and safety measures.

To achieve comprehensive risk reduction and enhance resilience, a paradigm shift towards a "big" safety and security model is essential. This approach integrates safety and security across Information Technology (IT), Operational Technology (OT), and strategic management levels, recognizing the convergence of these previously siloed domains. The model, aligned with the framework discussed in Chapter 8, acknowledges the interconnected nature of modern industrial systems and the need for a dynamic, adaptive strategy to address emerging and evolving threats.

Key elements of this contemporary approach include:

1. AI-Driven Integrated Cybersecurity and Safety Systems: Leveraging advanced AI and machine learning algorithms for real-time threat detection, anomaly identification, and automated incident response. This includes the implementation of adaptive defense-in-depth strategies that evolve based on emerging threat intelligence.
2. Quantum-Ready Security Measures: Preparing for the post-quantum era by implementing quantum-resistant cryptographic algorithms and exploring quantum key distribution for ultra-secure communication, particularly crucial for protecting sensitive data in CBRN facilities.
3. Zero Trust Architecture: Adopting a "never trust, always verify" approach across all levels of the industrial ecosystem, including IoT devices, cloud services, and third-party integrations. This principle is essential in an era of distributed work environments and interconnected supply chains.
4. Advanced Threat Intelligence and Predictive Analytics: Utilizing big data analytics and AI to predict potential security and safety risks, enabling proactive mitigation strategies rather than reactive responses.
5. Cyber-Physical Resilience by Design: Integrating security and safety considerations from the earliest stages of system and process design, ensuring that resilience is built into the core of industrial operations rather than added as an afterthought.
6. Human-AI Collaboration in Security Operations: Developing advanced security operations centers (SOCs) that optimize the synergy between human expertise and AI capabilities, enhancing threat detection and response capabilities.
7. Continuous Adaptive Risk and Trust Assessment (CARTA): Implementing dynamic risk assessment models that continuously evaluate and adjust security measures based on real-time threat landscapes and operational contexts.
8. Privacy-Enhancing Technologies (PETs): Incorporating advanced privacy-preserving techniques such as homomorphic encryption and secure multi-party computation to enable data analysis and sharing without compromising sensitive information.
9. Cyber Range Training and Digital Twins: Utilizing virtual environments and digital replicas of industrial systems for advanced training, scenario planning, and testing of security measures without risking live operations.
10. Ethical AI and Responsible Innovation: Ensuring the development and deployment of AI systems adhere to ethical guidelines, with a focus on transparency, accountability, and fairness in decision-making processes.

This integrated approach to resilience aligns with and extends beyond the core competencies outlined in the key qualifications developed by the International Centre for

Chemical Safety and Security (ICCSS). It recognizes the need for continuously evolving skill sets and knowledge bases in the rapidly changing digital landscape.

By adopting this comprehensive "big" safety and security approach, industries can not only prepare for current threats but also position themselves to adapt to future challenges. This strategy ensures operational continuity, protects critical infrastructure, and maintains public trust in an era characterized by technological convergence, geopolitical uncertainties, and unprecedented digital interconnectedness.

In conclusion, the path to true resilience in the modern industrial context requires a paradigm shift in how we conceptualize and implement safety and security measures. It demands a forward-thinking, adaptive approach that leverages cutting-edge technologies while remaining grounded in robust risk management principles and ethical considerations. As we move towards increasingly autonomous and interconnected industrial systems, the integration of safety, security, and resilience will be paramount in shaping a sustainable and secure future for critical infrastructure sectors.

1.6 Objectives and Scope

1.6.1 Objectives of Manual

The primary objectives of this Manual are to elucidate the interplay between cybersecurity, reliability, and resilience in the chemical and energy carriers industries. Assurance is examined as a concept for establishing confidence that critical systems meet their requirements.

The current state of the art in cybersecurity, reliability, and resilience for these industries reveals gaps in addressing the unique characteristics of these critical domains. Therefore, special attention is paid to their vital peculiarities.

This Manual provides recommendations for industrial cybersecurity based on the IEC 62443 series of standards for countering cyberattacks in Industrial Automation and Control Systems (IACS). While primarily designed for IACS managers in industrial enterprises and other critical infrastructure, it will benefit all managers and specialists involved in enterprise cybersecurity measures.

1.6.2 Objectives "Beyond the Horizon of the Manual"

This Manual aims to provide a forward-looking perspective, preparing industries not just for current challenges but equipping them to proactively address future cybersecurity risks and opportunities. Key focus areas include:

1. Future Cybersecurity Threats: Assessing potential threats, including advanced persistent threats, AI-driven attacks, and quantum computing's impact on encryption and data security.
2. Emerging Technologies: Analyzing how blockchain, Internet of Things (IoT), 5G networks, and edge computing will transform the industrial cybersecurity landscape.

3. Adapting to Changing Global Dynamics: Considering geopolitical shifts and their impact on cybersecurity, including nation-state cyber warfare and cyber espionage tactics.
4. Industry 5.0 and Beyond: Projecting into the era of Industry 5.0, focusing on the integration of human-centric technologies, advanced robotics, and AI in industrial operations, and their cybersecurity implications.
5. Regulatory Evolution: Predicting future changes in international and national cybersecurity regulations and standards, preparing industries for compliance and proactive engagement with regulatory bodies.
6. Cybersecurity as a Strategic Business Function: Elevating cybersecurity from a technical issue to a strategic business function, integral to enterprise risk management and business continuity planning.
7. Developing a Future-Ready Workforce: Addressing the need for continuous skill development and training programs to prepare the workforce for emerging cybersecurity challenges and technologies.
8. Collaborative Security Efforts: Encouraging greater collaboration among industries, governments, and international bodies to develop unified and effective responses to global cybersecurity threats.

1.6.3 Scope

The scope of this Manual is comprehensive and multi-faceted, targeting a broad spectrum of concerns within cybersecurity, reliability, and resilience, specifically tailored to the chemical and energy carriers industries. Key areas of focus include:

1. Industrial Automation and Control Systems (IACS): In-depth coverage of cybersecurity strategies, best practices, and risk management for IACS.
2. Stakeholder Engagement: Addressing the diverse needs of various stakeholders, including managerial staff, cybersecurity specialists, and operational personnel.
3. Industry-Specific Challenges: Exploring unique cybersecurity challenges and resilience strategies pertinent to the chemical and energy sectors.
4. Regulatory Compliance and Standards: Guiding adherence to relevant cybersecurity regulations and standards, including international and national frameworks.
5. Emerging Trends and Technologies: Keeping pace with the latest developments in technology and cybersecurity threats.
6. Practical Implementation: Providing actionable advice and strategies for implementing cybersecurity measures.
7. Resilience and Recovery: Focusing on building resilience against cyber threats and establishing robust recovery protocols.

1.6.4 Approach

The approach of this Manual is holistic, bridging the gap between theoretical knowledge and real-world practice in industrial cybersecurity. Key elements include:

1. Integration of Theory and Practice: Melding academic concepts with practical, industry-driven applications.
2. Utilization of Case Studies: Incorporating real-world scenarios from the chemical and energy sectors.
3. Focus on Best Practices: Emphasizing proven strategies and methods for enhancing cybersecurity and resilience.
4. Dynamic Content: Regularly updating content to reflect the latest trends and developments.
5. Stakeholder Involvement: Engaging cybersecurity experts, industry practitioners, and regulatory bodies to ensure comprehensive and relevant perspectives.
6. Actionable Insights: Providing clear, step-by-step guidelines for implementing effective cybersecurity measures.

1.6.5 Structure

The Manual contains eight substantive chapters, each focusing on various aspects of cybersecurity, reliability, and resilience in the chemical and energy carriers industries:

1. Methodology: Outlining foundational methodologies and principles guiding IT-OT-ET safety and security management systems, including cyber security, reliability and resilience concepts, lifecycle models, and regulatory frameworks.
2. Security (Information, Cyber, Physical) for Resilience: Covering a wide range of topics from cybersecurity governance and frameworks to security architecture, operations, and industrial automation and control systems (IACS) security.
3. Safety (Functional): Delving into the regulatory framework for functional safety, including standards like IEC 61508 and IEC 61511, safety audits, assessments, and best practices.
4. Risk Management and Security Audits of OT Systems and Processes: Addressing standards, guidelines, and practices for managing risks and conducting security audits in operational technology (OT) environments.
5. Developing Competencies and Training in Reliability and Cybersecurity Management in the Industrial Sector: Discussing the evolving cybersecurity landscape, professional competencies, and training programs for the industrial sector.
6. Industrial Reliability, Cybersecurity, and Resilience Education: Concept: Presenting an integrated educational framework for developing necessary competencies and skills in industrial cybersecurity and resilience.
7. Digitalization of Energy Assets for Measuring Risk – Roadmap for Insurance and the Role of Cybersecurity and Reliability: Presenting now the digital transformation of the energy sector has revolutionized how risk is measured and managed, particularly in the context of insurance.
8. Cyber and AI Risks for CBRN-Related Facilities - Industrial Cybersecurity and Reliability Protection Strategies: Examining potential cyber and AI-related risks to Chemical, Biological, Radiological, and Nuclear facilities and outlining comprehensive mitigation strategies.

Each chapter offers both theoretical insights and practical applications, addressing the critical needs of the chemical and energy carriers industries in the evolving landscape of Industry 4.0/5.0. The Manual provides a comprehensive approach to understanding and implementing cybersecurity, reliability, and resilience measures in these critical sectors.

1.7. Key Terminology and Acronyms

The key terminology, used definitions and acronyms in the Manual are based on the international normative regulations – IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems" series, IEC 62443 "Industrial communication networks - IT security for networks and systems" series, IEC/ISO 15408 the Common Criteria for Information Technology Security Evaluation, IEC TR 63069 "Industrial-process measurement, control and automation - Framework for functional safety and security", ISO 22316:2017 "Security and resilience — Organizational resilience — Principles and attributes", ISO/IEC 27032:2023 "Cybersecurity — Guidelines for Internet security", HSPD-7 "Homeland Security Presidential Directive 7", NIST Special Publication 800-30 "Guide for Conducting Risk Assessments", NIST series SP 800, NISTIR 8074.

Critical Infrastructure Sectors – Information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping [HSPD-7]

Dependability – of a (computing) system is the ability to deliver service that can justifiably be trusted [A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Transactions on dependable and secure computing, Vol. 1, No. 1, January-March 2004]

Reliability – the ability of an item to perform a required function under given conditions for a given time interval [IEC TR 62511:2014]

Reliability – probability that a component, device, or assembly functions properly for a definite period of time under the influence of specific environmental and operational conditions [IEC 60194-1:2021]

Resilience – (organizational) is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper [ISO 22316:2017]

Safety – freedom from unacceptable risk [IEC 61508-4:2010].

Security – [IEC TS 62443-1-1:2009]

a) measures taken to protect a system;

b) condition of a system that results from the establishment and maintenance of measures to protect the system;

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss;

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems;

e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system.

Cybersecurity – safeguarding of people, society, organizations and nations from cyber risks [ISO/IEC 27032:2023].

Cybersecurity – the ability to protect or defend the use of cyberspace from cyberattacks [NIST SP 800-30].

Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [NIST SP 800-30].

Assurance – measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy [CNSSI 4009].

Assurance Case – a structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute [Software Engineering Institute, Carnegie Mellon University].

ET – environmental technologies

IT – information technology

OT – operational technology

Cyber resilience taxonomy

Cyber Resilience – the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources [NIST SP 800-160 Vol. 2].

Information System Resilience – The ability of a system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and recover to an effective operational posture in a time frame consistent with mission needs [NIST SP 800-53].

Resilience in Cyberspace – The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption [Department of Homeland Security Risk Steering Committee].

Operational Resilience – The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions [Department of Defense].

2 METHODOLOGY FOR INTEGRATED CYBERSECURITY AND SAFETY MANAGEMENT

2.1 General Structure of Safety and Security Management System

The proposed approach of treating the mentioned dependability attributes (safety, security and reliability) interplay for chemical and energy carriers industries (but not limited to) can be represented in a form of IT, OT and ET management systems which in its union form enterprise security management system.

The integration of the enterprise security management system into the enterprise management system involves the interaction of production process management subsystems with security management subsystems. A similar interaction exists between production subsystems and subsystems that describe several levels of security - namely the signal, information and physical levels. The formation of security subsystems for these levels can be carried out using different methods of forming management systems,

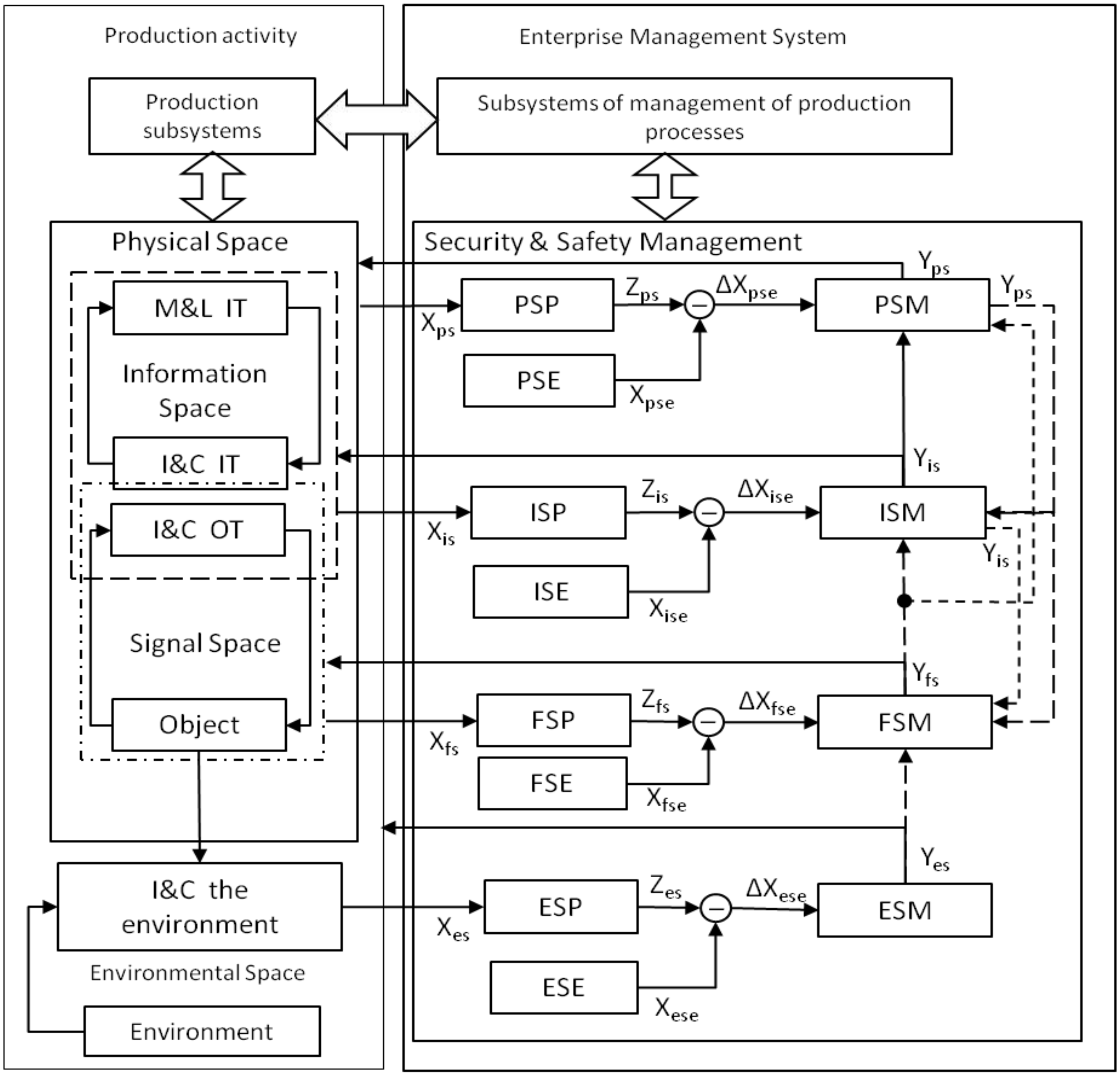
In the following structure (Fig. 2.1) of the integrated representation of enterprise security by allocation in its structure of the systems responsible for physical security is offered – Information security and functional security with environmental management system. The global digitalization of industry poses the problem of cyber threats to any of the information processes that are implemented using digital technologies for receiving, transmitting, storing and presenting data and information.

Developed and applied information technologies are based on a functional representation. Best practices claim that the most significant is the methodology of enterprise representation where the physical, informational and cybernetic (in the form of data transmission) components are represented explicitly. This requirement is especially important in Industry 4.0.

Further development of the enterprise security management system is a system that includes an environmental management channel (Fig. 2.2).

The interrelation between IT, OT and, ET of the enterprise and the environment is described on the Figure 2.3, whereas IT – information technology (resources/assets), OT – information technology (resources/assets), ET – environment/engineering technology (resources/assets), PhSM – physical security management (channel), PhSM – physical security management (channel), ISM – information/cyber security management (channel), FSM – functional safety management (channel), ESM – ecological safety management (channel), C – coordination units, AEntMS – automated enterprise management system, ATPMS – automated technology processes management system, ATPEcMS – automated technology processes and ecology management system, ATPEcMS – automated technology processes and ecology management system, AEcPMS – automated ecology management system.

The nesting of the assets of the enterprise (in terms of the Manual “spaces”) is depicted in the Figure 2.3, where Physical, Data, Signal, Ecological spaces are nested within one another.



M&L – management & logistic; I&C – instrumentation & control;
OT – operation technical; IT – information technical; PS – Physical Security
IS – Information Security; P – processing; E – Etalon; M – Maker
ES – Environmentall Securiti

Figure 2.1 – Integrated enterprise management system with environmental management system

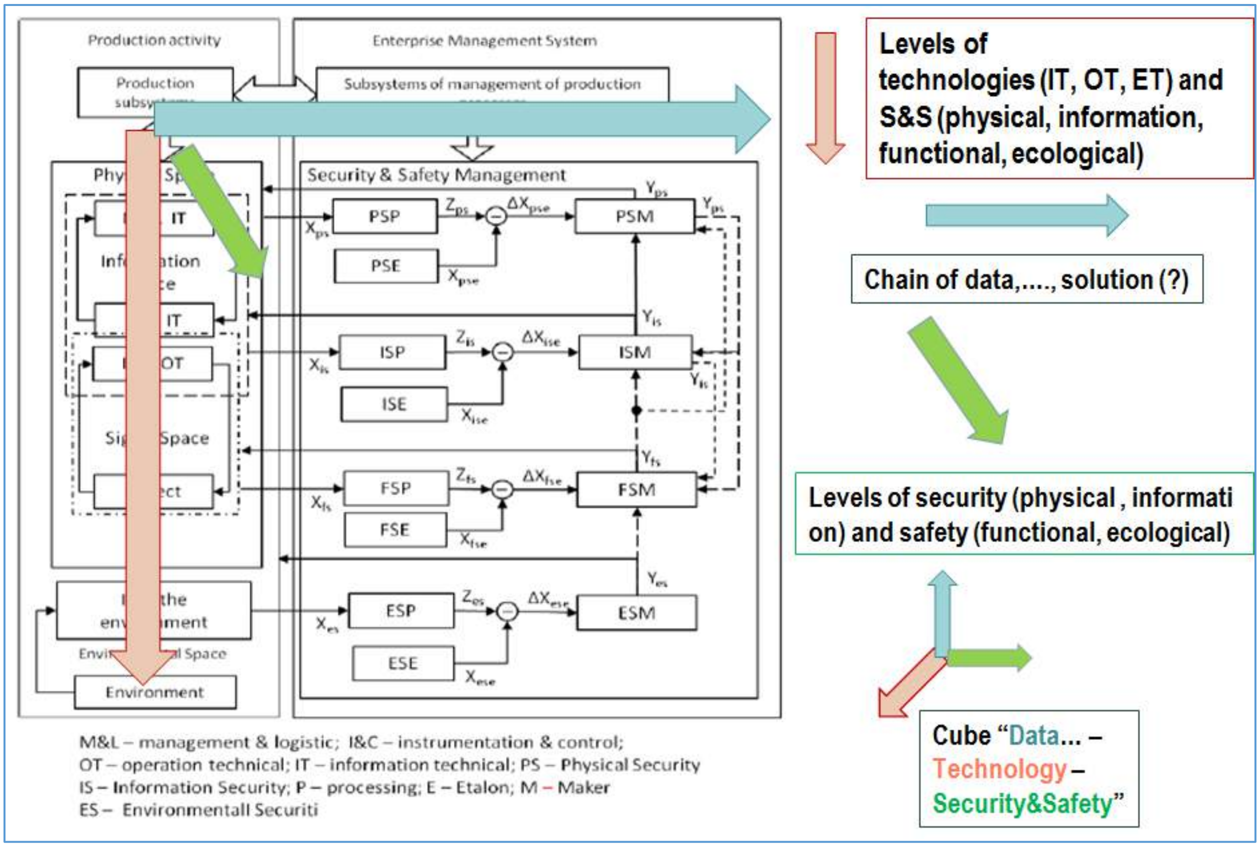

Production activity
Enterprise Management System
Production subsystems
Subsystems of management of production
Security & Safety Management
IT
Information Space
IT
OT
Signal Space
Object
the environment
Environmental Space
Environment
PSP
PSE
PSM
ISP
ISE
ISM
FSP
FSE
FSM
ESP
ESE
ESM
Z_{ps}
ΔX_{pse}
X_{ps}
X_{pse}
Y_{ps}
Z_{is}
ΔX_{ise}
X_{is}
X_{ise}
Y_{is}
Z_{fs}
ΔX_{fse}
X_{fs}
X_{fse}
Y_{fs}
Z_{es}
ΔX_{ese}
X_{es}
X_{ese}
Y_{es}
M&L – management & logistic; I&C – instrumentation & control;
OT – operation technical; IT – information technical; PS – Physical Security
IS – Information Security; P – processing; E – Etalon; M – Maker
ES – Environmentall Securiti
Levels of technologies (IT, OT, ET) and S&S (physical, information, functional, ecological)
Chain of data,...., solution (?)
Levels of security (physical , informati on) and safety (functional, ecological)
Cube "Data... – Technology – Security&Safety"

Figure 2.2 – Integrated enterprise management system with environmental management system

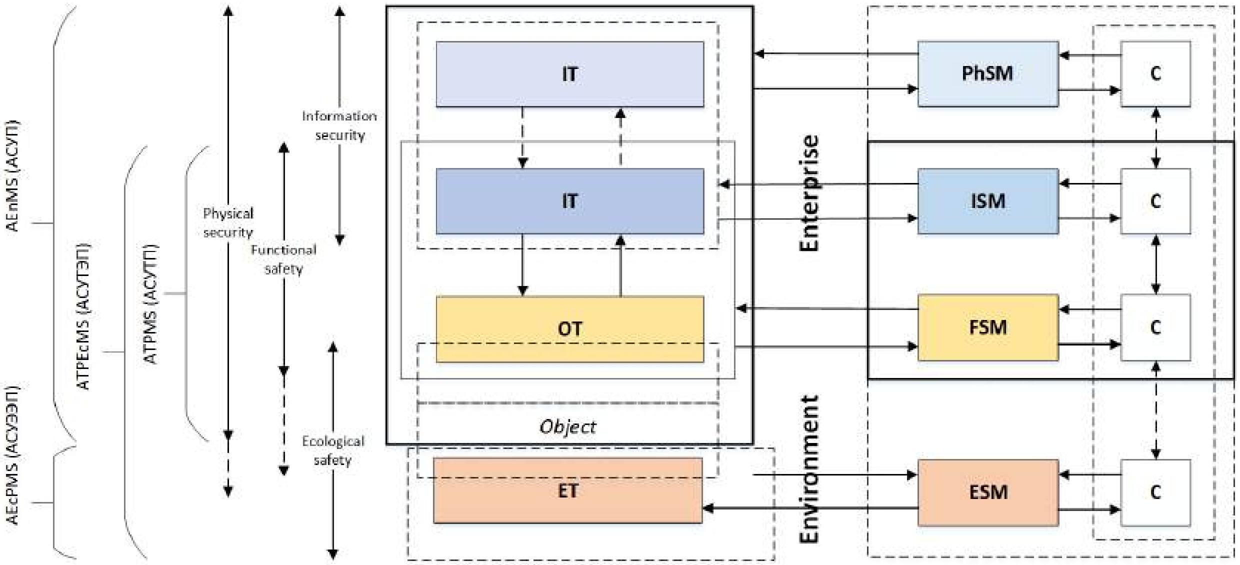


Figure 2.3 – Structure of integrated safety and security management system

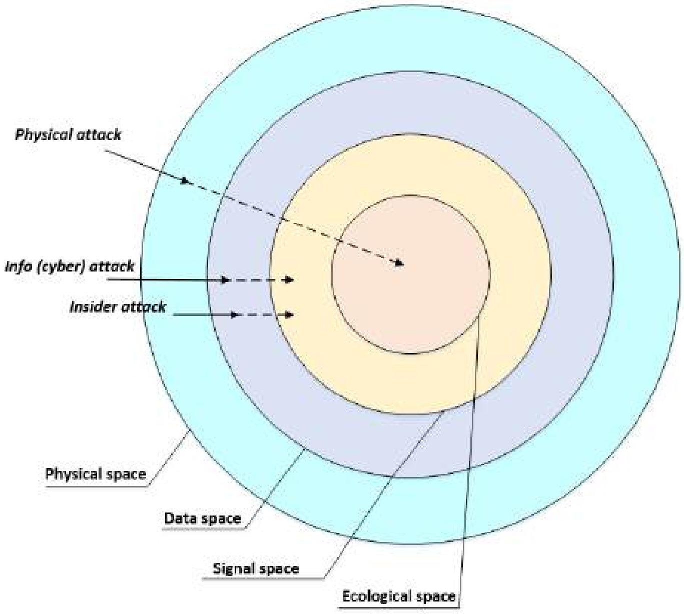


Figure 2.4 – Scheme of the spaces (assets)

The main features of the presented method of integrating the environmental management system into the enterprise management system are as follows:

- sources of information are actually technological processes for which additional special sensors of deviations of technological parameters from the set, and also sensors of system of monitoring of parameters of environment are provided;
- the methodological basis for building an environmental management system is the theory of automated and automatic control systems, which provides for the modeling of both control objects and the control system itself.
- the main attention in the work of the environmental management system is focused on the management of environmental safety risks and not on the continuous improvement of the actual elements of the system itself.

2.2 Regulation

2.2.1 Standards as a Base for Safety, Security and Resilience

The regulation procedures are described in the international standards on process and functional safety, security (including cyber aspects), resilience (the organizational aspect).

There are no industry-specific standards on resilience for chemical and energy carriers industries. One of the possible evolving ways could be in adopting the existing regulations on safety and security to address resilience for the mentioned safety-critical domains.

2.2.2 Requirements Profiling and Harmonization

European regulation and procedures are based on the documents developed by ISO/IEC and IEEE organizations. In the USA the dominant body is NIST. All mentioned bodies develop and umbrella-level standards, which should be implemented on the several levels, e.g. national, industry, enterprise. The already existed regulation base in the countries sometimes may it different to use the international standard in a form “as it is”, so the harmonization of cybersecurity, reliability and resilience requirements with the development of the corresponding methodology for its assurance can be the solution. At the same time the profiling of high-level requirements into the project/object specific seems as a better option (in terms of time to market and costs reduction) if the national standardization bodies and compliance procedures will allow to do that.

2.2.3 Standardization of Security for Safety-Critical Systems

2.2.3.1 General Analysis

At the present security standards are developed by many national and international standardization organizations. The most relevant to safety critical systems are the following security standards sets:

- ISO/IEC 27000 “Information technology – Security techniques – Information security management systems” standards family states requirements to the Information Security Management System (ISMS) independently from type of computer system or organization; this series contains about 40 parts and is an umbrella document for all other documents in security;
- ISO/IEC 15408 “Information technology – Security techniques –Evaluation criteria for IT security” establishes Common Criteria to evaluate security functions and assurance techniques for information product;
- ISA/IEC 62443 “Security for Industrial Automation and Control Systems”;
- The United States National Institute of Standards and Technology (NIST) developed NIST SP 800 series which cover many security issues; formally NIST standards are national but many countries and companies apply it as valuable state-of-the-art requirements; the NIST Cybersecurity Framework (SCF) based on NIST SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”;
- Institute of Electrical and Electronics Engineers (IEEE) standards, such as IEEE 1686-2007 “Standard for Substation Intelligent Electronic Devices IED Cybersecurity Capabilities”, IEEE P1711 “Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links”, IEEE 1815-2012 “Standard for Electric Power System Communications-Distributed Network Protocol (DNP3)”;
- Standards applicable to specific domains which give details of the above standards requirements; we consider nuclear standard IEC 62645 “Nuclear power plants – Instrumentation and control systems – Cybersecurity requirements” with associated IEC 62859 “Nuclear power plants – Instrumentation and control systems – Coordination between safety and cybersecurity” and IEC 62988 “Nuclear power plants – Instrumentation and control important to safety – Selection and use of wireless devices”.

Also, it should be mentioned a lot of activities, performed in different industrial domains by technical and research organizations. The most powerful organizations are working in USA as a part of the continuing effort to provide effective security standards and guidance to federal agencies and their contractors in support of the Federal Information Security Management Act

(FISMA). FISMA was signed into law part of the Electronic Government Act of 2002. There are the following organizations, addressing security:

- The USA Department of Energy (DOE) developed the Cybersecurity Capability Maturity Model (C2M2) from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) by removing sector specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the DOE, in partnership with the Department of Homeland Security (DHS), and in collaboration with private and public sector experts;
- The American Gas Association (AGA), representing energy utility organizations that deliver natural gas customers industries throughout the United States. The AGA 12 series of documents recommends practices designed to protect supervisory control and data acquisition (SCADA) communications against cyber incidents;
- The American Petroleum Institute represents members involved in all aspects of the oil and natural gas industry. API 1164 provides guidance to the operators of oil and natural gas pipeline systems for managing SCADA system integrity and security;
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS Strategy for Securing Control Systems. ICS-CERT works with the control systems community to ensure that recommended practices, which are made available, have been vetted by subject-matter experts in industry before being made publicly available in support of this program;
- The North American Electric Reliability Corporation (NERC) mission is to improve the reliability and security of the bulk power system in North America. NERC has issued a set of security standards, named as Critical Infrastructure Protection (SIP), to reduce the risk of compromise to electrical generation resources and high-voltage transmission systems above 100 kV, also referred to as bulk electric systems.

Also, there are a lot of non-profit organizations which develop free guidelines and best practices on security issues including the following:

- The Open Web Application Security Project (OWASP) Foundation supports the following projects: OWASP Software Assurance Maturity Model, OWASP Development Guide, OWASP Testing Guide, OWASP Code Review Guide etc.;
- The Institute for Information Infrastructure Protection (I3P) is a consortium of leading national cybersecurity institutions, including academic research centers, government laboratories, and non-profit organizations. It was founded in September 2001 to help meet a well-documented need for improved research and development (R&D) to protect the nation's information infrastructure against catastrophic failures. The institute's main role is to coordinate a national cybersecurity R&D program and help build bridges between academia, industry, and government;
- International Professional Association ISACA (the former Information Systems Audit and Control Association) developed the good-practice framework Control Objectives for Information and Related Technologies (COBIT) which is created for information technology management IT governance. COBIT provides an implementable set of controls over information

technology and organizes them around a logical framework of IT-related processes and enablers. COBIT components include process descriptions, control objectives, management guidelines, and maturity models;

- Center for Internet Security (CIS) released Critical Security Controls for Effective Cyber Defense (CSC) framework, which is also known as CIS CSC or CCS CSC. CCS CSC includes he guidelines consist of 20 key actions, called CSC, that organizations should take to block or mitigate known attacks. The controls are designed so that primarily automated means can be used to implement, enforce and monitor them.

Taking into account variety of security standards, it should be noted they focus on some common issues. These issues include the following:

- Risk Management and Assessment;
- Information Security Management System;
- Security Life Cycle;
- Security Levels;
- Failures and attack avoidance;
- Security and safety relation for critical systems.

Below in this section a survey is done for the main security standards, such as ISO/IEC 27000, ISA/IEC 62443, and NIST SP 800.

2.2.3.2 Standards Family ISO/IEC 27000

ISO/IEC 27000 “Information technology – Security techniques– Information security management systems” standards family contains about 40 parts and is an umbrella document for all other documents in security. Now many parts of ISO/IEC 27000 are booming, so many new parts are appearing and some existing parts are reworking once per 3-5 years.

The title standard in the family is ISO/IEC 27000:2016 “Information security management systems – Overview and vocabulary”.

All ISO/IEC 27000 standards family can be divided in the three following sets:

- Standards specifying requirements;
- Standards describing general guidelines;
- Standards describing sector-specific guidelines.

Standards specifying requirements include the following:

- ISO/IEC 27001 “Information security management systems – Requirements” formally specifies ISMS against which thousands of organizations have been certified compliant;
- ISO/IEC 27006 “Requirements for bodies providing audit and certification of information security management systems” provides a formal guidance for the for accredited organizations which certify other organizations compliant with ISO/IEC 27001;
- ISO/IEC 27009 “Sector-specific application of ISO/IEC 27001 – Requirements” at the time of 2016 is existing as a draft intended to provide guidance for those developing new ISO/IEC 27000 family standards.

Standards describing general guidelines include the following:

- ISO/IEC 27002 "Code of practice for information security controls" provides a reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
- ISO/IEC 27003 "Information security management system implementation guidance" provides basic advices on implementing ISO/IEC 27001;
- ISO/IEC 27004 "Information security management – Measurement" provides description for a set of security metrics,
- ISO/IEC 27005 "Information security risk management" discusses risk management principles;
- ISO/IEC 27007 "Guidelines for information security management systems auditing" provides recommendations for auditing of management elements of the ISMS;
- ISO/IEC TR 27008 "Guidelines for auditors on information security management systems controls" provides recommendations for auditing the information security elements of the ISMS;
- ISO/IEC 27013 "Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1" combining ISO/IEC 27000 ISMS with ISO/IEC 20000 IT Service Management, particularly for ITIL (IT Infrastructure Library)
- ISO/IEC 27014 "Governance of information security" provide governing recommendations in the context of information security;
- ISO/IEC TR 27016 "Information security management – Organizational economics" provides economic theory applied to information security.

Standards describing sector-specific guidelines cover such domains as energy, medicine, telecommunications, finance, cloud computing and others.

For example, ISO/IEC 27010 "Information security management for inter-sector and inter-organisational communications" sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure".

2.2.3.3 Standards Series ISO/IEC 15408

Standards series ISO/IEC 15408, which is also known as the Common Criteria includes the following three parts:

- ISO/IEC 15408-1 "Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model";
- ISO/IEC 15408-2 "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components";
- ISO/IEC 15408-3 "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security assurance components";

Part 1 "Introduction and general model" defines the general concepts and principles of IT security evaluation and presents a general model of evaluation (see Fig. 2.5). At the time evaluation concept is based on a confidence in correctness and sufficiency of security countermeasures (see Fig.2.6).

Part 2 "Security functional components" establishes a set of functional components that serve as standard templates upon which to base functional requirements for Targets of

Evaluation (TOEs). ISO/IEC 15408-2 catalogues the set of functional components and organizes them in families and classes. There are the following classes of functional components described in ISO/IEC 15408-2: Security audit, Communication, Cryptographic support, User data protection, Identification and authentication, Security management, Privacy, Protection of the security functionality, Resource utilization, Access, Trusted path/channels.

Part 3 “Security assurance components” establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs. ISO/IEC 15408-3 catalogues the set of assurance components and organizes them into families and classes. There are the following classes of assurance components described in ISO/IEC 15408-3: Development, Guidance documents, Life-cycle support, Security Target evaluation, Tests, and Vulnerability assessment.

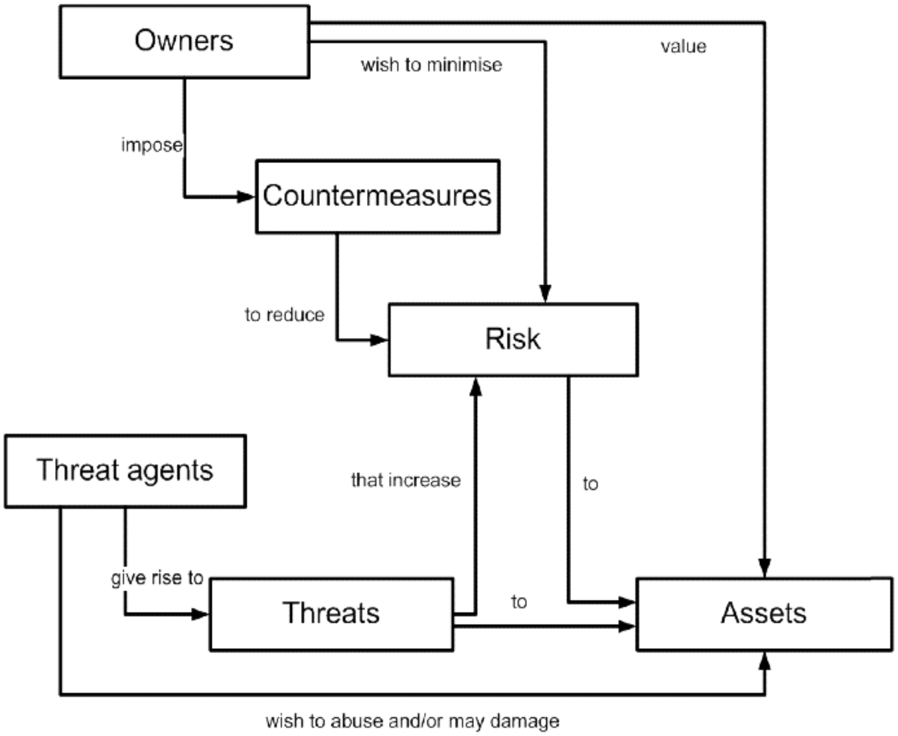


Figure 2.5 – Security concepts and relationships (source: ISO/IEC 15408-1)

ISO/IEC 15408-3 also defines evaluation criteria for Protection Profiles and Security Targets and presents seven pre-defined assurance packages which are called the Evaluation Assurance Levels (EALs). ISO/IEC 15408-3 states the following EALs:

- EAL1: functionally tested;
- EAL2: structurally tested;
- EAL3: methodically tested and checked;
- EAL4: methodically designed, tested, and reviewed;
- EAL5: semiformally designed and tested;
- EAL6: semiformally verified design and tested;
- EAL7: formally verified design and tested.

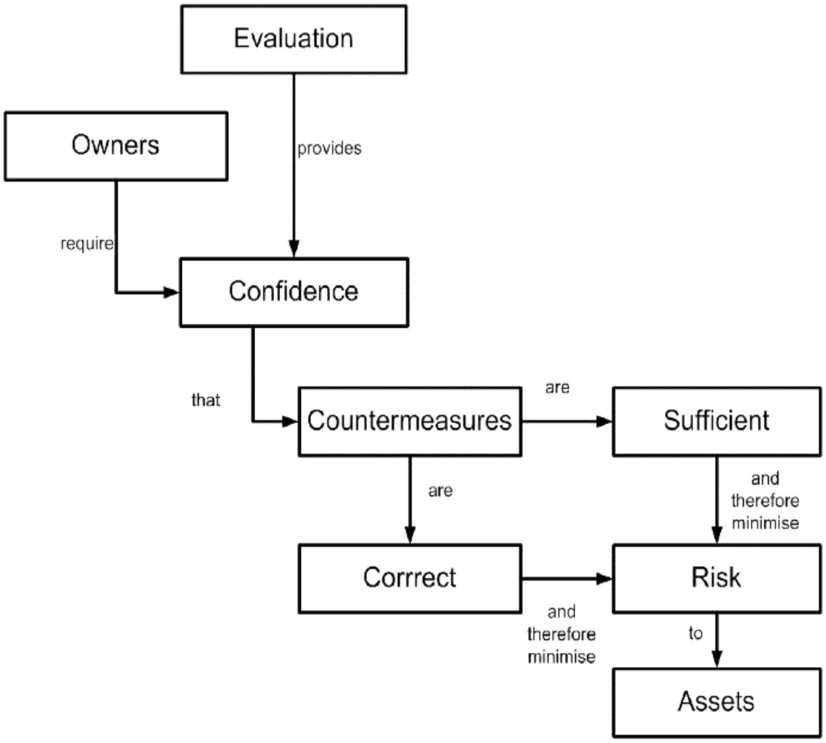


Figure 2.6 – Evaluation concepts and relationships (source: ISO/IEC 15408-1)

2.2.3.4 Standards Series ISA/IEC 62443

Originally these standards have been developed by International Society of Automation (ISA) as series ANSI/ISA-99.00.

After that these standards have been adopted by International Electrotechnical Commission. At the present there are the following standards in force adopted by IEC:

- IEC TS 62443-1-1:2009 “Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models”;
- IEC 62443-2-1:2010 “Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program”;
- IEC TR 62443-2-3:2015 “Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment”;
- IEC 62443-2-4:2015 “Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers”;
- IEC PAS 62443-3:2008 “Security for industrial process measurement and control – Network and system security”;
- IEC TR 62443-3-1:2009 “Industrial communication networks - Network and system security – Part 3-1: Security technologies for industrial automation and control systems”;
- IEC 62443-3-3:2013 “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”.

Now a structure of series is updated and new versions of the standards are in progress. ISA is developing master versions for the 62443 series, after that IEC should reissue identical standards. The developed 62443 series includes the following thirteen standards divided into four groups:

1) General:

- ISA/IEC 62443-1-1 “Terminology, concepts and models”;
- ISA/IEC 62443-1-2 “Master glossary of terms and abbreviations”;
- ISA/IEC 62443-1-3 “System security compliance metrics”;
- ISA/IEC 62443-1-4 “Industrial Automation and Control Systems (IACS) security lifecycle and use-case”;

2) Policies and Procedures:

- ISA/IEC 62443-2-1 “Requirements for an IACS security management system”;
- ISA/IEC 62443-2-2 “Implementation guidance for an IACS security management system”;
- ISA/IEC 62443-2-3 “Patch management in the IACS environment”;
- ISA/IEC 62443-2-4 “Installation and maintenance requirements for IACS suppliers”;

3) System:

- ISA/IEC TR 62443-3-1 “Security techniques for IACS”;
- ISA/IEC 62443-3-2 “Security levels for zones and conduits”;
- ISA/IEC 62443-3-3 “System security requirements and security levels”;

4) Component:

- ISA/IEC 62443-4-1 “Product Development Requirements”;
- ISA/IEC 62443-4-2 “Technical Security Requirements for IACS Components”.

The ISA/IEC 62443 series address the needs to design electronic security robustness and resilience into industrial automation control systems (IACS). Robustness provides the capabilities for the IACS to operate under a range of cyber-induced perturbations and disturbances. Resilience provides the capabilities to restore the IACS after unexpected and rare cyber-induced events. Robustness and resilience are not general properties of IACS but are relevant to specific classes of cyber -induced perturbations. An IACS that is resilient or robust to a certain type of cyber-induced perturbations may be brittle or fragile to another. Such a trade-off is the subject of profiles, which others can derive from the ISA/IEC 62443 requirements and guidelines. The goal in developing the ISA/IEC 62443 series is to improve the availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems. Application of the requirements and guidance in ISA/IEC 62443 is intended to improve electronic security and help to reducing the risk of compromising confidential information or causing degradation or failure of the equipment (hardware and software) of systems under control. The concept of IACS electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Automation and control systems include, but are not limited to:

- Hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems;
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

The requirements and guidance are directed towards those responsible for designing, implementing, or managing IACS. This information also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

2.2.3.5 National Institute of Standards and Technology Cybersecurity Framework

The United States National Institute of Standards and Technology (NIST) has created a framework for improving critical infrastructure cybersecurity, referred to as the NIST Cybersecurity Framework. The main objective of this framework is to offer organizations a list of items for assessing and enhancing their capacity for preventing, detecting and responding to cyberattacks. According to the framework, cybersecurity should be considered part of an organization's risk management operations.

The NIST Cybersecurity Framework is a set of best practice guidelines to help organizations and businesses improve their cybersecurity processes. It was established by NIST under the U.S. Commerce Department. The standards aim at preparing private sector companies to prevent and recover from cyberattacks. Having a website security platform can be vital to follow the framework, because it can protect websites from cyberattacks as well as recover a website if an incident has already occurred.

Moreover, NIST has developed and maintains standards that form the normative basis for ensuring cyber security. FISMA standards, as defined by the NIST, include the following, with emphasis on SP 800-53 and SP 800-137:

- **FIPS 199:** The Federal Information Processing Standard for security categorization in federal information systems
- **FIPS 200:** Minimum security requirement set for federal information and information systems
- **SP 800-18:** Developing security plans for federal information systems
- **SP 800-30:** Conducting risk assessments
- **SP 800-37 Rev.2:** Risk Management Framework for Information Systems and Organizations
- **SP 800-39:** Special publication on managing information security risk
- **SP 800-47 Rev.1:** Managing the Security of Information Exchanges
- **SP 800-53 Rev.5:** Covers security and privacy controls for federal information systems and organizations Addendum SP 800-53A, covers assessment of these controls
- **SP 800-59:** Guideline for identifying an information system as a national security system
- **SP 800-60:** Since August 2008, a guide for mapping types of information systems to security categories
- **SP 800-128:** Security-focused configuration management of information systems
- **SP 800-137:** Information security continuous monitoring for federal information systems and organizations
- **SP 800-160:** A systems security engineering guideline, integrated approach to building trustworthy and resilient systems

NIST SP 800-53 Rev. 5"Security and Privacy Controls for Information Systems and Organizations" provides a catalog of security controls measures. This catalog includes seventeen parts covering different organizational, technical and physical sides of security control (see Fig. 2.7).

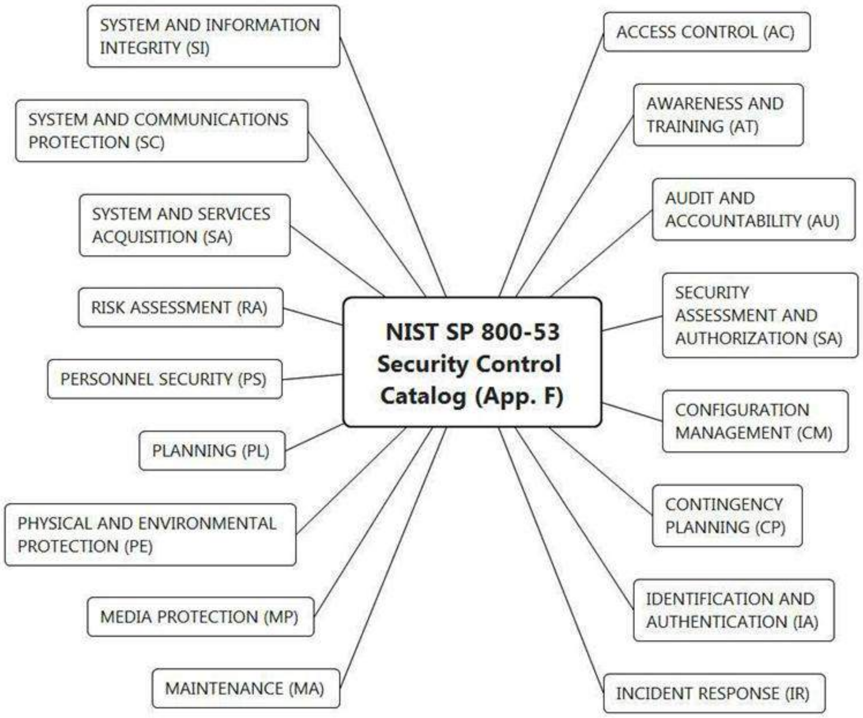

SYSTEM AND INFORMATION INTEGRITY (SI)
SYSTEM AND COMMUNICATIONS PROTECTION (SC)
SYSTEM AND SERVICES ACQUISITION (SA)
RISK ASSESSMENT (RA)
PERSONNEL SECURITY (PS)
PLANNING (PL)
PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)
MEDIA PROTECTION (MP)
MAINTENANCE (MA)
NIST SP 800-53 Security Control Catalog (App. F)
ACCESS CONTROL (AC)
AWARENESS AND TRAINING (AT)
AUDIT AND ACCOUNTABILITY (AU)
SECURITY ASSESSMENT AND AUTHORIZATION (SA)
CONFIGURATION MANAGEMENT (CM)
CONTINGENCY PLANNING (CP)
IDENTIFICATION AND AUTHENTICATION (IA)
INCIDENT RESPONSE (IR)

Figure 2.7 – NIST SP 800-53: Structure of Security Control Catalog

Additionally, NIST SP 800-53 it is a base for NIST CSF which harmonizes security control requirements with the following standards and good practices frameworks:

- ISO/IEC 27000 “Information security management systems;
- ISA/IEC 62443 “Security for Industrial Automation and Control Systems”
- Control Objectives for Information and Related Technologies (COBIT) framework
- Center for Internet Security Critical Security Controls for Effective Cyber Defense framework (CIS CSC).

NIST CSF describes security activities by systematic way dividing into five the main functions: Identify, Protect, Detect, Respond, and Recover.

Each of the function is described through categories which include subcategories. Subcategories refer to Security Control Catalog (Appendix F of NIST SP 800-53), which provides a range of safeguards and countermeasures for organizations and information systems.

The following contains functions and categories description (see Fig. 2.8).

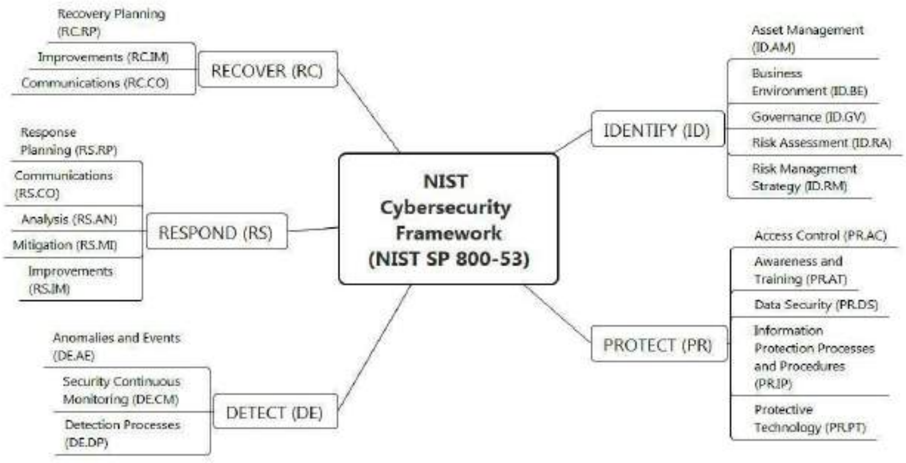

Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)
RECOVER (RC)
Response Planning (RS.RP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
RESPOND (RS)
Anomalies and Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Detection Processes (DE.DP)
DETECT (DE)
NIST Cybersecurity Framework (NIST SP 800-53)
IDENTIFY (ID)
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GV)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
PROTECT (PR)
Access Control (PR.AC)
Awareness and Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes and Procedures (PR.IP)
Protective Technology (PR.PT)

Figure 2.8 – NIST SP 800-53: Cybersecurity Framework (NIST CCF)

“Identify” means to develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities, what should be done with the following categories:

- – Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy;
- Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions;
- Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk;
- Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals;
- Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

“Protect” means to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, what should be done with the following categories:

- Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions;
- Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements;
- Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information;

- Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets;
- Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures;
- Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

"Detect" means to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, what should be done with the following categories:

- Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood;
- Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures;
- Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

"Respond" means to develop and implement the appropriate activities to take action regarding a detected cybersecurity event, what should be done with the following categories:

- Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events;
- Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies;
- Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities;
- Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident;
- Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

"Recover" means to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event, what should be done with the following categories:

- Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events;
- Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities;
- Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, and vendors.

3 SECURITY (INFORMATION, CYBER, PHYSICAL) FOR RESILIENCE

3.1 Cybersecurity Governance

Most organizations have good enterprise-level security policies that define their approach to maintaining, improving, and securing their information and information systems. However, once the policies are signed by senior leadership and distributed throughout the organization, significant cybersecurity governance challenges remain. Organizations must solve five fundamental challenges to cybersecurity governance:

a) Cybersecurity Strategy and Goals;
b) Standardized Processes;
c) Enforcement and Accountability;
d) Senior Leadership Oversight;
e) Resources.

3.1.1 Cybersecurity Strategy and Goals

To establish a good cybersecurity governance program, the organization must clearly define its risk management policies, strategy, and goals. Senior leadership must assess their current risk management approach prior to defining the strategy and goals for the organization's preferred state. The strategy should be a high-level document that establishes the roadmap for the organization to maintain and improve its overall risk management approach. Once the strategy and goals are finalized, an enterprise-level policy must be implemented and distributed throughout the organization. Key components to developing an effective cybersecurity strategy include:

- understanding how cybersecurity risk relates to your critical business operations;
- developing strategic goals for the organization;
- defining the scope;
- identifying cybersecurity needs and develop objectives;
- establishing key performance indicators (KPIs);
- determining resource needs;
- determining risk appetite;
- establishing continuous monitoring.

3.1.2 Standardized Processes

Many organizations have processes and personnel to ensure that daily tasks are completed. However, the management of specific tasks isn't always done as effectively as it could be. Without approved, standardized processes that are repeatable, organizations cannot ensure efficiency, quality, or consistency. Consistency is critical to ensure a common understanding and management approach to risks throughout the organization. Establishing repeatable processes is a key factor in an organization's overall cybersecurity governance program.

3.1.3 Enforcement and Accountability

Processes should be in place to enforce requirements. Otherwise, the cybersecurity program will become inconsistent, requirements will be ignored, and failure will occur. Once those with program responsibilities perceive or observe that accountability and cybersecurity governance are lacking, they will come up with their own way of doing things, which is counter to establishing standardized processes. Cybersecurity governance must be measurable and enforced, and there must be accountability for compliance across all personnel levels.

3.1.4 Senior Leadership Oversight

Because cybersecurity governance is an enterprise concern, the focus and direction for the cybersecurity program must come from the top to ensure that the process is achieving its goals. Unless senior leadership supports cybersecurity governance with a strong "tone at the top" approach, the organization's risk management efforts will most likely fail. Senior leadership must remain engaged in the lifecycle of the program. This engagement helps to ensure that the entire organization not only understands senior leadership's commitment to cybersecurity governance but is implementing it at a high standard. For example ISO 27001, section five, has a list of leadership principles that are relevant in establishing an effective cybersecurity governance program.

Top management shall establish a cybersecurity policy that:

- is appropriate to the purpose of the organization;
- includes information security objectives or the framework for setting information security objectives;
- includes a commitment to satisfy applicable requirements related to information security;
- includes a commitment to continual improvement of the information security management system;
- is available as documented information;
- is communicated within the organization and is available to relevant parties, as appropriate.

3.1.5 Resources

Senior leadership must ensure adequate resources are available to meet basic cybersecurity governance and compliance needs commensurate with the organization's cybersecurity strategy and goals. Funding must be allocated to the highest priorities to secure information and information systems, adequate for the levels of risk. Resourcing must also include dedicated funding for qualified personnel and their training. In addition, resources must allow for the procurement of sufficient tools for adequately measuring KPIs as well as maintaining repeatable processes.

3.2 Cybersecurity Audit

Cybersecurity audit probes the effectiveness and safety of the systems and their security components. Audit plays a very important role in assessing the opportunities for making the organization more secure. Organizations have a number of cybersecurity policies, security restrictions, actions, trainings, practices, and technologies that are used to protect all the data contained in the systems. A cybersecurity audit is an analysis to validate whether all the existing cybersecurity measures are being followed and implemented properly.

The purpose of a cybersecurity audit is to act as a 'checklist' that validates that what you've said in policy is actually happening and that there's a control mechanism in place to enforce it.

As the organizations constantly face cyber-threats, conducting regular cybersecurity audits is an excellent opportunity to assess the cybersecurity effectiveness of an organization. Cybersecurity auditing will help an organization to determine the current level of its cybersecurity, identify vulnerabilities and identify protection mechanisms against possible threats and attacks.

An audit must be performed by an independent third-party organization, and that third party typically must have some kind of certification. (An organization can have an internal audit team, but that team should act as an independent agency).

3.3 Company's Written Supervisory Procedures

Organizations to consider sound principles and effective practices as they develop or enhance their cybersecurity programs. In the development of an effective Cybersecurity program, best practices include written policies and procedures that include:

- defining a governance framework to support decision making based on risk appetite;
- ensuring active senior management, and as appropriate to the firm, board-level engagement with cybersecurity issues;
- identifying frameworks and standards to address cybersecurity;
- using metrics and thresholds to inform governance processes;
- dedicating resources to achieve the desired risk posture; and
- performing a cybersecurity risk assessment.

The organization must prepare customized CyberSecurity Written Supervisory Procedures (WSPs) to protect against the devastating effects of a cyber attack. Thorough and robust CyberSecurity Written Supervisory Procedure (WSP) manuals are at the heart of every good compliance program.

WSPs:

1) provide compliance cybersecurity regulatory scrutiny;

2) provide organization and its employees with a road map to navigate the regulatory rules and obligations;

3) define minimum cybersecurity controls and formalize the oversight of branch offices;

4) mandate the supervision of privileged user system access activities.

WSP is a fundamental component of cybersecurity culture. In it, the organization identifies explicit and implicit cybersecurity norms, practices and expected behaviors designed to influence how employees make and carry out decisions in the course of conducting the cybersecurity program. Reasonably designed WSPs will typically address the “Who”, “What” and “When” along with the document and/or procedure corroborating the cybersecurity policy.

3.4 Executive Management Involvement

Cybersecurity is a CEO-level issue. The risks of cyberattacks span functions and business units, companies and customers. And given the stakes and the challenging decisions posed by becoming cyberresilient, making the decisions necessary can only be achieved with active engagement from the CEO and other members of the senior-management team.

Senior-management time and attention is the biggest driver of maturity in managing cybersecurity risks—more important than company size, sector, and resources provided.

We Recommend four actions common among senior managers:

- Actively engaging in strategic decision making. Just as with other types of enterprise risk, CEOs and the rest of the senior management team must provide input on the organization’s overall level of risk appetite for loss of intellectual property, disclosure of customer information, and disruption of business operations. Subsequent to that, business-unit heads—and their management teams—must engage with cybersecurity managers to help prioritize information assets and make specific trade-offs between risk reduction and operational impact;
- Driving consideration of cybersecurity implications across business functions. Senior managers must ensure business managers incorporate cybersecurity considerations into product, customer, and location decisions, while functional leaders are responsible for addressing cybersecurity considerations in human-resources and procurement decisions. In addition, they make sure that the disclosure of cybersecurity priorities is incorporated into the company’s public-affairs agenda.
- Pushing changes in user behavior. Given how much sensitive data senior managers interact with, they have the chance to change and model their own behavior for the next level of managers. This can begin with simple steps, such as becoming more judicious about forwarding documents from corporate to personal e-mail accounts. In addition, senior management can and should provide the communications “airtime” and reinforcement required to help frontline employees understand what they need to do to protect critical information assets.

Ensuring effective governance and reporting is in place. No matter how thoughtful a set of cybersecurity policies and controls maybe, some managers will seek to circumvent them. Senior management obviously needs to make sure that policies and controls make sense from a business standpoint. If they do, senior managers then need to backstop the cybersecurity team to help with enforcement. In addition, senior management should put in place effective, granular reporting on how the company is progressing against specific milestones in its cybersecurity program.

Cybersecurity standards are collections of best practice, created by experts to protect organisations from cyber threats. Cybersecurity standards and frameworks are generally applicable to all organizations, regardless of their size, industry or sector.

3.5 Cybersecurity Risk Assessment

A Cybersecurity Risk Assessment is a strategic tool that aligns a company’s priorities and budgets within the organization’s high-level threat landscape. It is often confused with other tools like cybersecurity audits, vulnerability assessments, and penetration tests. Each tool is important, but they are not interchangeable.

Cyber risk assessments are defined by NIST as *risks assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.*

There are a number of reasons to perform a cyber risk assessment:

Reduction of long-term costs: identifying potential threats and vulnerabilities, then working on mitigating them has the potential to prevent or reduce security incidents which saves your organization money and/or reputational damage in the long-term

Provides a cyber security risk assessment template for future assessments: Cyber risk assessments aren't one of processes, you need to continually update them, doing a good first turn will ensure repeatable processes even with staff turnover

Better organizational knowledge: Knowing organizational vulnerabilities gives you a clear idea of where your organization needs to improve

Avoid data breaches: Data breaches can have a huge financial and reputational impact on any organization

Avoid regulatory issues: Customer data that is stolen because you failed to comply with HIPAA, PCI DSS or APRA CPS 234

Avoid application downtime: Internal or customer facing systems need to be available and functioning for staff and customers to do their jobs

Data loss: theft of trade secrets, code, or other key information assets could mean you lose business to competitors

Beyond that, cyber risk assessments are integral to information risk management and any organization's wider risk management strategy.

General steps of cyber risk assessments are:

Step 1: Determine information value

Step 2: Identify and prioritize assets

Step 3: Identify threats

Step 4: Identify vulnerabilities

Step 5: Analyze controls and implement new controls

Step 6: Calculate the likelihood and impact of various scenarios on a per-year basis

Step 7: Prioritize risks based on the cost of prevention vs information value

Step 8: Document results in risk assessment report

3.5.1 Data-Centric Risk Assessment

Most security technology focuses on where data is— protecting, for example, all the data stored on a specific laptop or server, or all the data that crosses a specific network. The problem with this approach is that as soon as data moves somewhere else, another solution is required, or data is left unprotected. Data-centric security, on the other hand, focuses on what needs to be protected—the files containing sensitive information—and applying the appropriate form of protection no matter where the data happens to be.

The defining characteristic of data-centric security is that protection is applied to data itself, independent of the data's location. To be effective, this must happen automatically—sensitive information should identified as soon as it enters an organization's IT ecosystem, and should be secured with policy-based protection that lasts throughout the data lifecycle. A typical implementation of data-centric security consists of software agents installed on every IT asset where sensitive data might be created or stored—laptops, desktops, servers, mainframes, mobile devices, and elsewhere. These agents are controlled by a centralized management console, where administrators define the appropriate form of protection for each data type and use case.

Each organization requires a unique solution—one tailored to fit the company's threat exposure and business needs. However, all successful implementations of data-centric security have certain characteristics in common: they're tightly controlled from a centralized management system, they provide coverage across the entire organization without security gaps, they rely on automation rather than manual intervention, and they're adaptable enough to grow and change along with the organization

3.5.2 Penetration Test

Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.

This is like a bank hiring someone to dress as a burglar and try to break into their building and gain access to the vault. If the 'burglar' succeeds and gets into the bank or the vault, the bank will gain valuable information on how they need to tighten their security measures.

3.5.3 Assets Inventory

Cyber Security Asset Inventory identifies cyber assets and captures updated inventory information on ports, services and software connected to the control networks. The solution enables users to make better operational, compliance and risk decisions related to cyber security controls, asset lifecycle and asset management.

3.5.4Threat Intelligence

Cybersecurity threat intelligence is **important for anyone who stores sensitive information** on a connected device—which pretty much includes everyone. Even if you already have firewalls and other security measures in place, staying up-to-date on the nature of threats is critical for securing your systems. **Large enterprises are especially vulnerable to cybersecurity threats** because they're so spread out, meaning the IT team may not know one of their departments has been hit until it's too late. The varied nature of cyberattacks today makes cybersecurity threat intelligence and awareness essential.

3.6 Security Architecture

3.6.1 Security Engineering

Security engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves. Security engineering requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law. System engineering skills, from business process analysis through software engineering to evaluation and testing, are also important; but they are not sufficient, as they deal only with error and mischance rather than malice.

Security engineering is the field of engineering dealing with the security and integrity of real-world systems.

3.6.2 Access Control

Access control is used to identify an individual who does a specific job, authenticate them, and then proceed to give that individual only the key to the door or workstation that they need access to and nothing more. Access control systems come in three variations: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).

3.6.3 Identity Management

Identity management (ID management) is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities. The managed identities can also refer to software processes that need access to organizational systems.

3.6.4 Cloud Security

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Cloud security is a form of cybersecurity.

3.6.5 Data Protection

Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Data protection is also known as data privacy or information privacy.

3.6.6 Secure Application Development

Application security is the process of making apps more secure by finding, fixing, and enhancing the security of apps. Much of this happens during the development phase, but it includes tools and methods to protect apps once they are deployed. This is becoming more important as hackers increasingly target applications with their attacks.

3.6.7 Cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Modern cryptography concerns with:

Confidentiality - Information cannot be understood by anyone

Integrity - Information cannot be altered.

Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage

Authentication - Sender and receiver can confirm each

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

3.7 Security Operation

3.7.1 Active Defense

Active defense is the fusion of timely threat intelligence with proactive measures that combat specific threat scenarios to yield a progressive reduction in enterprise risk. To attackers, the effect is a continuously increasing level of effort required to succeed in an attack against an enterprise that uses an active defense.

Active defense does not replace traditional security operations. Instead, active defense comprises a toolkit of tactics to be deployed by high functioning security operations teams after they have mastered basic security operations functions. Deploying the tactics described herein requires a functioning security operations center (SOC), a basic vulnerability management program, and a moderate level of data and asset classification. Practitioners will also need leadership buy-in, since active defense tactics can be disruptive or even invasive in some instances.

3.7.2 Data Leakage

A data leak is when sensitive data is accidentally exposed physically, on the Internet or any other form including lost hard drives or laptops. This means a cyber criminal can gain unauthorized access to the sensitive data without effort.

While the terms data breach and data leak are often used interchangeably, they are two separate data exposure types:

- A data breach is when a successful attack is able to secure sensitive information.
- A data leak does not require a cyber attack and generally stems from poor data security practices or accidental action or inaction by an individual.

3.7.3 Incident Response

Incident response (IR) is the systematic approach taken by an organization to prepare for, detect, contain, and recover from a suspected cybersecurity breach. An incident response plan helps ensure an orderly, effective response to cybersecurity incidents, which in turn can help protect an organization’s data, reputation, and revenue. So, incident response is the methodology an organization uses to respond to and manage a cyberattack. An attack or data breach can wreak havoc potentially affecting customers, intellectual property company time and resources, and brand value. An incident response aims to reduce this damage and recover as quickly as possible. Investigation is also a key component in order to learn from the attack and better prepare for the future. Because many companies today experience a breach at some point in time, a well-developed and repeatable incident response plan is the best way to protect your company.

An incident response plan helps ensure the proper steps are taken. It often includes the following elements:

- how incident response supports the organization’s broader mission
- the organization’s approach to incident response
- activities required in each phase of incident response
- roles and responsibilities for completing IR activities
- communication pathways between the incident response team and the rest of the organization
- metrics to capture the effectiveness of its IR capabilities

According to the National Institute of Standards and Technology (NIST), there are four key phases to IR:

- *Preparation*
- *Detection and analysis*
- *Containment and eradication*
- *Post-incident recovery*

3.7.4 Vulnerability Data Management

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their "attack surface."

3.7.5 Security Operation Center

A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery.

Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

3.7.6 Security Information and Event Management

Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security.

SIEM tools provide:

- Real-time visibility across an organization's information security systems.
- Event log management that consolidates data from numerous sources.
- A correlation of events gathered from different logs or security sources, using if-then rules that add intelligence to raw data.
- Automatic security event notifications. Most SIEM systems provide dashboards for security issues and other methods of direct notification.

SIEM works by combining two technologies: a) Security information management (SIM), which collects data from log files for analysis and reports on security threats and events, and b) security event management (SEM), which conducts real-time system monitoring, notifies network admins about important issues and establishes correlations between security events.

3.7.7 Prevention

Information security professionals must continuously mature their capabilities by working smarter not harder. It is always better to prevent, then to pursue and prosecute. Preventing an incident requires careful analysis and planning. Information is an asset that requires protection commensurate with its value. Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional. During the prevention phase, security policies, controls and processes should be designed and implemented. Security policies, security awareness programs and access control procedures, are all interrelated and should be developed early on. The information security policy is the cornerstone from which all else is built.

3.7.8 Detection

Detection of a system compromise is extremely critical. With the everincreasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. There is no full proof “silver bullet” security solution. A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm. The most important element of this strategy is timely detection and notification of a compromise. Intrusion detection systems (IDS) are utilized for this purpose. IDS have the capability of monitoring system activity and notifies responsible persons when activities warrant investigation. The systems can detect attack signatures and also changes in files, configurations and activity. To be protected, the entire system should be monitored. Intrusion detection tools should be strategically placed at the network and application levels. However, monitoring a busy network or host is not a simple task. Intrusion detection tools must have the ability to distinguish normal system activity from malicious activity. This is more of an art than a science. The IDS must be fine-tuned or ‘tweaked” in order for the IDS to work in accord with a particular network or host. This tuning process must take into account known threats, as well as intruder types, methods and processes.

3.7.9 Response

For the detection process to have any value there must be a timely response. The response to an incident should be planned well in advance. Making important decisions or developing policy while under attack is a recipe for disaster. Many organizations spend a tremendous amount of money and time preparing for disasters such as tornados, earthquakes, fires and floods. The fact is, the chances are greater that a computer security incident will occur than any one of these scenarios. Equivalent if not more effort and resources should be expanded on a computer security incident response plan. The response plan should be written and ratified by appropriate levels of management. It should clearly prioritize different types of events and require a level of notification and/or response suitable for the level of event/threat. A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified. These roles should be assigned to competent members of the organization. A team leader/manager should be appointed and assigned the responsibility of declaring an incident, coordinating the activities of the CSIRT, and communicating status reports to upper management.

3.7.10 Recovery

Recovery is steps to return to normal operations and limit damage to the organization and its stakeholders continue after the incident or crisis. Post-event steps include assessments of the causes and of the management of the incident or crisis, and promulgation of lessons learned. Effective crisis management extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. From the standpoint of cybersecurity—the main deterrent to cyber incidents—the goal is to develop a secure, vigilant, and resilient organization.

3.8 Physical Security

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

As cybersecurity and physical security converge, organizations should consider the next steps to develop a more comprehensive security strategy. By thinking of cyber-physical security in a unified way, teams can invest in advanced digital technology that makes their network and facilities safer while simultaneously accounting for the vulnerabilities of increasingly connected physical assets. This means that organizations will need to consider necessary changes to bring cybersecurity and physical security planning together. Moving forward, it’s going to be essential that facilities staff and IT professionals collaborate if organizations are going to successfully counter physical cybersecurity threats. Ultimately, key decision-makers will need to work with stakeholders across cybersecurity and physical security teams to determine the best path forward. While the exact makeup of these arrangements will differ from one organization to the next, security professionals will need to work together to prevent cybercriminals from breaching their networks and inflicting damage on their physical infrastructure.

3.9 Security and Resilience Assurance of Industrial Automation and Control Systems

3.9.1 Security Concept of Industrial Control Systems

Result of many standards considering allows representing existing security requirements to Industrial Control Systems (ICS) related with a restricted set of categories (see Fig. 3.1).

This conceptual security requirements taxonomy includes four the main parts:

– Risk management and assessment as a corner stone for definition of acceptable risks levels and countermeasures for risks reduction;

– Categories of security features implementation which include triad “People – Process – Technologies”;

– ICS context which drive to define requirement taking into account specifics of ICS; this concept includes three types of models (reference, physical architecture and zone models) as well as functionality, components, assets and other definitions, and security and safety coordination issues;

– ICS security levels (concept which grades risk levels for ICS separated parts and establishes different life cycle processes and countermeasures for different security levels.

The following sections use statements of ISA/IEC 62443 “Security for Industrial Automation and Control Systems” and NIST SP 800-82.

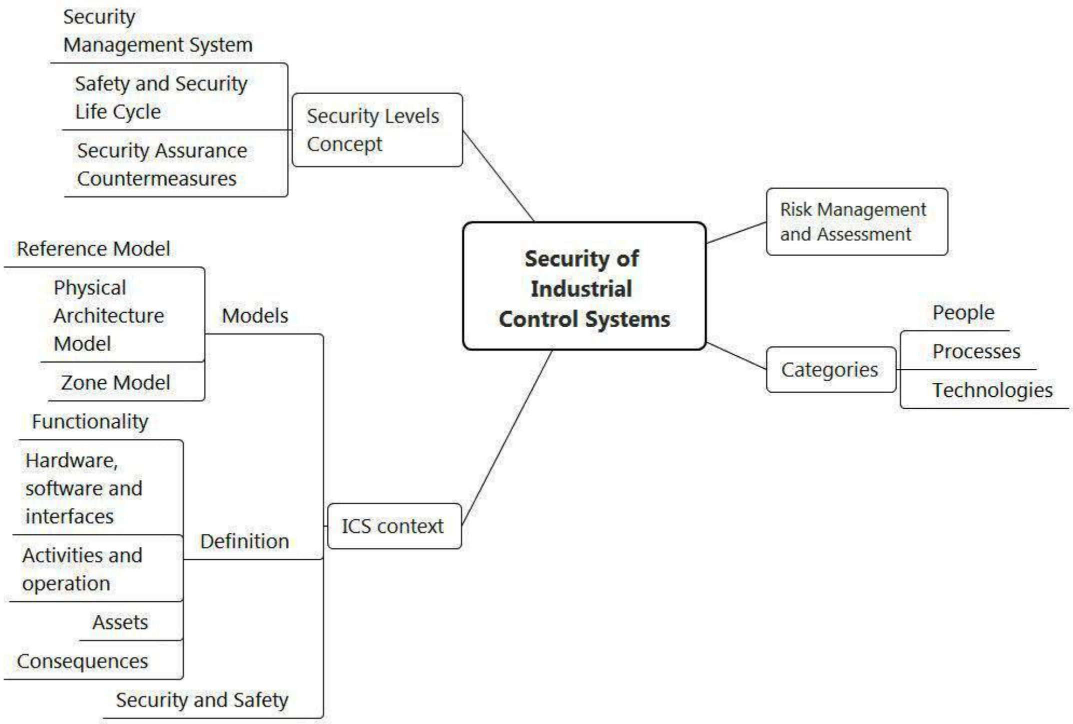

Security Management System
Safety and Security Life Cycle
Security Assurance Countermeasures
Security Levels Concept
Risk Management and Assessment
Security of Industrial Control Systems
Reference Model
Physical Architecture Model
Zone Model
Models
People
Processes
Technologies
Categories
Functionality
Hardware, software and interfaces
Activities and operation
Assets
Consequences
Definition
ICS context
Security and Safety

Figure 3.1 – Security concepts and requirements taxonomy

3.9.2 Industrial Automation and Control Systems Models and Definitions

The basis for identifying the security needs and important characteristics of the environment at a level of details necessary to address security issues can be expressed with three models (see Fig. 3.1), each of which is described below.

A reference model establishes a frame of reference for the more detailed information that follows. It describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels. The reference model used by the ISA/IEC 62443 series of standards appears in Fig. 3.2, including the following levels:

– Level 4 (Enterprise Business Systems): This level includes the functions involved in the business-related activities needed to manage a manufacturing organization. For the purposes of this standard, engineering systems are also considered to be in this level;

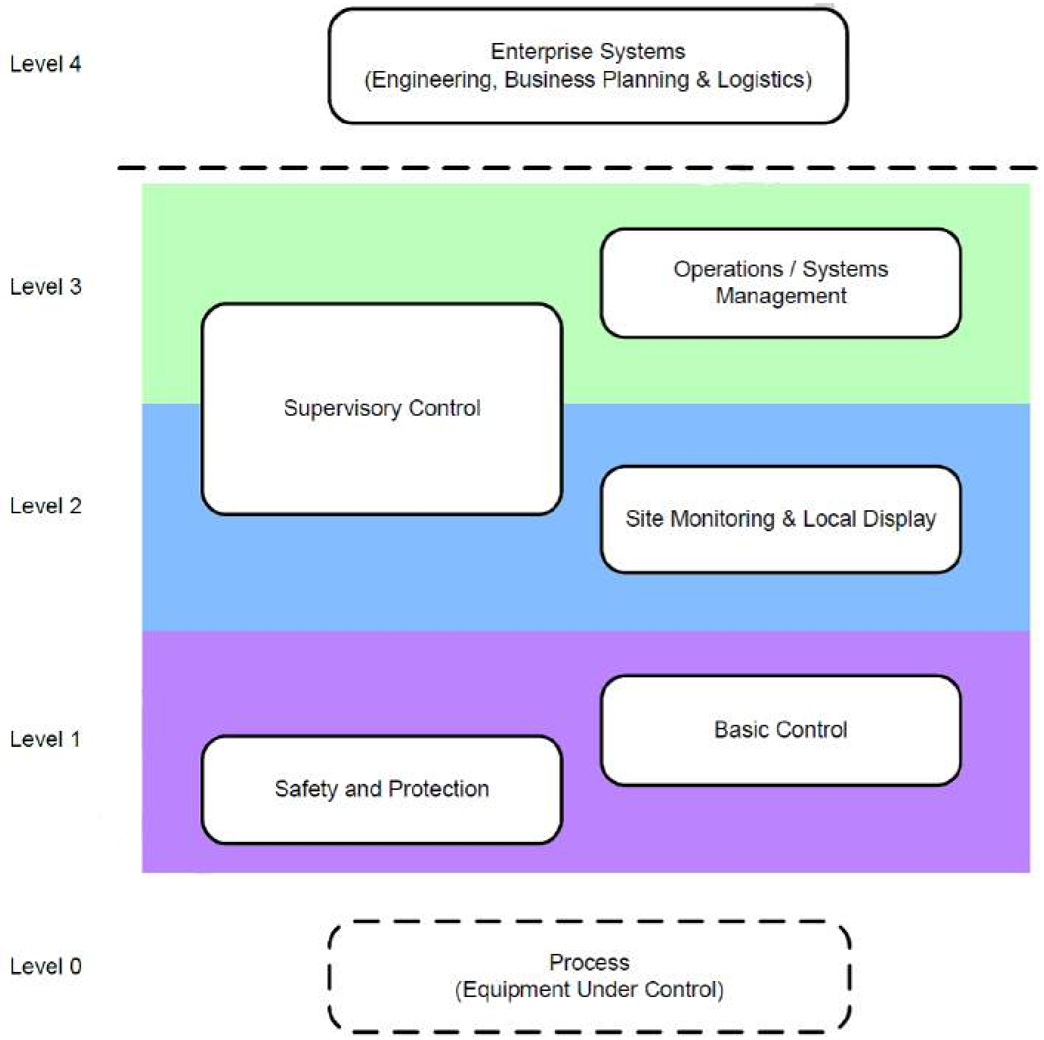

Level 4
Enterprise Systems
(Engineering, Business Planning & Logistics)
Level 3
Operations / Systems Management
Supervisory Control
Level 2
Site Monitoring & Local Display
Level 1
Basic Control
Safety and Protection
Level 0
Process
(Equipment Under Control)

Figure 3.2 – Reference model of Industrial Control Systems (source: ISA/IEC 62443)

– Level 3 (Operations Management): This level includes the functions involved in managing the work flows to produce the desired end products. Examples include dispatching production, detailed production scheduling, reliability assurance, and site-wide control optimization;

– Level 2 (Supervisory Control): This level includes the functions involved in monitoring and controlling the physical process. There are typically multiple production areas in a plant or facility;

– Level 1 (Local or Basic Control): This level includes the functions involved in sensing and manipulating the physical process. Process monitoring equipment reads data from sensors, executes algorithms if necessary, and maintains process history. It includes continuous control, sequence control, batch control, and discrete control. Equipment at this level includes, but is not limited to DCS and PLC. Also included in Level 1 are safety and protection systems that monitor the process and automatically return the process to a safe state if it exceeds safe limits. This category also includes systems that monitor the process and alert an operator of impending unsafe conditions. Safety and protection systems often have additional safety requirements that may not be consistent or relevant to cyber security requirements;

– Level 0 (Process): This level is the actual physical process, which includes a number of different types of production facilities in all sectors including, but not limited to, discrete parts manufacturing, hydrocarbon processing, product distribution, pharmaceuticals, pulp and paper, and electric power. It includes the sensors and actuators directly connected to the process and process equipment.

A physical architecture model is used to describe the various operational components and how they are connected. The details are specific to each individual system under consideration. It is common for an organization to have a single generic model that has been generalized to cover all operating facilities. An example of a simplified reference architecture model for a manufacturing function is shown in Fig. 3.3.

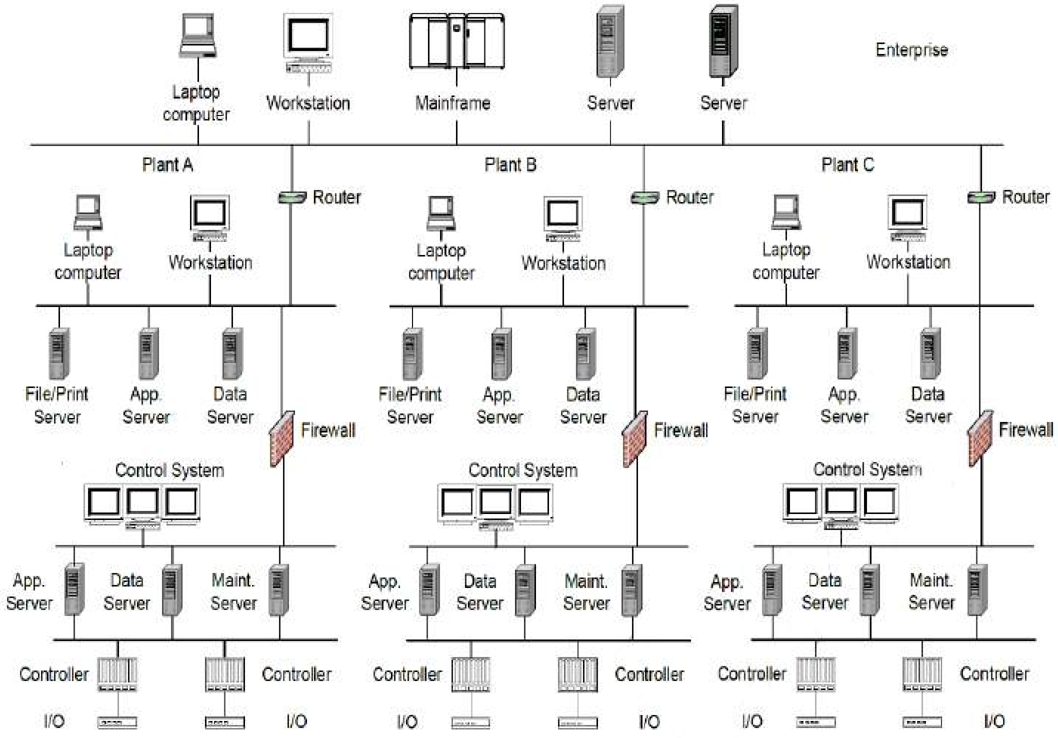


Figure 3.3 – Physical architecture model of Industrial Control Systems (source: ISA/IEC 62443)

A zone model is derived from the physical architecture model. The assets are grouped into entities (e.g., business, facility, site, or ICS) that are then analyzed for security policies and hence requirements. Fig. 3.4 is an example of a zone model. This model provides the context for assessing common threats, vulnerabilities, and the corresponding countermeasures needed to attain the level of security required to protect the grouped assets. After grouping assets in this manner, a security policy is defined for all assets that are members of the zone. The results of this analysis are used to determine the appropriate protection required based on the activities performed in the zone.

Every situation has a different acceptable level of security. For large or complex systems, it may not be practical or necessary to apply the same level of security to all components. Differences can be addressed by using the concept of a zone, defined as a logical or physical grouping of physical, informational, and application as sets sharing common security requirements. This concept can be applied in an exclusive manner where some systems are included in the security zone and all others are outside the zone. A conduit is a particular type of zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone.

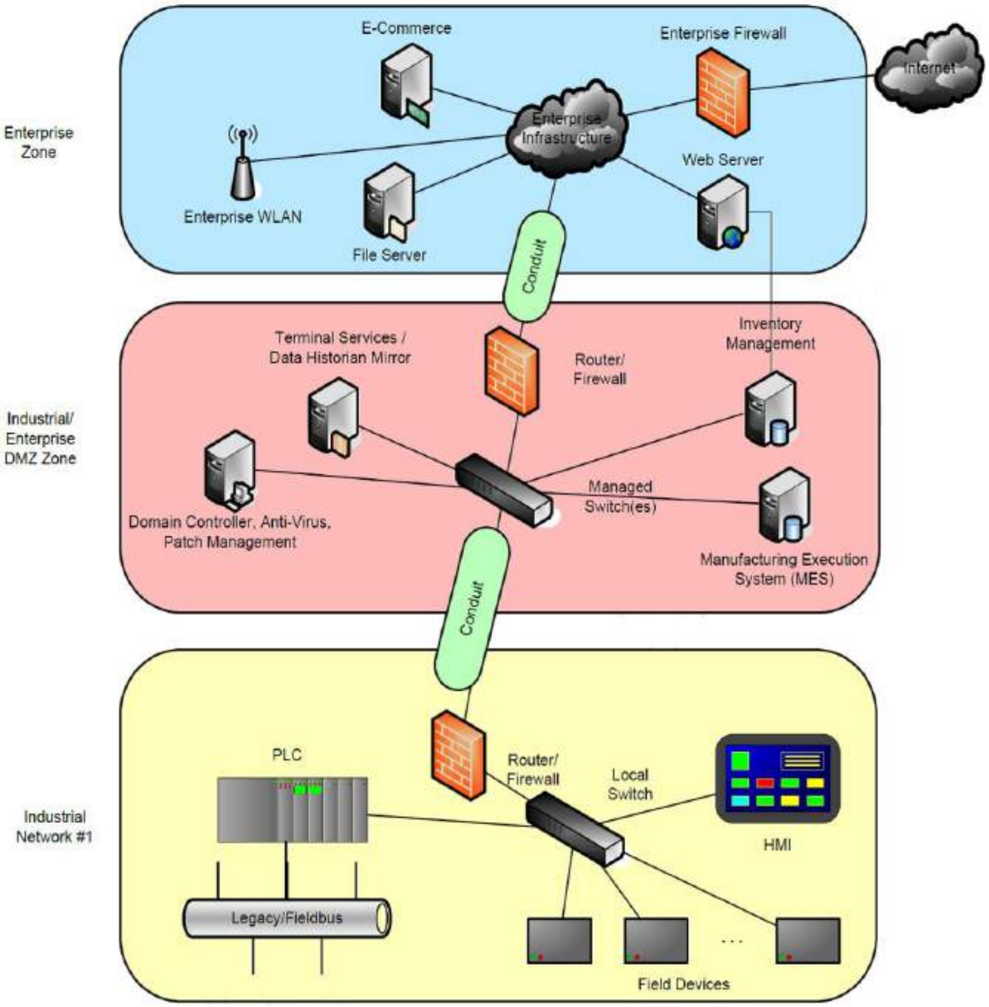


Figure 3.4 – Zone model of Industrial Control Systems (source: ISA/IEC 62443)

Channels are the specific communication links established within a communication conduit.

In order to fully articulate the systems and components, the range of coverage may be described from several perspectives, including (see Fig. 3.1):

– Range of functionality included;

– Systems and interfaces;
– Criteria for selecting included activities;
– Criteria for selecting included assets;
– Consequence based criteria.

The scope of ICS security can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

It is also possible to describe the ICS in terms of connectivity to associated systems and interconnectivity of hardware and software components. All issues that can affect or influence the safe, secure, and reliable operation of industrial processes should be covered.

Activities associated with manufacturing operations includes the following: predictable operation of the process, process or personnel safety, process reliability or availability, process efficiency, process operability, product quality, environmental protection, compliance with relevant regulations, and product sales or custody transfer affecting or influencing industrial processes.

ICS are usually related with assets for which security is essential to the protection. This range of coverage includes systems whose compromise could result in the endangerment of public or employee health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, environmental contamination, and/or economic loss or impact on an entity or on local or national security.

It shall be taken in account ICS compromise could result in any or all of the following situations: endangerment of public or employee safety, environmental protection, loss of public confidence, violation of regulatory requirements, loss of proprietary or confidential information, economic loss, impact on entity, local, state, or national security.

3.9.3 Industrial Automation and Control Systems Security Features

3.9.3.1 Industrial Automation and Control Systems Security: a Problem Statement

Typical Industrial Automation and Control Systems (IACS) includes supervisory control and data acquisition (SCADA) systems networked with distributed control systems (DCS). DCSs and other control systems are usually based on Programmable Logic Controllers (PLC).

ICSs are typically used in industries such as electric, water and wastewater, oil and gas, transportation, chemical, pharmaceutical, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, etc.) SCADA systems are generally used to control dispersed assets. DCS are generally used to control production systems within a local area such as a factory using control. The basic structure of an ICS with key components is shown in Figure 3.5.

The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller.

Operators and engineers use HMI to monitor operation and configure set points, control algorithms, and to adjust and establish parameters in the controller. The HMI also displays process status information and historical information. Diagnostics and maintenance utilities are used to prevent, identify, and recover from abnormal operation or failures.

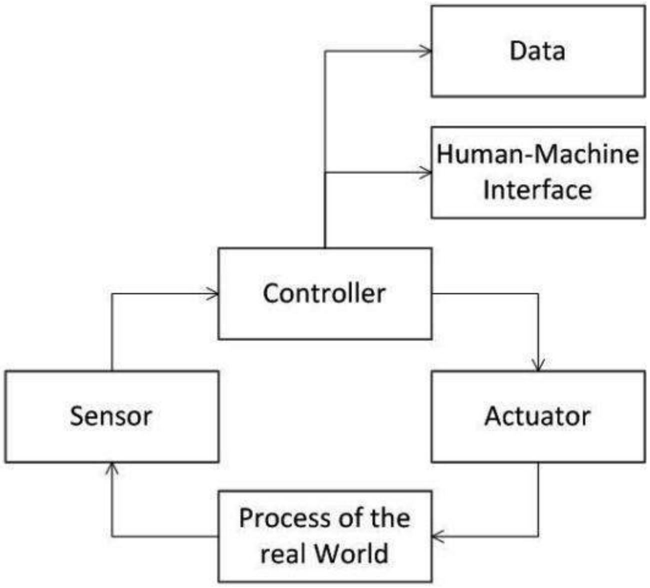


Figure 3.5 – Main components of Industrial Control Systems

While control systems used in manufacturing and distribution industries are very similar in operation, they are different in some aspects. Manufacturing industries are usually located within a plant-centric area of a factory or, when compared to geographically dispersed distribution industries. Communications in manufacturing industries are usually performed using local area network (LAN) technologies that are typically more reliable and high speed as compared to the long-distance communication wide area networks (WAN) used by distribution industries. The ICS used in distribution industries are designed to handle long-distance communication challenges such as delays and data loss posed by the various communication media used. The security controls may differ among network types.

Typical SCADA hardware (see Figure. 3.6) includes a control server placed as the Main Terminal Unit (MTU) at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites consisting of Remote Terminal Units (RTUs) and/or PLCs, which controls actuators and/or monitors sensors. The control server stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process.

The communications hardware allows the transfer of information and data back and forth between the control server and the RTUs or PLCs. An Intelligent Electronic Device (IED), such as a protective relay, may communicate directly to the control server, or a local RTU may poll the IEDs to collect the data and pass it to the control server. IEDs provide a direct interface to control and monitor equipment and sensors.

ICSs consist of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that operate together to achieve an industrial objective such as manufacturing and transportation. The control part of the system includes the specification of the desired outputs or performance. Control can be fully automated or may include a human in the loop. Systems can be configured to operate open-loop, closed-loop, and manual mode. In open-loop control systems the output is controlled by established settings. In closed-loop control systems, the output has an effect on the input in such a way as to maintain the desired objective. In manual mode the system is controlled completely by humans. A typical ICS may contain numerous control loops, Human Machine Interfaces (HMI), and remote diagnostics and maintenance tools built using an array of network protocols. Some critical processes may also include safety systems.

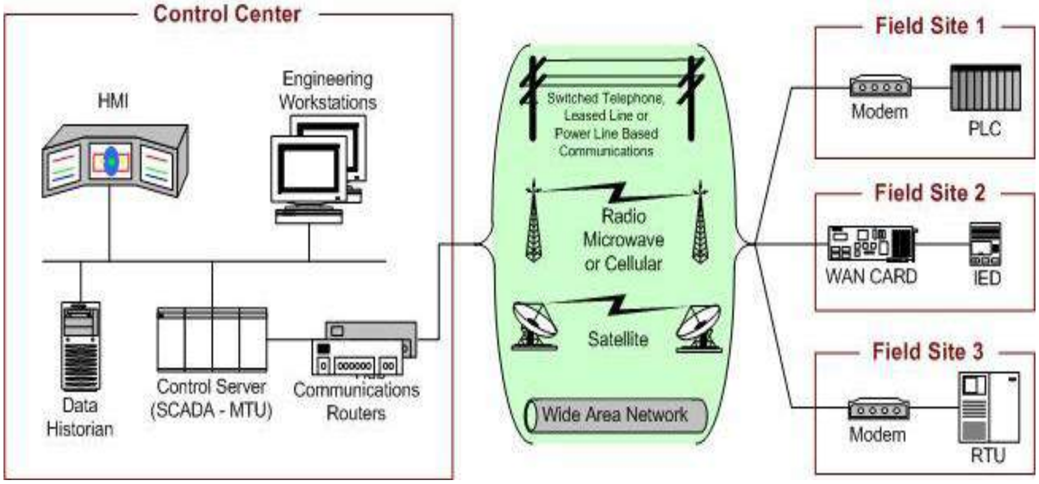


Figure 3.6 – SCADA System General Layout (source: NIST SP 800-82)

Figure 3.7 shows control of a manufacturing process being performed by a PLC over a fieldbus network. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all connected on a LAN.

The United States Department of Homeland Security takes into account the following sixteen critical infrastructure sectors, which, probably, are applicable for any of national infrastructure: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems.

ICSs have some specific features which make them different from other Information Technologies (IT) systems. ICS control the physical world and IT systems manage data. It raises many ICS characteristics, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, damage to the environment, and financial issues such as production losses, and negative impact to a nation’s economy. ICS have different performance, resilience, safety and reliability requirements, and also use operating systems and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyber-attack.

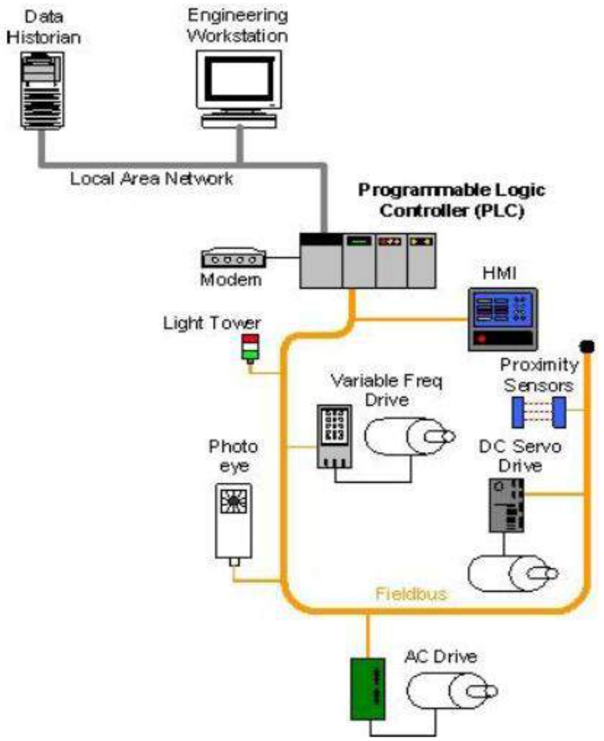


Figure 3.7 – Manufacturing process control performed by a PLC

Table 3.1 provides summary of IT system and ICS differences according to NIST SP 800-82 statements.

Table 3.1 – Summary of IT system and ICS differences

Category	**Information Technology System**	**Industrial Control System**
Performance Requirements	Non-real-time. Response must be consistent. High throughput is demanded. High delay and jitter may be acceptable. Less critical emergency interaction. Tightly restricted access control can be implemented to the degree necessary for security	Real-time. Response is time-critical. Modest throughput is acceptable. High delay and/or jitter is not acceptable. Response to human and other emergency interaction is critical. Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	Responses such as rebooting are acceptable. Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements. Availability requirements may necessitate redundant systems. Outages must be planned and scheduled days/weeks in advance. High availability requires exhaustive pre-deployment testing

Category	Information Technology System	Industrial Control System
Risk Management Requirements	Manage data. Data confidentiality and integrity is paramount. Fault tolerance is less important – momentary downtime is not a major risk. Major risk impact is delay of business operations	Control physical world. Human safety is paramount, followed by protection of the process. Fault tolerance is essential, even momentary downtime may not be acceptable. Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
System Operation	Systems are designed for use with typical operating systems. Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without built-in security capabilities. Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	Standard communications protocols. Primarily wired networks with some localized wireless capabilities. Typical IT networking practices	Many proprietary and standard communication protocols. Several types of communications media used to include dedicated wire and wireless (radio and satellite). Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use operating systems that are no longer supported
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Components Lifetime	Lifetime on the order of 3 to 5 years	Lifetime on the order of 10 to 15 years (for some domains, with opportunity up to 30 years of operation)
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

3.9.3.2 Industrial Automation and Control Systems Features

The first feature of industrial networks is their "openness". This is due to the convenience of configuration, maintenance, changing applications on network devices.

Many programmable logic controllers (PLCs) have the ability to use SD cards to store data and applications. Automatics manufacturers, beyond any doubt, make every effort to protect the network assets from unauthorized access.

The fact that there is a large number of industrial automation manufacturers raises the issue of vulnerabilities of the devices produced by them. How many specialists have passed through the manufacturers' developing centers, what are the former developers currently engaged in, which data have they had access to? Which part of the work do manufacturers trust to the third-party organizations; how many developers have left these ouward organizations? Do manufacturers consider signing non-disclosure agreements with outsourcers and employee as a sufficient condition to be sure in the confidentiality of information?

Many manufacturers of PLCs and robots use third-party real-time operating systems for their hardware. Do they have any control over the developers of these operating systems? Other manufacturers use third-party devices on the rights of rebranding. Is there an interaction between manufacturer and its subcontractors considering the staff turnover? It is clear that these questions are rhetorical, and relations between manufacturers and subcontractors are regulated by themselves and by the desire to reduce costs.

It is also obvious that in the conditions of formed economic relations there are no guarantees protecting from information leak.

The existance of backdoors in automation devices made by manufacturers for either themselves or by the request of special services, and the ability of access these devices by considerable number of specialists, even though it is limited, worth a separate notice. During the HatMan attack process the malefactor has gained the access to the controller with the help of the privileged user account, that was (possibly) used by manufacturer's technical support. It is clear that proprietary and commercially important information along with its carriers are "wandering" on the market.

Part of the enterprises, especially the process industry ones, use project departments or departments of partners, who are distributed control systems (DCS) manufacturers, to implement, maintain automation and visual control systems for changing technological processes. Consequently, third-party organizations with their employees and staff turnover have access to an industrial network infrastructure. The same applies to system integrators that introduce control systems and SCADA in production.

Most often machine-building equipment is used with built-in automation devices with private access in order to protect control algorithms that are considered to be an intellectual property. In addition to well-known problems with "opacity" of operation, diagnostics in the event of breakdowns, such kind of systems are served only by the manufacturer staff. Most often, one of the conditions of guarantees is a remote control of mechanics operation (vibration and temperature of bearings) from the manufacturer side. This leads to the "blind zones" in the network, access to which is limited for the automation control system experts.

Therefore, despite all security measures taken by the manufacturer security service, information security, automation control system specialist, the industrial network of the enterprise is not positively "covered from below". An example of the Stuxnet shows a successful attack on physically isolated from external networks facility.

Target cyberattacks, as shown by Hatman, from the side of compromised enterprise IT network are also quite possible, despite the use of specialists in the information security and extensive means of security like antiviruses, firewalls, SIEM event management tools, intrusion detection and prevention (IDS / IPS) systems, etc.

Separately there are wireless solutions. Without any doubt, such solutions significantly help to economize due to the absence of cable-conductor products. However, despite different data encryption measures, the issue remains open. In addition, many issues are caused by access to built-in web servers of industrial devices (for example, to frequency converters) by built-in Wi-Fi communication module.

All these circumstances cheerlessly define the picture of the automation control system network security.

A large number of different devices, most often from the different manufacturers, various communication protocols integrated into a single system with a huge number of entry points for potential vulnerabilities, "blind zones", heterogeneity of devices types and their manufacturers make an industrial network potentially dangerous. All this requires the most up-to-date approaches and means of control of vulnerabilities.

3.9.3.3 Industrial Automation and Control Systems Threats and Vulnerabilities

A threat is any circumstance or event with the potential to adversely impact organization operations, assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [3].

Threats have some intent or method that may exploit of vulnerability through either intentional or unintentional means, this intent or method referred to as the threat source.

A vulnerability is a weakness in an information system (including an ICS), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

A threat event is an event or situation that has the potential for causing undesirable consequences or impact. When a threat event occurs it becomes an incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Threats to ICS can come from numerous sources, which can be classified as the following:

- Adversarial treats are caused by individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies);
- Accidental threats are caused by erroneous actions taken by individuals in the course of executing their everyday responsibilities;
- Structural threats are caused by failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters;
- Environmental threats are caused by Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

It is necessary to create a risk management strategy for the ICS that protects the system against these possible threat sources. The threat source must be well understood in order to define and implement adequate protection.

Understanding the source of vulnerabilities and predisposing conditions can assist in determining optimal mitigation strategies. Predisposing conditions are properties of the organization, mission/business process, architecture, or information systems that contribute to the likelihood of a threat event. The groups of vulnerabilities may be the following:

- Policy and procedure vulnerabilities; can be considered, for example, such vulnerabilities, as absence of formal ICS security training and awareness program, inadequate incident detection and response plan, etc.;
- Architecture and design vulnerabilities; can be considered, for example, such vulnerabilities, as non-controlled traffic in security network, no security perimeter defined, etc.;
- Configuration and maintenance vulnerabilities; can be considered, for example, such vulnerabilities, as absence of patch maintenance, inadequate change control and testing of security changes, Denial of Service (DoS), absence of critical configuration backup, poor passwords management, inadequate access controls, inadequate malware protection, etc.;
- Physical vulnerabilities; can be considered, for example, such vulnerabilities, as lack of backup power, physical access of unauthorized personnel, unsecured physical ports, lack of defense against environmental and electromagnetic impacts, etc.;
- Software development vulnerabilities; can be considered, for example, such vulnerabilities, as improper data validation, inadequate authentication and access authorization, etc.;
- Communication and network vulnerabilities; can be considered, for example, such vulnerabilities, as improper firewalls and routers configuration, using of unsecure industry-wide ICS protocols, lack of integrity checking for communications, etc.

3.9.3.4 Industrial Automation and Control Systems Security Incidents

Possible security incidents for ICS may face include the following:

- Blocked or delayed information through ICS networks, which could disrupt ICS operation;
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life;
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects;
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects;
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment;

- Interference with the operation of safety systems, which could endanger human life.

The first described ICS related cyber security incident happened in 1982. Thomas Reed, senior US national security official, claims in his book "At the Abyss" that the United States allowed the USSR to steal pipeline control software from a Canadian company. This software included a Trojan Horse that caused a major explosion of the Trans-Siberian gas pipeline in June, 1982. The Trojan ran during a pressure test on the pipeline but doubled the usual pressure, causing the explosion. "In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds." The scheme to plant bugs in Soviet software was masterminded by Gus Weiss, who at the time was on the National Security Council and who died last year. Soviet agents had been so keen to acquire US technology, that they didn't question its provenance. Russian newspaper sources deny the report, saying an explosion did take place, but it was caused by poor construction, not by planted software. "What the Americans have written is rubbish," said Vasily Pchelintsev, who in 1982 headed the KGB office in the Tyumen region, the likely site of the explosion described in the book." The software sabotage had two effects, explains Reed. The first was economic. By creating an explosion with the power of a three kiloton nuclear weapon, the US disrupted supplies of gas and consequential foreign currency earnings. But the project also had important psychological advantages in the battle between the two superpowers. "By implication, every cell of the Soviet leviathan might be infected," Reed writes. "They had no way of knowing which equipment was sound, which was bogus. All was suspect, which was the intended endgame for the entire operation.

At the same time, many researcher conclude, that the above situation could not happen (http://ogas.kiev.ua/perspective/vzryv-kotorogo-ne-bylo-581). Firstly, gas transportation system in the USSR was not been equipped with digital control. Secondly, gas pressure increasing was handled by diverse protection system. Thirdly, the described explosion with the power of a three kiloton is physically impossible in the described conditions.

Any case, this incident is considered in many data bases as the first documented cyber weapon.

NIST SP 800-82 describes the following notorious incidents related with ICSs.

Bellingham, Washington Gasoline Pipeline Failure. In June 1999, 900 000 liters (237 000 gallons) of gasoline leaked from a 16 in. (40.64 cm) pipeline and ignited 1.5 hours later causing 3 deaths, 8 injuries, and extensive property damage. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. "Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation." A key recommendation from the NTSB report issued October 2002 was to utilize an off-line development and testing system for implementing and testing changes to the SCADA database.

Maroochy Shire Sewage Spill. In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264 000 gallons of raw sewage into nearby rivers and parks.

CSX Train Signaling System. In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, ten Amtrak trains were affected in the morning. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were also delayed between four and six hours.

Northeast Power Blackout. In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. Additionally, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345 kV transmission lines in Northern Ohio tripped due to contact with trees. This eventually initiated cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. A total of 61 800 MW load was lost as 508 generating units at 265 power plants tripped.

Davis-Besse nuclear power plant. In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.

Zotob Worm. In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, stranding workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were knocked offline. While the worm affected primarily Windows 2000 systems, it also affected some early versions of Windows XP. Symptoms include the repeated shutdown and rebooting of a computer. Zotob and its variations caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.

Taum Sauk Water Storage Dam Failure. In December 2005, the Taum Sauk Water Storage Dam suffered a catastrophic failure releasing a billion gallons of water. The failure of the reservoir occurred as the reservoir was being filled to capacity or may have possibly been overtopped. The current working theory is that the reservoir's berm was overtopped when the routine nightly pump-back operation failed to cease when the reservoir was filled. According to the utility, the gauges at the dam read differently than the gauges at the Osage plant at the Lake of the Ozarks, which monitors and operates the Taum Sauk plant remotely. The stations are linked together using a network of microwave towers, and there are no operators on-site at Taum Sauk.

Browns Ferry-3 PLC Failure. In August 2006, Tennessee Valley Authority was forced to manually shut down one of their plant's two reactors after unresponsive PLCs problems caused two water pumps to fail and threatened the stability of the plant itself. Although there were dual redundant PLCs, they were connected to the same Ethernet network. Later testing on the failed devices discovered that they would crash when they encountered excessive network traffic.

Stuxnet Worm. Stuxnet was a Microsoft Windows computer worm discovered in 2010 that specifically targeted industrial software and equipment. The worm initially spread indiscriminately, but included a highly specialized malware payload that was designed to target only specific SCADA systems that were configured to control and monitor specific industrial processes. Once the machine is infected, Stuxnet looks to see if the computer is running Siemens' Simatic WinCC or PCS 7 software. The malware then automatically uses a default password that is hard-coded into the software to access the control system's Microsoft SQL database. The password has been available on the Internet for several years. An estimated 10,000 machines, mostly in US, Iran, Iraq and Indonesia, reported infections within the first week. Iranian sources confirmed that the Stuxnet malworm shut down uranium enrichment at Natanz for a week from November 16 to 22, 2010. The centrifuge spinning speed was fluctuating without the monitors detecting any malfunction. The International Atomic Energy Agency (IAEA) director, Yukiya Amano, reported the shutdown to the IAEA board in Vienna on Tuesday, November 23, 2010.

Brute Force Attacks on Internet-Facing Control Systems. On February 22, 2013 ICS-CERT received a report from a gas compressor station owner about an increase in brute force attempts to access their process control network. The forensic evidence contained 10 separate IPs and additional calls of a similar nature from additional natural gas pipeline asset owners, which yielded 39 additional IPs of concern. Log analysis showed a date range from January 16, 2013 but there have been no reports since March 8, 2013.

German Steel Mill Attack. In 2014, hackers manipulated and disrupted control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive" – though unspecified – damage.

Blackout in Ukrainian power system. Hackers have used highly destructive malware and infected, at least, three regional power authorities, causing blackouts across the Ivano-Frankivsk region of Ukraine on December 23, 2015. Power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers. While power has been restored, all the impacted Oblenergos continue to run under constrained operations. Over the past year, the group behind BlackEnergy has slowly ramped up its destructive abilities. The KillDisk malware that hits the Ukrainian power companies contained similar functions but was programmed to delete a much narrower set of data. KillDisk had also been updated to sabotage two computer processes, including a remote management platform associated with the ELTIMA Serial to Ethernet Connectors used in industrial control systems.

The USA Industrial Control Systems Cyber Emergency Response Team of National Cybersecurity and Communications Integration Center (NCCIC/ICS-CERT) periodically issues annual reports which provide information concerning ICS vulnerabilities and cyber incidents around the USA. ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships. ICS-CERT has been involved in investigation BlackEnergy Malware, which caused power outage in Ukraine at December 23, 2015.

In 2015, ICS-CERT responded to 295 cyber incidents. This represented a 20 percent increase over FY 2014. The Critical Manufacturing Sector nearly doubled to a record 97 incidents, becoming the leading sector for ICS-CERT in FY 2015.The Energy Sector had the second most incidents with46 incidents, and the Water and Wastewater Systems Sector was third with 25.

In 2015, the ICS-CERT vulnerability coordination team handled 486 vulnerabilities. ICS-CERT reduced the average number of days to close a ticket from 108 days in 2014 to 55 days in 2015 and closed 76 percent of tickets that had been open over 365 days.

Many relevant records cncening security incidens, vulnerabilities and other issues can be founded in the following online resources:

– Repository of Industrial Security Incidents (RISI) at the link http://www.risidata.com/;

– U.S. National Vulnerability Database supported by NIST at the link https://nvd.nist.gov/;

– Alerts of the U.S. Computer Emergency Readeness Team (US-CERT) which provide timely information about current security issues, vulnerabilities, and exploits at the link https://www.us-cert.gov/ncas/alerts;

– Newly developed vulnerabilities search engine VULNERS, which integrated search results from many databases at the link https://vulners.com.

3.9.4 Information Technologies Security vs Industrial Automation and Control Systems Security

It is important to recognize and understand the differences between cybersecurity of IT systems and IACS cybersecurity. In Table 3.2, some of the most important factors that should be taken into account are highlighted.

Industrial security includes security / cyber security and safety. The IEC 62443 series is adopted as state standards in many countries. In Ukraine at the level of Ukrainian State Standard. only IEC 62443-4-2 Since September 2019 is used (Order SE "UkrNDNC" dated 13.08.2019 No. 249), admitting the part of the translation of IEC 62443-2-1 is in perspective. At the time of this white book issuance, the working versions of translation of parts IEC / TS 62443-1-1: 2009 and IEC 62443-2-1: 2010 are ready.

Current chapter 4 includes an overview of the standards of the ISA99 / IEC 62443 series and some other normative documents, the current state of addressing issues related to cybersecurity in Ukraine, main challenges and development directions in the introduction of a complex and comprehensive cybersecurity system of industrial structures based on ISA99 / IEC 62443 standard series.

Table 3.2 – IT security vs IACS security

Attribute	IT security	IACS security
Confidentiality (Privacy)	High	Low
Message integrity	Low – Middle	Very high
System availability	Low – Middle	Very high
Authentification	Middle - High	High
Non-repudiality (Proof of integrity and origin of data)	High	Low – Middle
Time	«Bearable» (days)	Critically high
System idle time	«Bearable»	Unaccepted
Security skills / Awareness	Ususally good	Usually bad
System lifecycle	3–5 years	15-25 years
Computing resources	«Almost unlimited»	Very limited with obsolete processors
Software changes	Often	Rare
The worst consequences	Frequent data losses	Equipment distraction

3.10 Industrial Automation and Control Systems Security Standards Analysis

Currently IEC 62443 standards consist of a number of refined and project documents. This document focuses on four of them. Figure 3.8 indicates the relationship between four standards IEC 62443. Organizations operating in industrial automation control systemst (IACS) must have a cyber security management system (CSMS) in accordance with IEC-62443-2-1. This standard describes the implementation, management and operation of the IACS based on ISO / IEC 27001 and ISO / IEC 27002. IEC 62443-3-2 establishes risk assessment requirements, which leads to identification of zones and conduit for IACS. On the basis of a detailed risk assessment for each area and conduit, it is possible to determine a sufficient target security level (SL-T) for each one. SL-T indicates the requirements and improvement of IEC 62443-3-3, which are to be evaluated to provide sufficient countermeasures. The IACS supplier must arrange an organization that can cope with technical requirements as well as with the organizational and operational requirements given in IEC 62443-2-4. In conjunction with the defined requirements in IEC 62443-3-3, the correct IACS with sufficient security can be delivered to the customer that is capable of maintaining its security level. It should be noted that parts 3-3 and 2-4 are partially overlapping.

Therefore, both 3-3, and 2-4 are used to determine the system security requirements at the stages of design and operation. The recommended practice is relevant to all industries that focus on engineering design (FEED), phase of production and operation of “Greenfield” and “Brownfield projects in the upper sector. Figure 3.9 shows the stages described in this recommended practice, that are related to the concept, Feed, the stages of design and operation. Part 5 and Part 6 features important requirements and practical recommendations on How to do it for designing and operation stages. It should be noted that these are recommendations, but not a complete list of measures.

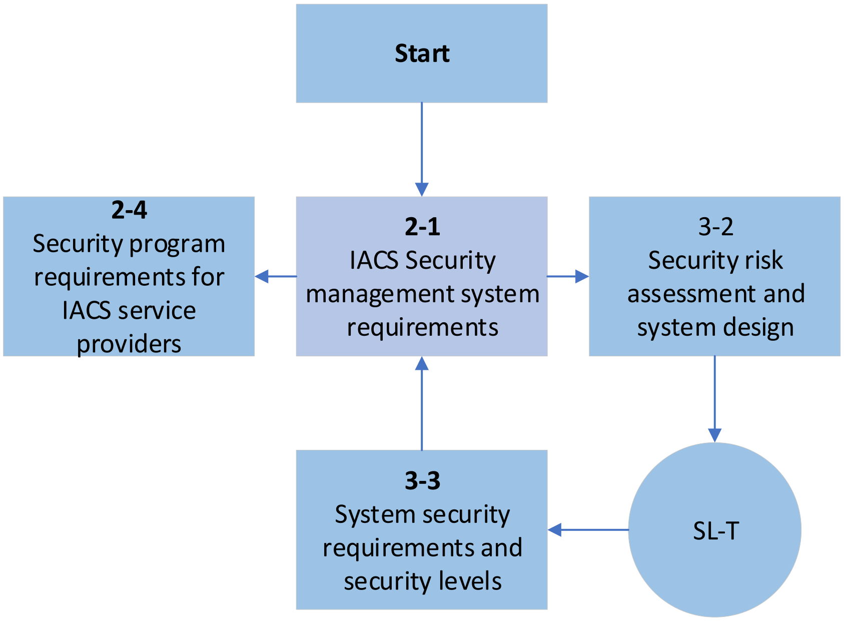

Start
2-4
Security program requirements for IACS service providers
2-1
IACS Security management system requirements
3-2
Security risk assessment and system design
SL-T
3-3
System security requirements and security levels

Figure 3.8 – Overview of IEC 62443 standards use

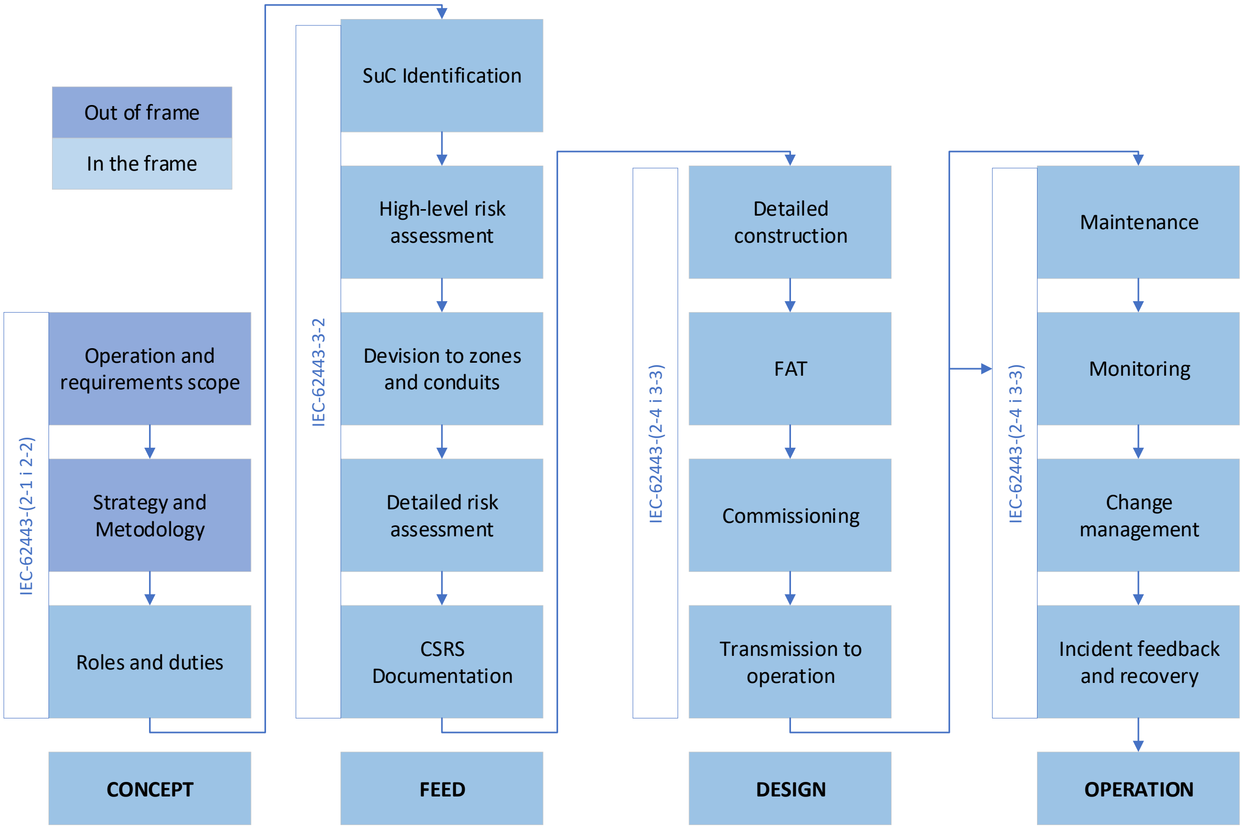


Figure 3.9 – IEC 62443 in Feed, Production and Operation

The target audience of this practice aims to include all elements (people, processes and technologies) involved in providing cybersecurity in the IACS (asset owner, system integrator, product supplier, service supplier, compliance authority).

This recommended practice explains the duties that are divided between these parties, and describes who performs the activities and to be involved, expected input and output data.

The assets owner (operator) must create a cybersecurity management system before launching the oil field project. CSMS requirements are defined in IEC 62443-2-1 and ISO 27001, and are not discussed in this recommended practice.

Cybersecurity is realized as a combination of technologies, processes and people. This recommended practice is focused on technology and processes. The concept of security level for grouping technical requirements is used throughout the document. The concept of maturity level, described in IEC-62443-2-4, groups processes and organizational requirements.

IEC62443 committees plan to release a new standard for protection levels (PL). The purpose is to determine the security control classes (SCC) and the creation of a comparison card with the requirements of IEC62443-2-1, IEC62443-2-4 and IEC62443-3-3. Technical implementation and configuration in IACS, as well as control method, support and deployment of IACS solutions will be displayed at the protection level (PL). The protection level is a methodology for assessing protection of facilities that function. The methodology includes the evaluation of technical capabilities and related processes in a combined assessment. PL combine the assessment of technical and organizational measures. The intention is to update this recommended practice after the disclosure of IEC standards definition for PL.

3.10.1 General Information on IEC 62443

IEC 62443, previously known as ISA 99, is a de facto world security standard for industrial control systems (ICS). The standard was created by the International Society of Automation (ISA) and was adopted by the International Electrotechnical Commission (IEC), which is currently responsible for its further development.

The IEC 62443 regulatory documents series were developed by the ISA99 and IEC Technical Committee 65 Working Group 10 (TC65WG10) to meet the needs of cybersecurity resilience in the industrial automation systems.

ISA99 / IEC 62443 refers to the security of industrial management systems, known as Industrial Automation and Control System. The purpose of this series of standards is to ensure that the product supplier, integrator and asset owner adhere an effective method of assured process with a key aspect of personnel and production security, availability, efficiency and quality of IACS products, as well as environmental safety.

The purpose of using the IEC 62443 series is to improve safety, availability, integrity and confidentiality components or systems used for industrial automation, including aspects of procurement.

The IEC 62443 seria is based on existing standards for information security of information technology of general use (eg ISO / IEC 27000), vary mainly in the following:

- some additional aspects of **safety, health and environment**, which have not been presented in ISO / IEC 27001 and ISO / IEC 27005);
- presence of some additional **terms and definitions.**

The main objective of the IEC 62443 series is to provide a flexible structure that facilitates the solution of current and future vulnerabilities in industrial automation systems and to apply the necessary remediation means in a systematic, protective way.

The IEC 62443 series aims to **expand corporate security** that adapt the requirements for business IT systems and combination of them with unique **availability** requirements needed in the industrial automation systms.

Focus of IEC 62443-2-1: 2010 is as follows:

- **Determines the elements needed to create cyber security management system, (CSMS)** for industrial automation systems, and provides instructions for their development.;
- **Provides a base in the form of policies and procedures** to create the final CSMS of organization;
- **covers personnel-related practices**;
- **emphasizes the need to reconcile the management of cybersecurity systems of industrial automation systems with the practice of cybersecurity management** of businnes systems and / or informational technologies.

3.10.2 Application of ISA99 / IEC 62443 in Industrial Automation and Control Systems

Currently, ISA99 / IEC 62443 covers aspects related to IACS for such domains:

- Production;
- Chemicals processing;
- Oil processing;
- Production of food and beverages;
- Energy;
- Pharmaceuticals;
- Water.

The following domains are considering ISA99 / IEC 62443 as a potential alternative to build systems:

- Automotive industry / Smart Mobility;
- Medical devices.

3.10.3 ISA99 / IEC 62443 Structure

The series of normative documents IEC 62443 contains 14 papers and is distributed to four levels (see Figure 3.10):

- General level.
- Management system (policies and procedures) level, industrial IT security.
- Industrial automation control systems (system requirements) level and built-in systems security.
- Component level.

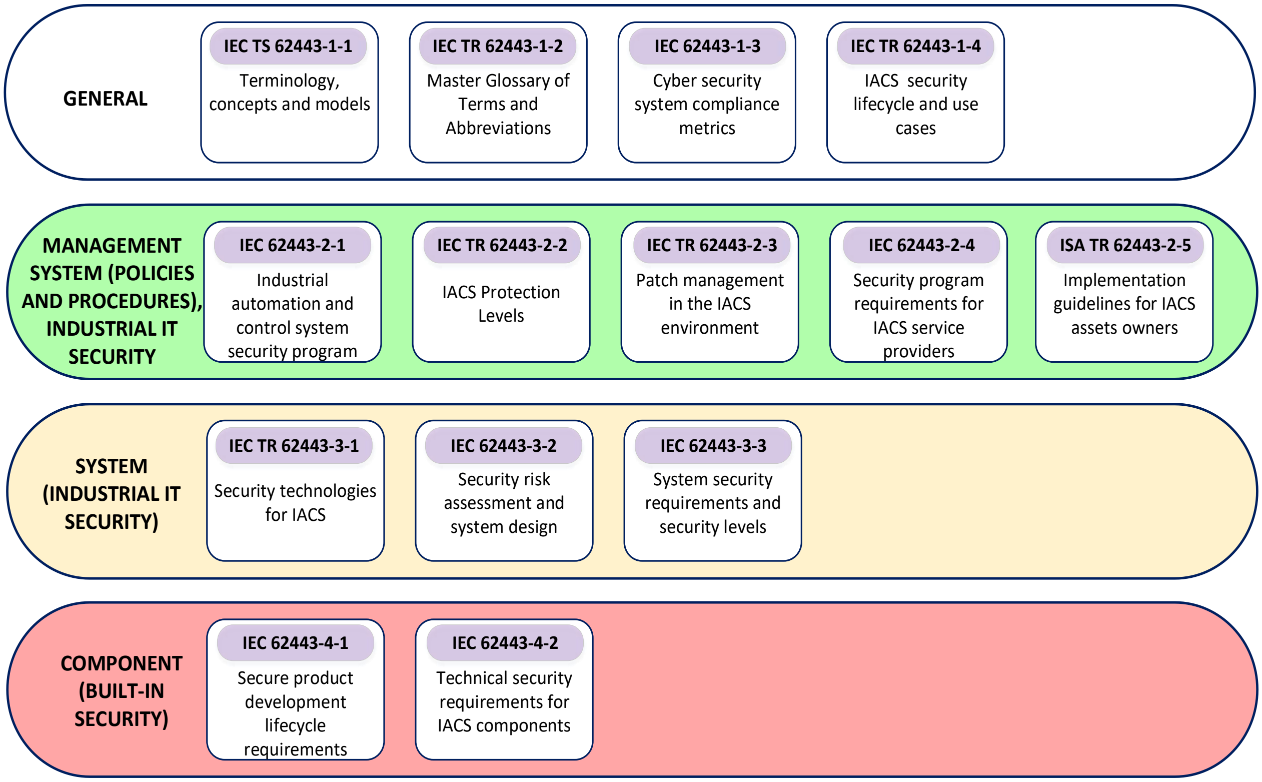

GENERAL
IEC TS 62443-1-1
Terminology, concepts and models
IEC TR 62443-1-2
Master Glossary of Terms and Abbreviations
IEC 62443-1-3
Cyber security system compliance metrics
IEC TR 62443-1-4
IACS security lifecycle and use cases
MANAGEMENT SYSTEM (POLICIES AND PROCEDURES), INDUSTRIAL IT SECURITY
IEC 62443-2-1
Industrial automation and control system security program
IEC TR 62443-2-2
IACS Protection Levels
IEC TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Security program requirements for IACS service providers
ISA TR 62443-2-5
Implementation guidelines for IACS assets owners
SYSTEM (INDUSTRIAL IT SECURITY)
IEC TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
COMPONENT (BUILT-IN SECURITY)
IEC 62443-4-1
Secure product development lifecycle requirements
IEC 62443-4-2
Technical security requirements for IACS components

Figure 3.10 – Structure of IEC 62443 Standards Series

Table 3.3 contains of names of all current regulatory documents of the 62443 series. Documents of various types (which have already been published and those that are in the development stage) are highlighted in different colors.

- Standard 62443-1-1 presents *general concepts* and models of the series.
  - The technical report 62443-1-2 contains glossary of terms and abbreviations that are used in the entire series.
  - Standard 62443-1-3 describes a series of metrics derived from the basic requirements (FR) and system requirements (SR).
- *Management system (IACS policies and procedures*): describes the necessary policies and procedures that are used to implement cybersecurity management system.
  - Standard 62443-2-1 describes what is required to determine and implement an effective IACS cybersecurity system. This standard is consistent with ISO 27000 Series.
  - Standard 62443-2 Provides specific guidelines concerninf the necessity of effective IACS cyber security system production.
  - Technical Report 62443-2-3 provides instructions on the patch management for IACS.
  - Standard 62443-2-4 determines IACS suppliers’ requirements.

Table 3.3 – Normative documents of the IEC 62443 series

Part	Status	Name
IEC TS 62443-1-1-2009	Technical specification	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
IEC TR 62443-1-2 *	Technical report	Security for industrial automation and control systems security – Part 1-1: Master Glossary of terms ans abbreviations
IEC TS 62443-1-3 *	International standard	Security for industrial automation and control systems – Part 1-3: Cyber security system compliance metrics
IEC TR 62443-1-4 *	Technical report	Security for industrial automation and control systems – Part 1-4: IACS security life cycle and use case
IEC 62443-2-1-2010	International standard	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
IEC TR 62443-2-2 *	Technical report	Security for industrial automation and control systems – Part 2-2: IACS protection levels
IEC TR 62443-2-3-2015	Technical report	Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment
IEC 62443-2-4-2015	International standard	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service suppliers
IEC TR 62443-2-5 *	Technical report	Security for industrial automation and control systems – Part 2-5: Implementation guidance for IACS asset owners
IEC TR 62443-3-1-2009	Technical report	Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems
IEC 62443-3-2 *	International standard	Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design
IEC 62443-3-3-2013	International standard	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
IEC 62443-4-1-2018	International standard	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements
IEC 62443-4-2-2019	International standard	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

**the documents have not been published yet*

- *Industrial IT security, (IACS system requirements)* describes cybersecurity requirements for the system in the IACS environment.
    - Technical report 62443-3-1 describes the use of various technologies for the IACS environment safety.

    - Standard 62443-3-2 relates to risk assessment and IACS sustem development.
    - Standard 62443-3-3 describes the basis of security requirements and security assurance Level (SL).
- *Built-in security (IACS component requirements):* describes the requirement of the component's cybersecurity in the IACS environment.
    - Standard 62443-4-1 describes the requirements related to the product development.
    - Standard 62443-4-2 contains requirements that allow to display system requirements (SR) on subsystems and system's components belonging to the specified scope of application in details.

Establishing the requirements for cybersecurity with the above standards for a specific case of automation at the enterprise are not a trivial task. Again, the starting point in industrial systems of automation and management should be the requirements for system's safety and the continuity of working on cybersecurity measures. In case of following the necessary requirements for safety and ensuring operation continuity, cyber security requirements can be analyzed using the installation environment, use cases and threats landscape as a basis for understanding threats to cybersecurity.

3.10.4 Defence in Depth

Defense-In Depth is a layered security mechanism that enhances the security of the entire system. The advantage of this mechanism is that during an attack, if one level suffers, other levels can still provide assistance in protecting, identifying and responding to attack. Levels (see Figure 3.11) can be described as follows:

- *Data layer* is the most internal layer. It can be used for access control list and data encryption.
- *Application layer* is the next layer used to install antivirus software and enhancing applications.
- *Host layer* is the next layer after the application layer, it is used to implement a vulnerability patch and to authenticate users.
- *Internal Network layer* is the next layer and is used for IPSec (Internet Protocol Security) for IP-communications, authentication and encryption of the package involved in the communication system, as well as for the intrusion detection system (IDS), which detects the invasion of each user (authorized or unauthorized).
- *Perimeter* layer is the next layer used to implement firewalls and VPN isolation;
- *Physical layer* is the next layer after the perimeter one where the switches, locks, ports, physical access, etc. are used.
- *Policies, Procedures layer* is the most external and the last level, where security policies and procedures for IACS networks are defined.

3.10.5 Security Zones and Conduits

Security zones are physical or logical assets that have phisical or logical assets joints, which have common security requirements and they separate the control systems critical components. A special type of security zone is a demilitarized zone (DMZ), which segment the external network with the internal IACS network using security components, such as a firewall. This concept involves a multilayer approach to security, taking into account defense-in-depth.

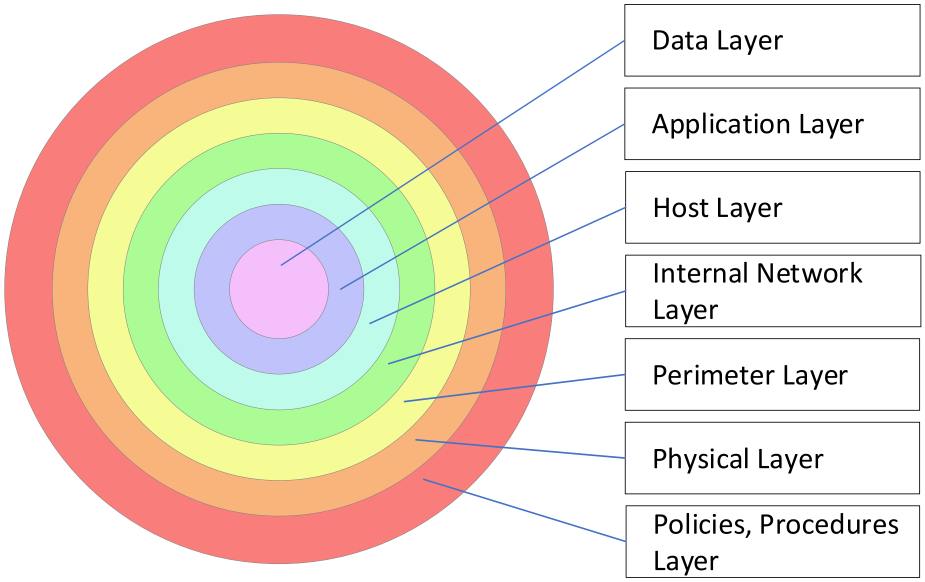


Figure 3.11 – Defence-in-depth layers

Conduit is a special type of security zone that group data that can be logically combined into information stream groups inside and out of the zone. The conduit can be a single service (for example, an Ethernet network), or several data carriers. The conduit controls access to the zone by confronting several attacks, such as Denial of Service, Malware attacks and protects the integrity and confidentiality of network traffic.

Figure 3.12 shows an organization (enterprise), which has three plants with a separate corporate headquarters. The plants A, B and C are connected to a global network of enterprise to provide communication with headquarters and other plants. The figure identifies the following four possible conduits (others should also be defined, but they are missed for brevity):

- The first is the conduit of the entire enterprise shown in the upper part of the figure (indicated in red). It is connecting a few plants in different locations to a corporate data center.
- If the global network of an enterprise is built using leased or private communications, it can be considered as a reliable conduit. If it uses both public and private networks, it should be attributed to the class of unreliable. All communication equipment and firewalls that form a plant communication system included in the relevant conduits of plant A, B and C (marked as purple color).
- Three copies of the second class conduits are located within each plant and are reflected in the figure. Each plant has its own reliable conduit that allows to control the connection.

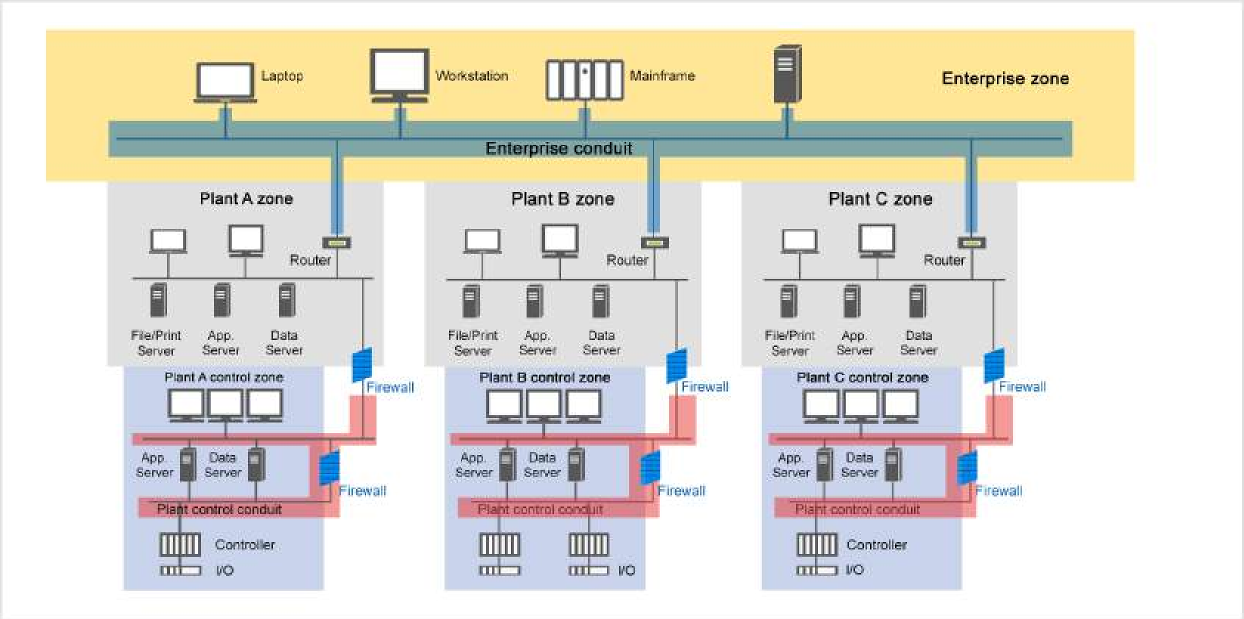


Figure 3.12 – Enterprise conduit example

3.10.6 Industrial Automation and Control Systems Cybersecurity Lifecycle

Cybersecurity lifecycle for IACS using the PCDA cycle (Plan, DO, Check and Act). This is a method of safety measures that are followed by the series of ISO 27000 standards. In IEC 62443 PDCA lifecycle is based on the main roles specified by the standard, that is: product developer, system integrator and asset owner.

Figure 3.13 depicts a PDCA cycle that can be implemented in an industrial automation control system with the reference to IEC 62443. Each of the three roles identified in the standard (that is, *product supplier, a system integrator and the owner of assets*), must match the PDCA cycle. The PDCA cycle for *product supplier* is a product lifecycle cycle, since it is specific for the product, or devices; as for the *integrator* and *asset owner* it is the lifecycle of the plant (production), since he concentrates on the whole plant.

Figure 3.14 shows the lifecycle process and the interaction of products and plant in the form of product development by the *supplier or manufacturer*, integration or commissioning by *system integrator* and operating and maintaining by *asset owner*. This is a continuous process and it is performed by a PDCA cycle.

3.10.7 Security levels based on IEC 62443 3-3 and IEC 62443 4-2

The concept of security level (SL) focuses on the IACS zones. It is believed that the security levels are adopted from previously proposed levels of safety, which are successfully used in industrial automation control systems, namely, with security integrity level (SIL).

The SL security level provides a landmark to make decisions on the use of countermeasures and devices with various security capabilities. The concept can be used to select the IACS industrial automation devices and countermeasures that will be used in the zone, it also provides the opportunity to classify the risks for a particular zone or conduit.

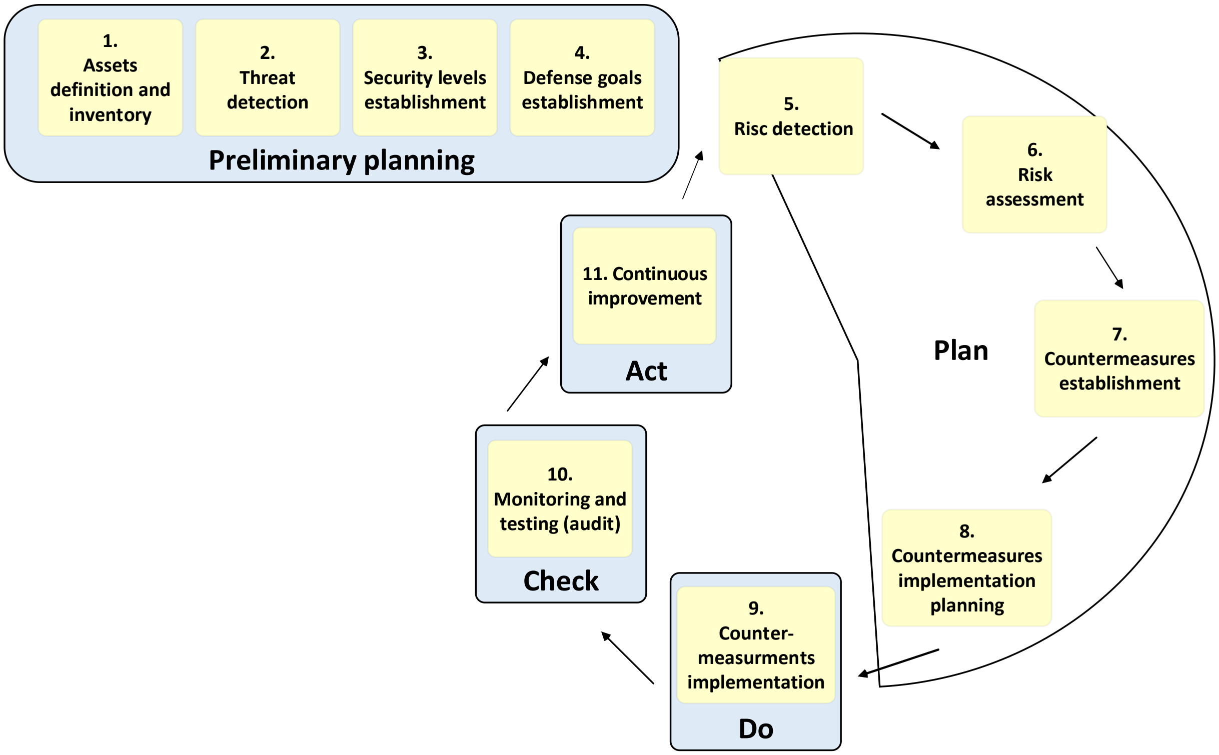

1. Assets definition and inventory
2. Threat detection
3. Security levels establishment
4. Defense goals establishment
Preliminary planning
5. Risc detection
6. Risk assessment
Plan
7. Countermeasures establishment
8. Countermeasures implementation planning
9. Counter-measurments implementation
Do
10. Monitoring and testing (audit)
Check
11. Continuous improvement
Act

Figure 3.13 – PDCA cycle for IEC 62443

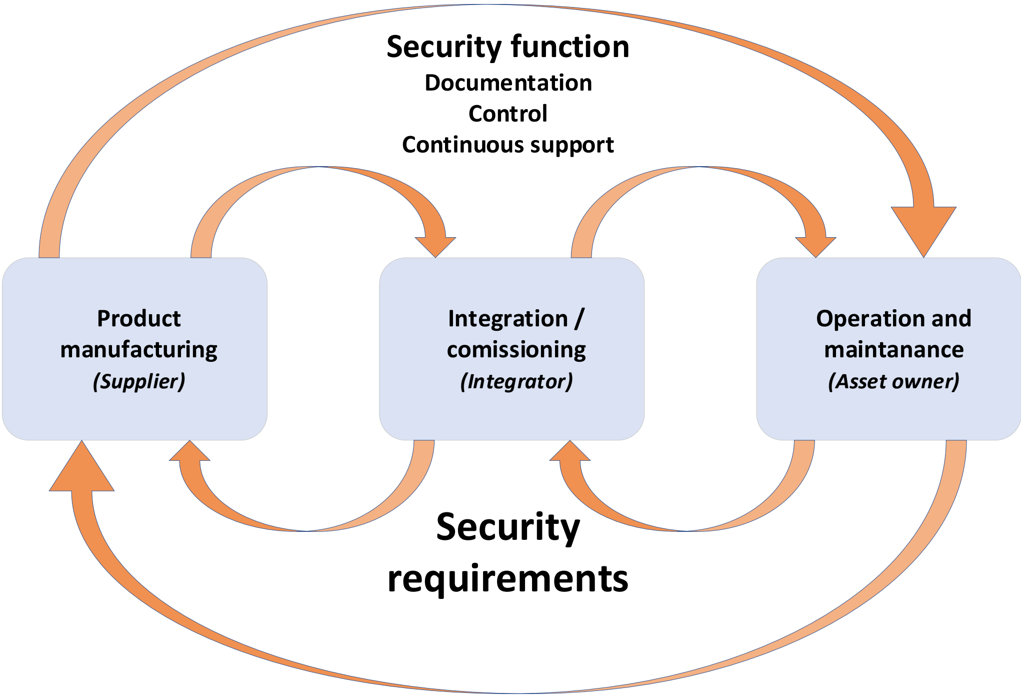


Figure 3.14 – Products and production lifecycle including cybersecurity

The SL security level can also be used to determine the layer defense-in-depth protection strategy to a zone, which includes hardware and software-based countermeasures.

Security levels determined for components are based on four types of devices defined in the standard, that is built-in device, host devices, network devices, and application software. Security level in a standard is recognized as follows:

- SL 1 – prevention of unauthorized disclosure of information by eavesdropping or by accidental impact;
- SL 2 – prevention of unauthorized disclosure of the information to the subject, which is actively looking for it using simple low-life tools, common skills and low motivation;
- SL 3 – prevention of unauthorized disclosure of the information to the subject, which is actively looking for it, using complex moderate resources, specific IACS skills and moderate motivation;
- SL 4 – prevention of unauthorized disclosure of the information to the subject, which is actively looking for it using complex tools with extended resources, specific IACS skills and high motivation.

Table 3.4 contains a brief description of security levels with an attached information on the hacking level and the tools used.

Table 3.4 – SL Security levels description

Security level	Description	Aim	Qualification	Motivation	Means usage
SL 1	Ability to protect against causal or random disturbance	Incorrect setting	No awareness	Non-systemized	Distributed
SL 2	Ability to protect against intentional violations using simple means with low resources, common skills and low motivation	No security measures implemented, the attacker is hacker	Basic	Low	Purposefully
SL 3	Ability to protect against intentional violations with complex means and moderate resources, specific IACS skills and moderate motivation	Only moderate security measures are taking place, high-level hacking is performed	Inherent in industrial domain	Medium	Intentionally
SL 4	Ability to protect against intentional violations with difficult tools, expanded resources, specific skills in IACS and high motivation	Ecomonic loss	Secific industrial	High	Aggressively

3.10.8 Maturity Levels Base on IEC 62443 2-4 and IEC 62443 4-1

Maturity levels are based on capability maturity model integration for services (CMMI-SVC). These levels determine the landmark that must meet the requirements specified by IEC

62443 2-4 and IEC 62443 4-1. Each level progressively moving forward comparing to the previous one. Service suppliers and assets owners are required to determine the maturity level associated with the implementation of each requirement.

Table 3.5 shows the output of each maturity level (ML) with categorization and description of each level.

Table 3.5 – Maturity levels description

Maturity level	**Category**	**Description**
ML 1	Elementary	The ability to provide a service without the support of the confirmed documentation process that is poorly controlled
ML 2	Controlled	Ability to provide a service with the support of formally documented process including the evidence of experience and trained personnel
ML 3	Determined	The ability to correspond to the ML2, including proof of personnel training, for example, a documented process and the participants of the personnel training
ML 4	Advanced	Ability to meet ML2 requirements, including a demonstration of continuous improvement, such as an internal audit report

3.10.9 ISA 99 / IEC62443 Target Audience

The target audience of ISA99 / IEC 62443 are:

- The suppliers of products (product developers) to be used on hazardous production.
- System integrators.
- Asset owners.

These roles are basic for the determination and connection of various parts in the IEC 62443 series, explained in the next Figure 3.15.

Figure 3.15 illustrates as a product developed by the supplier relates to maintenance and integration by the system integrator and its functioning by the owner of the asset. It also illustrates the role and interconnection between the *supplier, the system integrator and the assets owner*.

- *Product supplier* is responsible for developing and testing the control system that includes applications (antivirus, white list, etc.), built-in devices (PLC, DCS, etc.), network devices (firewalls, routers, switches, etc.), host devices (stations operators, engineering stations, etc.) that work together as a system or a subsystem, which is defined in IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2.
- *System integrator* is responsible for integrating and introducing a product to automation solutions, using a process compatible with IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-*3*.
- The *asset owner* is responsible for operational capabilities and maintenance through policies and procedures identified in IEC 6243-2-1, IEC 6243-2-3 and IEC 62443-2-4 for automation system developed by the implementation of automation on a particular area.

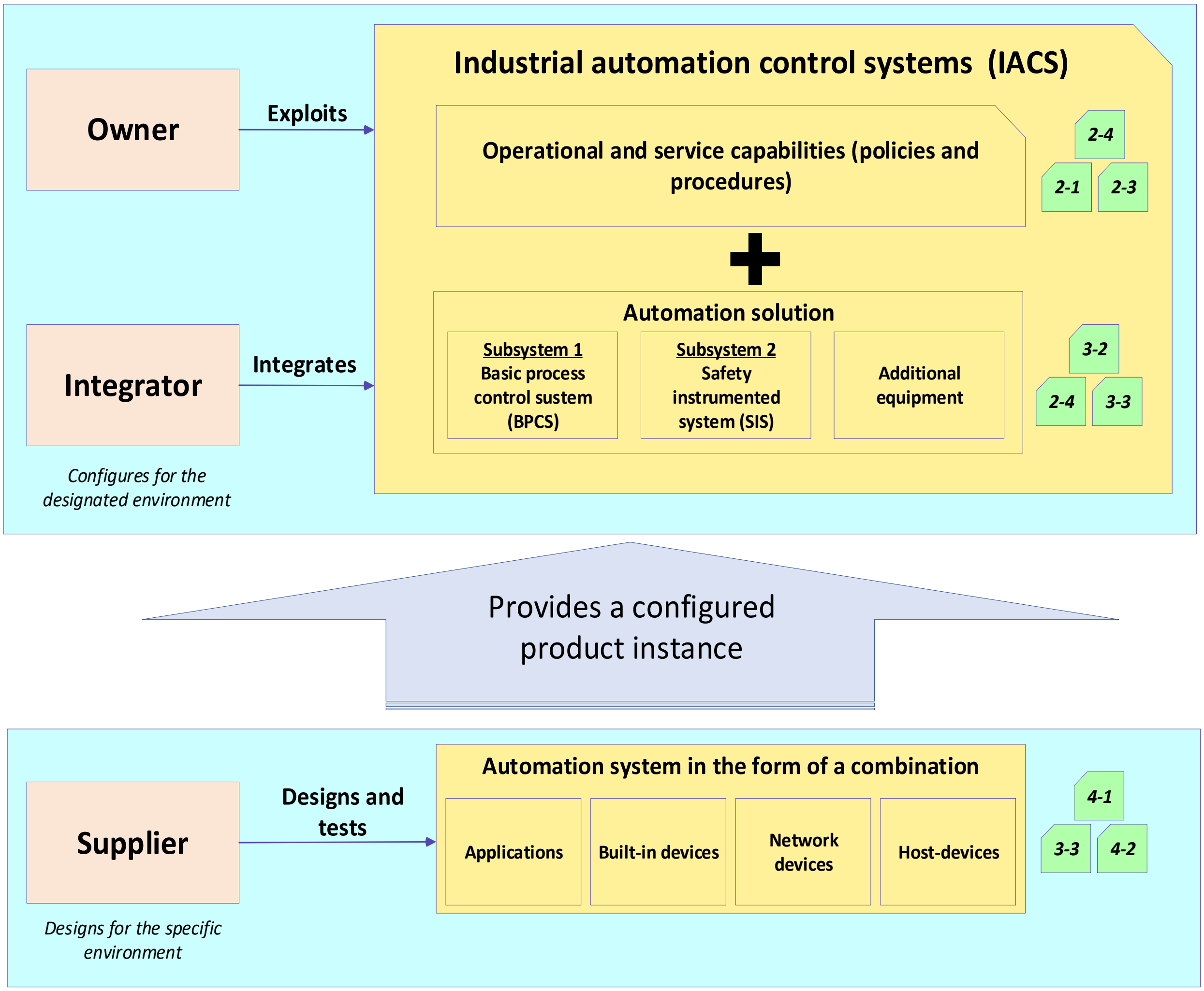

Industrial automation control systems (IACS)
Owner
Exploits
Operational and service capabilities (policies and procedures)
2-4
2-1
2-3
Integrator
Integrates
Automation solution
Subsystem 1
Basic process control sustem (BPCS)
Subsystem 2
Safety instrumented system (SIS)
Additional equipment
3-2
2-4
3-3
Configures for the designated environment
Provides a configured product instance
Supplier
Designs and tests
Automation system in the form of a combination
Applications
Built-in devices
Network devices
Host-devices
4-1
3-3
4-2
Designs for the specific environment

Figure 3.15 – Roles distribution in IEC 62443 series

3.10.10 Cybersecurity Lifecycle

The ISA / IEC 62444 standard determines the cybersecurity lifecycle as a powerful basis for the protection of industrial automation systems. The cybersecurity lifecycle is a process consisting of four basic phases that are reflected in Figure 3.16.

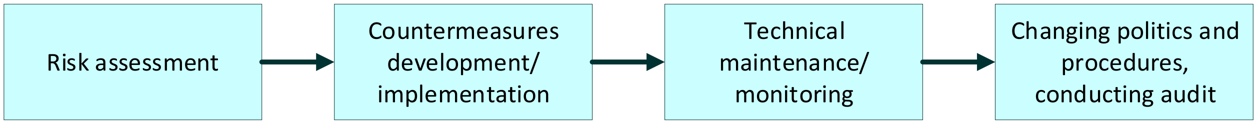

Risk assessment
Countermeasures development/ implementation
Technical maintenance/ monitoring
Changing politics and procedures, conducting audit

Figure 3.16 – Cybersecurity lifecycle

The assessment phase is an analysis of Industrial automation control systems. Distribution of assets on the zones and establishing communication of conduits between them. In this phase, it is necessary to determine vulnerabilities, calculate the risk and set the priorities based on relative risk.

The input data of the *implementation phase* is the results of assessment and risks and vulnerabilities prioritization from the evaluation phase, if it's used to create detailed security requirements. They, in turn, are used to develop and implement countermeasures that can be presented in the forn of the applied technologies, corporate policies or organizational practices (training, accountability, etc.).

The maintenance phase - through this phase, the enterprise actively watches the industrial automation system, responds to incidents, performs maintenance tasks (backup, correction, etc.) and manages changes.

The continuous improvement phase is the phase of analyzed lessons received from incidents, while introducing the necessary changes and implementation of periodic audits.

Further in the focus unit is aimed at two latest phases: technological maintenance and continuous improvement, since it is precisely that they are crucial for constant security of industrial management systems.

The maintenance phase consists of a variety of independent measures that need to be effectively managed on a permanent basis. Measures can be divided into 2 key types: constantly happening, and those that occur after events. Each will be discussed in details.

3.11 Ongoing Cybersecurity Measures During Maintenance

There are two main measures that are carried out by an enterprise when operating with IACS, they are assets monitoring and security monitoring:

- *Constant system monitoring.* Networks for tracking devices connected to the system where the latest software versions are used. Any new devices added to the system must be fully investigated. Possibilities of asset monitoring are usually provided by internal or third-party tools and applications;
- *Constant security monitoring.* In the phase of a cybersecurity life cycle introduction, various means and security systems, including network detection systems, security information and event management products (SIEM), antivirus programs and other security systems. This constant activity focuses on tracking technologies that have been implemented to detect harmful activity. Notification about adverse events received from these systems should be evaluated and processed within the incident handling process.

Cybersecurity monitoring is not a simple process as a for personnel to check the notifications in the morning after coming to the workplace. The staff must have deep knowledge of applications used to monitor and an idea of the false positives of protection systems, and also be able to configure the means and systems used to monitor security to optimize their accuracy.

3.12 Situational Cybersecurity Measures During Maintenance

In addition to the measures that are constantly operating on the background, there are many components of the maintenance phase, which are managed through incidents.

Patch management. Patches are used by suppliers to eliminate vulnerabilities and therefore are critical to cybersecurity systems. Patches can apply to endpoints protection systems and intrusion detection systems to update malicious programs signature base. Traditionally, companies with industrial automation systems update software during planned system shutdowns. However, this methodology is not compatible with the requirements for cybersecurity. Industrial automation and control systems should be able to distribute security patches in the periods between scheduled disconnections.

Potential patches must be rated begore the installation in the system. The patch can be addressed to vulnerabilities that are not a problem for the system of industrial automation, and in this case, it should not be installed. For example, a patch to eliminate vulnerabilities with File Transfer Protocol (FTP) is not a problem for a device where FTP has been disabled. The new patch should be analyzed for the purpose of determining whether there are new vulnerabilities that could lead to an increase in risk than addressed ones. Patches should also be tested in sandbox before placing in production network.

The patch management process can be simplified if the company with IACS equipment supports a list of all devices / applications. It is necessary to accurately identify the process that requires regular software reviewing to fix detected vulnerabilities.

Software patches are usually loaded from the enterprise to the Patch server, which is located within the DMZ between the enterprise and the management network.

System backup. Companies with IACS usually have internal guidance or policies that determine the system backup. Such policies determine the elements that require backup, backup interval, backup copies number, manual or automatic backup, backup schedules, file storage facilities (which should be safe), and also indicate how to correctly dispose the backup systems, that have reached the end of service/life. Backup policies may also require a specific functionality, such as signing the code to ensure the integrity of backups of files. It is important to note that both *baëckup* files and functionality restoration should be checked to guarantee the functioning of the system if the company has faced an incident associated with security.

Change management. At the implementation phase, diagrams with a description of the system architecture, network, inventory of assets, as well as various additional documents were created. Changes will take place during the system operation - when new modules, subsystems are added, the network changes, or a replacement of devices occurs. Each change may require not only fix in the system documentation, but also the corresponding changes of the document itself. In order to ensure effective decisionmaking, implementation and documentation in the IACS should be introduced by a formal process of change management. Otherwise, documentation will not be accurate, which can lead to problems when troubleshooting.

Incident processing. Processing of incidents. One of the most critical processes through the maintenance phase is the response and processing of incidents. The procedure for processing incidents creates a plan for fighting unauthorized invasions, cyberthefts, denial of service, malicious code and other events associated with cybersecurity. A key result is the creation and dissemination of the incident response plan.

3.13 Implementation-Related Challenges

Although the series of documents IEC 62443 has many advantages, but unfortunately, as the survey results (sub. 3.2) showed its implementation at the moment is quite problematic for Ukrainian enterprises.

Among the main obstacles the following are currently allocating:

1. The IEC 62443 series is not entirely complete. Some specifications haven't been published yet.

2. The IEC 62443 series is a comprehensive: with a total length of more than 800 pages currently and with the expected additional specifications in the near future, it requires a significant amount of time and effort to understand the entire series.

3. The cost of receiving a full copy of the standard in the web-store of the International Electrotechnical Commission is the equivalent of over $ 2,600 USD.

4. Standards and normative documentation in general are changing extremely rapidly, so it is important to review them regularly and promptly actualize national norms.

5. Lack of certification center market in Ukraine, which would be able to certify products for compliance with the requirements of the standards of 62443 series.

6. The culture of the security standards use at the enterprises of Ukraine is now being formed, unfortunately, only under the influence of external factors, among which there are both successful attacks on facilities and / or systems of critical infrastructure and mandatory, enshrined in normative legal Acts (including those which are currently being prepared) regulated procedures for security, non-fulfillment of which will be strictly punished following the certain procedural norms.

3.14 Security and Resilience Assurance Countermeasures for Industrial Automation and Control Systems

This Section is mainly based on statements of the document "NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security", which provides guidance for establishing secure ICSs, including SCADA, DCS and PLCs.

It is typically not possible to achieve the security objectives through the use of a single countermeasure or technique. A superior approach is to use the concept of defense in depth, which involves applying multiple countermeasures in a layered or stepwise manner. For example, intrusion detection systems can be used to signal the penetration of a firewall.

Defense-in-depth strategy should be implemented to assure security and resilience for ICS. ICS defense-in-depth may include the following countermeasures and means:

– Developing security policies, procedures, training and educational material that applies specifically to the ICS;

– Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases;

– Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning;

– Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer;

– Providing logical separation between the corporate and ICS networks (e.g., inspection firewall(s) between the networks, unidirectional gateways);

– Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks);

– Ensuring that critical components are redundant and are on redundant networks;

– Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events;

– Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation;

– Restricting physical access to the ICS network and devices;

– Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege);

– Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts);

– Using modern technology, such as smart cards for Personal Identity Verification;

– Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS;

– Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate;

– Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS;

– Tracking and monitoring audit trails on critical areas of the ICS;

– Employing reliable and secure network protocols and services where feasible.

Technological security assurance countermeasures are based mainly on implementation of secure ICS architecture including the following issues:

– Network segmentation and segregation;

– Boundary protection;

– Encryption;

– Firewalls and DMZ establishing;

– Protocols choice and control;

– Redundancy and fault tolerance;

– Authentication and authorization;

– Monitoring, logging, and auditing;

– Incident detection, response, and system recovery.

3.15 Industrial Automation and Control Systems Security Provision Principles

3.15.1 Security Levels

The IEC 62443 standard includes the concept of security levels. The specification defines a number of requirements designed to withdraw the security of the system to one of the four defined levels. A description of each level in conjunction with the characteristic of the type of attacker, from which the level is protected, presented in the Table 3.6 below.

Table 3.6 – IEC 62443 Security levels description

Security Level	Aim	Skills	Motivation	Means	Resources
SL1	Unplanned and disruption violations	No skills for attack handling	Mistake	Unintended	Person
SL2	Cybercrime, hacker	General	Low	Easy	Low (isolated person)
SL3	Activist, terrorist	Special for ICS	Middle	Intermediate (Attack)	Moderate (hacker group)
SL4	State level	Special for ICS	High	Intermediate (Campaign)	Extended (Multi-disciplinary teams)

The end-users are interested in supplying a solution for protection from conventional hackers or cybercrime must, for example, implement a system with functions determined by security level 2. It should be noted that the characteristics presented in the table are common classifications for providing the implementation of SL2 for high-level management users, does not guarantee that the system can stop the attack by any hacker or cybercriminal.

3.15.2 Defence in Depth

Defence-in-depth is a coordinated use of countermeasures to protect the integrity of information assets on the network. The proper implementation of the defence-in-depth strategy involves performing six steps. Below there is a brief description of each step.

– *Creating a security plan*. The most important step in the overall process of defence-in-depth includes the creation of a security plan. In the security plan, the staff creates a detailed audit of all equipment connected to the industrial control network, displays how the equipment connects, reviews the equipment security configuration and evaluates the potential vulnerabilities of the system. The security plan includes the impact of products, architecture, people and corporate processes. A completed security plan is required before taking any additional steps to improve system security. Otherwise, the staff may think that the system is protected without knowing potential vectors of the attack.

– *Separate networks* – Once in the security plan, a detailed network map was created, the network can be divided by basic functions. An example may be division of the network to the enterprise zone, plant, processes and areas. All conduits between zones must be defined..

– *Perimeter protection* – In this step, the conduits between the areas are properly protected. An important part of this step involves providing the remote access.

– *Network segmentation* – On this step zone created in the second step, can be split into smaller zones by location or functions. Perimeters of these segmented zones are protected. It is important to note that the security level intended for each zone may vary. For example, the security level, which is provided to the equipment with monitoring role, may be set to level 1, while the security level assigned to the security system may be set to level 3. The level of each segmentated zone should not be the same as its neighbors.

– *Devises enhancing* is adding functions to ICS devices to improve their ability to resist cyberatics. This reduces the likelihood that the network elements will be violated, as a hacker receives access to the network.

– *Monitoring and update* is active network monitoring to detect potential threats and product fixes, since new software / firmware are available to eliminate vulnerable places or to add security features.

3.16 General Stages of Industrial Automation and Control Systems Security Assessment

This recommended practice focuses on pre-project planning (Feed), design and operational phases, but alsoit includes best practices for roles and responsibilities that must be determined at the stage of concept development. Definition of roles and responsibilities is applicable to all stages, though the special attention should be paid to the stage of the concept development.

This section is based on IEC 62443-3-2 / 3 /, and describes the proper practice on how to assess the risk and design the system during the FEED phase. Recommended steps listed in Figure 3.17. The execution of the steps will be documented in the cybersecurity requirements specification (CSRS). The CSRS will then be used to transfer cybersecurity requirements to stakeholders, as well as developing / implementing groups that perform a detailed development, installation, FAT, commissioning and inspection.

For some projects, the initial CSRS can be prepared until the risk assessment is finished, as the purchase of equipment packages is often completed at the beginning of the FEED phase. It is recognized that by that time, all information used as input data for CSRS may not be available. However, it is extremely important to establish some of the initial cybersecurity requirements during the procurement process to provide the necessary equipment with the necessary capabilities of cybersecurity to meet the expected level of control / security requirements.

3.16.1 Identification of the considered system

Input data:

1) Initial system architecture schemes and inventory
2) Initial network topology charts for all packets that will be included in IACS

The input data should be as:

1) Diagrams of high-level network topology
2) Diagrams example
3) System of communication inside and outside of the considered system (SuC)

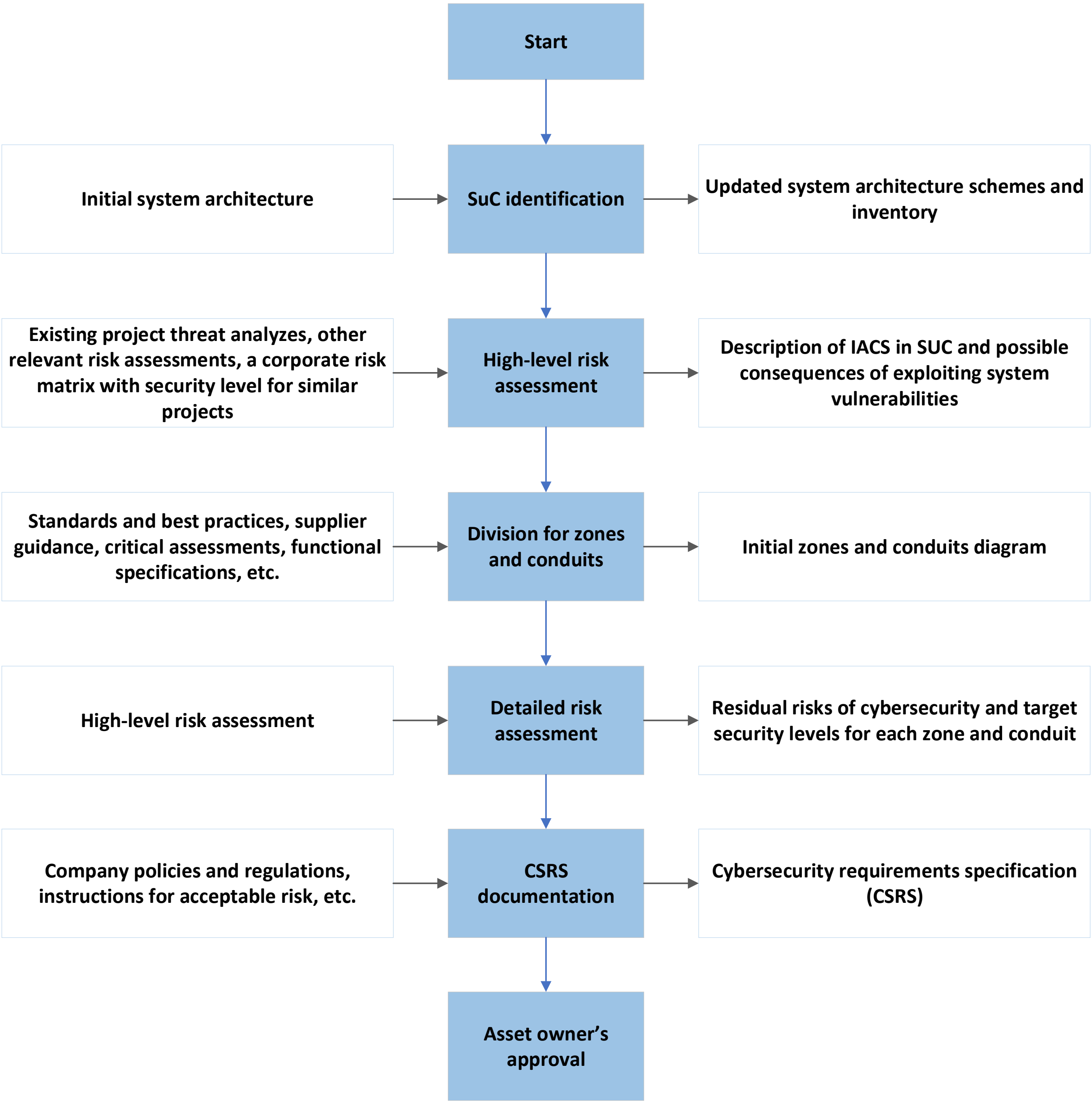

Start
Initial system architecture
SuC identification
Updated system architecture schemes and inventory
Existing project threat analyzes, other relevant risk assessments, a corporate risk matrix with security level for similar projects
High-level risk assessment
Description of IACS in SUC and possible consequences of exploiting system vulnerabilities
Standards and best practices, supplier guidance, critical assessments, functional specifications, etc.
Division for zones and conduits
Initial zones and conduits diagram
High-level risk assessment
Detailed risk assessment
Residual risks of cybersecurity and target security levels for each zone and conduit
Company policies and regulations, instructions for acceptable risk, etc.
CSRS documentation
Cybersecurity requirements specification (CSRS)
Asset owner's approval

Figure 3.17 – Steps on the FEED stage

Detecting SuC best practice:

1) Include an overview of all system assets needed to provide a solution concerning IACS.

2) Describe security perimeters:

– Turn on firewalls that are used for the perimeter implementation.

3) Determine which external access / login points will exist for SUC after transferring it into production:

– IACS remote access

– Online file transferring requirements

– Online file transferring into offline systems (USB)
– Data flows from/to outer systems.

Output data: Description of the designated operating environment, updated system architecture diagrams and assets list describing SuC, perimeters and access points.

3.16.2 High-Level Cybersecurity Risk Assessment

The high-level risk assessment is used to determine the impact on business and HSE in the event of a system compromentation or failure. The purpose of risk assessment is to identify the worst risk for SuC. The result of a high level risk assessment will be included in the grouping of assets into zones and conduits, and a detailed risk assessment. Steps involved in the high-level cyber security estimation are shown in Figure 3.18.

The target group for the high-level risk assessment includes stakeholders that may have limited knowledge of cybersecurity risks. The high-level risk assessment should be documented in a way that allows all interested parties to get a clear understanding of existing high-level cyberrisks.

The high-level risk assessment is usually based on a supervisory seminar. The result must be represented by the relevant local / regional asset owners and stakeholders.

Input data:

– Matrix of corporate risks, business impact assessment, recovery after incidents plans, incident response plan, functional characteristics, etc.

– Relevant security assessments (such as specification of safety requirements)

– Description of the asset owners activity on security systems and barriers standards. Best practice to assess high risk level:

1) Assemble information about which systems / packages IACS in SuC to purchas and install.

2) Identify on the framework level the worst cyberthreats scenarios based on input data, such as corporate risk matrix, impact on business assessment, etc.

3) Identify business criticality and consequences of the worst scenarios (security, ecology, finances, brand). Consider using input security data related to HAZID and HAZOP activities.

4) Describe which of IACS systems / packages will have a critical functionality necessary for the implementation of security systems and barriers, and identify general independent layers of protection.

5) Determine the probability of worst scenarios (for example, high, medium, low). For example, the probability can be based on the capacity, motivation and the ability of a threat agent to use the threat vector. Ability is based on vulnerability in appropriate systems / packages.

6) Based on previous steps, conduct a relative risk classification of not mitigated risks relating to SUC systems / packages.

Output data:

– Description of IACS in SuC and possible consequences in case of vulnerability exploitation, which causes inaccessibility to systems or loss of integrity or confidentiality. An assessment of what is the least risk that is not a mitigation.

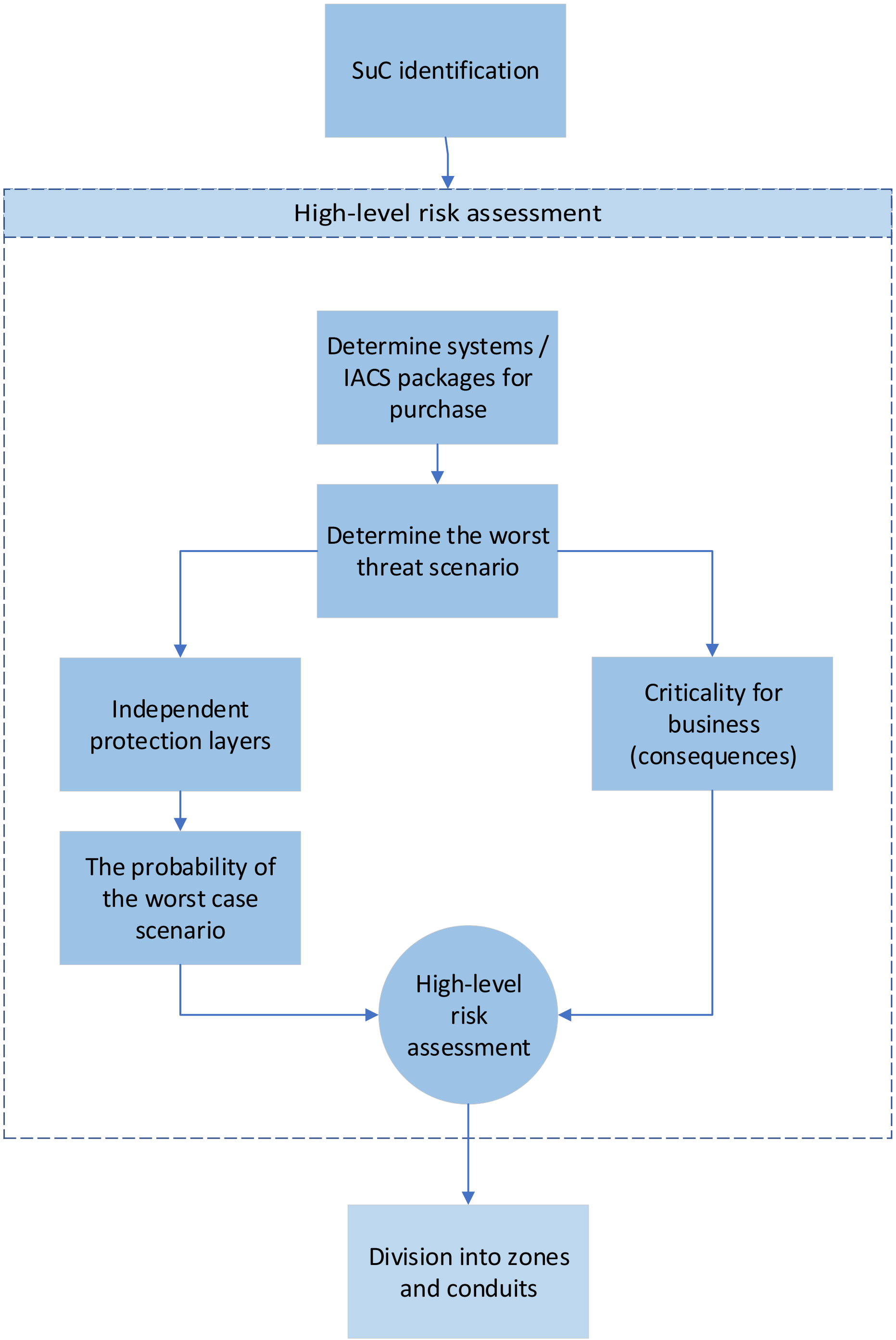

SuC identification
High-level risk assessment
Determine systems / IACS packages for purchase
Determine the worst threat scenario
Independent protection layers
Criticality for business (consequences)
The probability of the worst case scenario
High-level risk assessment
Division into zones and conduits

Figure 3.18 – High-level risk assessment

3.16.3 The Division of the Considered System into Security Zones and Conduits

Input data:

1) Cybersecurity high-level risk assessment results.
2) A reference model defined in this document.

The input data should be as:

1) High-level cybersecurity risk assessment. Consider reuse risk assessments for similar IACS solutions.
2) Reuse the division into zones and conduits for such projects.
3) Reuse the supplier's best practice packages.

3.17 The General Strategy of System Division into Security Zones and Conduits

Data network connecting components in SuC must be divided into zones based on system functionality, location, responsible organization or risk assessment.
It is recommended to start with a functional segmentation that divides the network into several layers, with an upper corporate zone, moving through DMZ to the control zones and, finally, to the IACS system and safe systems (SIS).

Dividing SuC on the zone and the conduits requires a good understanding:

– how different systems interract
– where the information exchange between systems takes place:
  - how the devices interract
  - how fast/often the devices interract
– what from the information takes
– security differences between system components
– system criticality (based on high-level risk assessment, as it is described above).

If the main initial zones are set, the attention can be payed to specific groups or subzones within each primary zone, and how these subzones interact with other ones. This step takes into account the nature of network traffic sent and taken by each subzone component, as well as specific network services offered or are necessary. Security and functionality requirements that are already defined in previous steps are improved and clarified.

3.17.1 Distribution of Functionally Safe System Zones

Safe system (SIS) zones can be separated from the control zone in various ways. ISA-TR84 describes four options: physically unbound, associated by the interface, integrated two and one-zone ones.

The distribution of SIS zones should be based on risk assessment. SIS-communication and process management communication must be physically or logically separated. Failures and cybersecurity incidents should not obstruck SIS to perform it's security features.

In addition, it should not be possible to establish a connection to SIS from other zones (including remote access programs) at level 3 or higher. (See IEC 62443-2-4 Req. ID SP 05.01 to SP 05.09) The SIS controller must be protected from unauthorized and unintentional changes loading, for example, with unique passwords for each SIS. The password must be known only by authorized personnel defined as SIS users.

Hard signals between SIS controllers can be used as an alternative for critical communication for secure communication in the general technological network.

To provide additional protection of SIS controllers, you can use a local protective device (for example, a local key switch). In the network where the SIS system and process control are physically linked, to ensure that logical separation (integrated 1 zone) must be used.

SUC consists of systems of different sizes, complexity and criticality. Engineering tools, configuration tools and diagnostic tools are required to work with and maintain these systems. For highly critical systems, these tools should be included as permanent equipment (for example, SIS, SAS, electric control, etc.).

For systems with low criticality, these tools can be connected using remote access solutions or with the help of temporary devices (such as a portable computer). This largely depends on the side that will work with and maintain systems in the operating phase. For example, if an asset owner works with and supports a system, permanent equipment can be a good solution.

For systems with extensive use of external suppliers providing temporary devices, you must create a separate zone for temporarily connected devices. In this area, procedures and technical solutions should be established to check the state of a patch, hardening and antivirus status. After this, the checked device can be provided to the IACS zones by the remote access or solution adapted for this temporary access zone. The device check may also be used as part of the approval process so that the device can physically connect to other zones.

The best practice of connecting PC to temporary service is:

– Use specially designated equipment.

– Obtain an official approval on a connection from an asset owner.

– Make sure the device has upgraded patches.

– Make sure that antiviruses are installed, endpoints protection and signatures are updated. Solutions that exhibit heuristic behavior are better.

– Make sure that an antivirus scans it before the connection is established.

Connecting a temporary device directly to the IACS zone should be processed as a deviatëion.

In addition to procedures and technical equipment for checking portable computers, it is necessary to install equipment for checking variable data storage devices. It is good to use two independent antivirus solutions on such equipment. Antivirus signature files should be continuously updated.

3.17.2 Distribution of Wireless Communication

Wireless conection can be divided into various categories, such as a wireless solution for an office network, a wireless communications for entertaining devices and wireless communications for industrial networks (for example, at the level of the control network).

Wireless communications requirements can be found in IEC-62443-2-4 SP04 and IEC62443-3-3 FR1 SR1.6 and FR2 SR2.2.

Traditionally IACS equipment connects on the building stage, but changes and new equipment are usually connected to a wireless network due to the cost of cables. Therefore, the security of wireless communication must be included in the network design and procedures.

Next best practices are concerning wireless communications:

– Wireless communication must be located in one or more zones divided from wired communication.

– Wireless networks must apply powerful authentification and encryption schemes (for example, WPA2 or EAP-TLS).

– Mobile Workers" and devices (except for planned barrier devices) should not simultaneously be connected to Wireless Office Networks and Wireless Industrial Networks.

3.17.3 Distribution of Devices Connected Through Unreliable Networks

Devices that are allowed to connect to SuC through an unreliable network must be allowed only through the remote access solutions. These include devices in the corporate network, devices connected to the zone of temporarily connected devices, and supplier's ones used for remote maintenance.

Permanent devices placed in a physically protected zone can be connected to segment's control processes as described earlier.

3.17.4 Security Zones and Conduits for Remote Controls

In practice, the there will be several applications / computers in different zones that require channels to communicate with the remote control. Each of these zones requires the corresponding zone in the remote control, preferably with the same security level.

Conduits are used to connect zones. To ensure proper cybersecurity it is considered to be a good practice to use the following design criteria in the implementation of the conduits:

– Conduits connecting zones with high criticality must be designed by two separate network routes between LCR and RCR. This will ensure high availability.

– The conduits connecting zones with high criticality should have a functionality for mutual authentication, checking the integrity and encryption of packets. This will let to avoid unauthorized access, attack "Man in the middle" and / or eavesdropping.

It is considered to be good practice to apply the conduits between zones of increased criticality using protected tunnels. The end point of the conduit should be in different zones. The decisions must be based on well-accepted network security standards.

For communication on L3 (which can be routed using IP routing), IPSEC may be used in tunnel mode. Mutual authentication, integrity of packages, encryption and playback protection mechanisms are included in this standard and must be configured. It is needed to avoid breaking the tunnel and allow it to end on the devices on the border (or within) of the zone.

For communications at L2 level (A1 and A2 zones should support communications with L2, since they belong to the same IP subnet, or because the non-IP traffic) IEEE 802.11AE (MACSEC) can be used. Mutual authentication, integrity of packages, encryption and mechanisms against playback are included in this standard and should be configured.

It is necessary to protect the solution control interface used to implement channels in the same way as protected hardware / software and information in zones.

It is necessary to establish procedures and responsibility for managing encryption keys. Typically, these keys are processed by digital certificates that have a validity period (usually three years). At the expiration date of the key, the device stops the connection. A general overview of certificates and periodic reviews should be established, or this service may be provided by an external certification authority.

3.17.5 Documentation of Security Zones and Conduits Characteristics

Input data:

– Initial topological schemes (high-level network topology diagrams, control system schemes).

– Results of high-level risks assessment.

How the data looks like:

– This document provides a general scheme of zones and conduits. Different SAS providers may have different benefits.

Output **data:** Updated system architecture and inventory schemes describing SuC, perimeter and entry points.

How should look (content and format) output data (delivery): IACS high-level network from representative suppliers**.**

– The following characteristics should be documented for zones and conduits:

– name and/or uniue identifier

– physical or logical boarder

– access points (integration, wireless access, remote access)

– list of external data streams (and internal data streams in the zone)

– assets (equipmrnt and software)

– compound zones

– security requirements

– SL-T

– security policy

– assumptions and dependences.

The conduits and their numbering should be reflected in the rules of network filtration for routers and firewalls.

3.17.6 Risk Assessment of Zones and Conduits Security

This subsection contains a brief description of a detailed risk assessment. A detailed risk assessment is initially carried out at the FEED stage, but is constantly updated, in accordance with similar principles, on the phases of design and operation (see Fig. 3.19).

Next recommendations are concerning detailed risk assessment:

Use the scenario-based approach.

– Do qualitative risks assessments because they are less complicated and will help compare risks in various projects and systems.

– Evaluate the risk for groups of systems when it’s appropriate. For example, if the supplier is involved

– In the SAS system consisting of several zones, estimation of the full SAS system risk may be expedient.

– Contractors should facilitate risk assessment by relevant suppler's system / packets according to the chosen risk assessment methodology.

– Characterize some assumptions that are needed at risk assessment:

- The project must determine and describe external interfaces.

- The asset owner must provide a description of policies and procedures. For example, existing operating and maintenance processes.
- The asset owner must describe the mechanisms used to control barriers.
- Internal interfaces and streams in zones should be taken into account because they can be used by an agent of risk.

–Good to use of risks estimates for similar systems where possible.

–It is necessary to use a general calibration scale. This will facilitate the comparison of input data and analysis between projects and systems.

–It is necessary to choose the highest risk associated with the worst scenario, while doing risk aggregation.

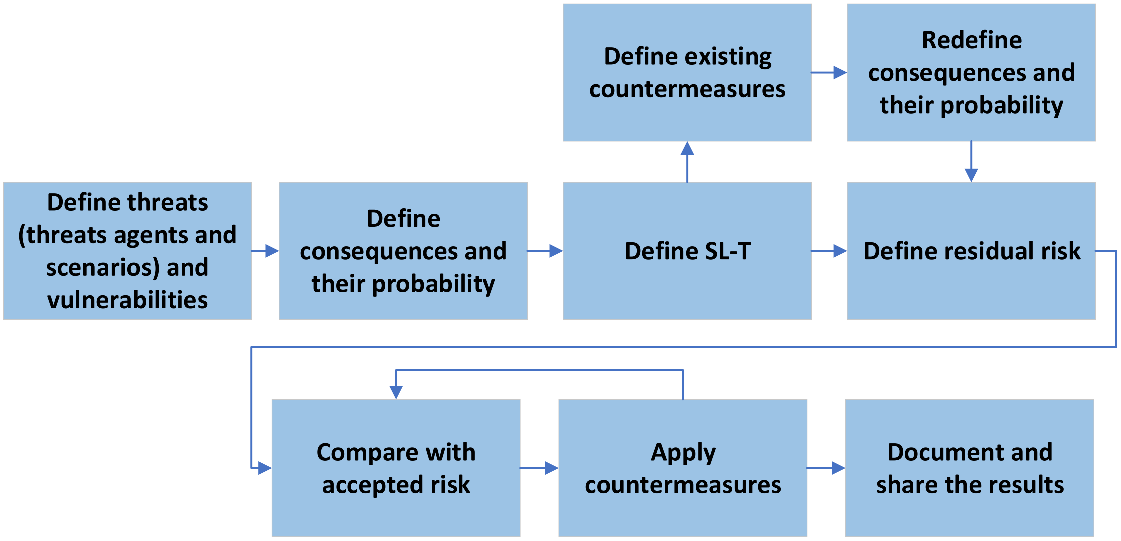

Define threats (threats agents and scenarios) and vulnerabilities
Define consequences and their probability
Define SL-T
Define existing countermeasures
Redefine consequences and their probability
Define residual risk
Compare with accepted risk
Apply countermeasures
Document and share the results

Figure 3.19 – Detailed risk assessment operation process overview

Output data of high-level risk assessment and division into zones and conduits gives a good review of software systems that are critical to this system. A detailed risk assessment should be made for each zone and conduit. However, it is important to arrange the priorities of systems with high consequences where the threats are relevant.

A detailed risk assessment is usually based on seminars covering all zones and conduits. The result must be represented by local / regional superior management, and mitigation measures should respectively be included.

The asset owner or relevant authority is obliged to accept residual risk. If the residual risk deviates from acceptable risk (ALARP), an appropriate control system should be applied to close gaps (for example, a design list, IOC, deviations).

To comply with IEC 61511 requirements for measuring the risk of cybersecurity, it is recommended to evaluate all stages of the project (from design to operation) when assessing risk.

The standard also refers to ISA TR 84.00.09. To comply with risks assessment requirements in this standard, danger and threat agentsthat are important for SIS, should be included in risk assessment.

3.18 Security and Safety Relation in Industrial Control Systems

Safety and security are included in IACS context, however, relation of these attributes requires a separated study. In an ICS context the subjects of security and safety are closely linked. A failure to secure an ICS can in turn result in a potentially unsafe system under control.

Safety Instrumented Systems (SIS), represent one layer of protection that may be implemented in order to reduce risks associated with ICS. Traditional risk assessment methodologies in the past, have generally excluded the potential for cyber related attacks to cause safety related incidents. Given that targeted attacks on ICS have occurred and these systems are increasingly being connected to other business systems, they represent a significant potential for common mode failure. As a result, it is necessary in today's world to include cyber security in the overall risk assessment. Without addressing cyber security throughout the entire safety lifecycle, it is impossible to adequately understand the relative integrity of the various layers of protection that involve instrumented systems, including the SIS.

The increasing inter-connectivity of control systems is equally important to industry since new benefits also bring new challenges. Open industrial networks that seamlessly coexist in broader Ethernet systems are being used to link various plant -wide control systems together and connect these systems into expansive, enterprise-level systems via the Internet. As the pace of control system and enterprise network architecture convergence quickens, industrial security depends on staying both flexible and vigilant and successfully controlling the space. What may be considered adequate protection today should evolve as vulnerabilities are identified and new threats emerge.

The discovery of malware that specifically targets industrial control systems brought industrial security to the forefront in manufacturing. As a result, there is growing recognition of the risks and real-world threats that are capable of disrupting control system operation and adversely affecting safety.

An approach to handle requirements to ICS security and functional safety in a general framework is described below.

A set of ICS functional safety requirement can be found in series of industrial standards, for example, IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems” or IEC 61511 “Functional safety – Safety instrumented systems for the process industry sector”.

These functional safety requirements can be divided in some following categories:

– Requirements to functional safety management;

– Requirements to functional safety life cycle;

– Requirements to systematic (system and software design) failures avoidance;

– Requirements to random (hardware) failures avoidance.

A scope of the above requirements is highly dependent from as named Safety Integrity Level (SIL) which establishes relation between ICS risk level and a scope of the related safety assurance countermeasures. The discussed approach can be represented in a view of a diagram (see Fig. 3.20).

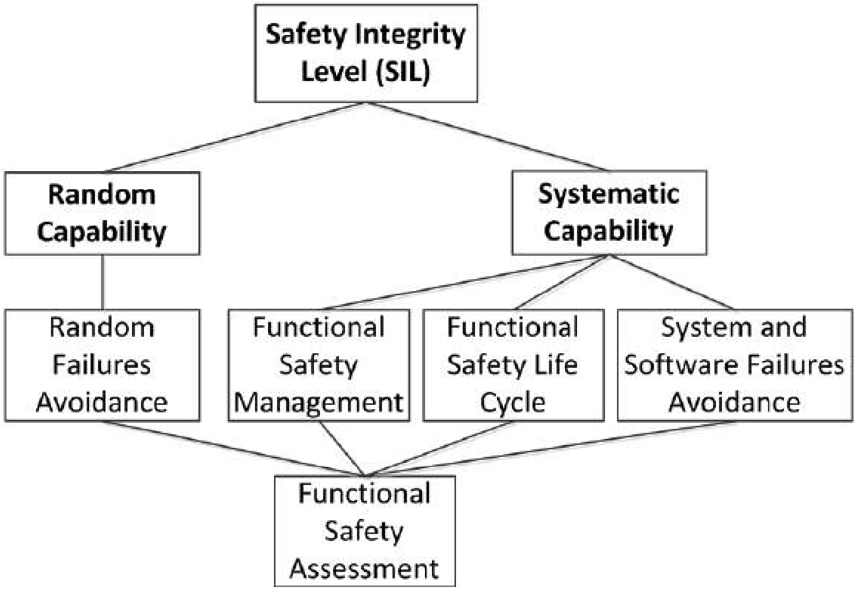

Safety Integrity Level (SIL)
Random Capability
Systematic Capability
Random Failures Avoidance
Functional Safety Management
Functional Safety Life Cycle
System and Software Failures Avoidance
Functional Safety Assessment

Figure 3.20 – A concept of ICS safety requirements

The above approach can be applied for ICS security concept. Firstly, Security Levels shall be implemented for ICS taken into account risks levels. Secondly, ISMS shall be implemented and coordinated with functional safety management issues. Thirdly, a common security and safety life cycle shall be established to cover all the process of ICS development, verification and validation. Fourthly, common safety and security risks shall be avoided to implement coordinated countermeasures against random (hardware) and systematic (system and software design) failures. Examples of common safety and security random failures avoidance countermeasure are redundancy, self-diagnostic, electromagnetic disturbances protection and others. Examples of common safety and security systematic failures avoidance (attacks avoidance for security) are access control and configuration control. Fifty, assessment shall be periodically performed for both, security and safety. The discussed approach is the base for security and safety coordination, as it is represented on Fig. 3.21

3.19 Summary

Cybersecurity is extremely important in the industrial sector. Cybersecurity management is not a one-time activity. As well as quality and safety management, cybersecurity management is a permanent activity where it is necessary to continuously improve the risk management.

Cybersecurity of industrial management systems is an issue with numerous aspects covering technology, processes, equipment and people, it crosses traditional barrier of geography, domains of industry and applications. Vulnerabilities and associated attacks, malicious or unintentional, can lead to devastating consequences for financial, security and reputational brands. Executive management should carefully consider their impact on these risks.

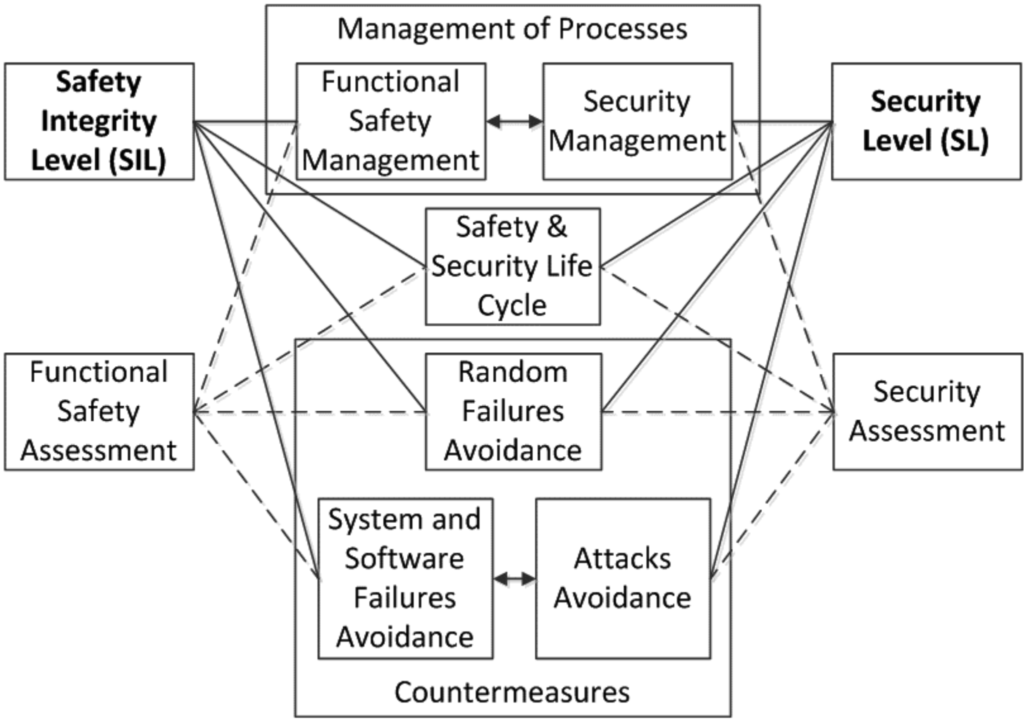

Management of Processes
Safety Integrity Level (SIL)
Functional Safety Management
Security Management
Security Level (SL)
Safety & Security Life Cycle
Functional Safety Assessment
Random Failures Avoidance
Security Assessment
System and Software Failures Avoidance
Attacks Avoidance
Countermeasures

Figure 3.21 – A concept of ICS harmonized security and safety requirements

Global consensual standards of the ISA 99 / IEC 62443 series, oriented on cybersecurity of industrial control systems, determine the requirements and procedures for implementing electronically protected automation systems for industrial control and security practices. The ISA 99 / IEC 62443 standards holistically approach the problem of cybersecurity, overcoming the gap between operating and information technologies, as well as between the safety of processes and cybersecurity.

Currently, in most companies there are still gaps in culture, knowledge and experience between representatives of information and operating technologies. Coordination of IT and OT functions with cybersecutiry management system (CSMS) expert team is an extremely important thing for successful introduction of a comprehensive cybersecurity program.

These standards may be applied to processes, relevant training and certification programs can be used to train personnel, and relevant compliance programs can be used to test and certify equipment. Using the data of well-known incidents and vulnerable situations and using the standards of the ISA 99 / IEC 62443 series, training and compliance programs, system engineers and specialists CSMS will be able to reduce the risks for critical infrastructure from the side of hostile participants, human errors and disadvantages that were made while designing systems of this kind.

Taking into account the interconnection of modern advanced computer and control networks, where the vulnerabilities operated in one sector may affect other sectors and damage several of them, it is important that cyber security standards are widely used in industries or sectors. The series of security standards for industrial automation and control systems ISA 99 / IEC 62443 is a multi-sectoral initiative to be applied to all key industries and critical infrastructure.

Standards of industrial automation and control systems are developing, and the IEC 62443 standard becomes the best approach to many. The difficulty is that this is a general standard for all industrial components and that it has not yet been finished.

Checking the correspondence to the entire IEC 62443 standard series is very expensive, and some parts may be inappropriate for certain industries. The standard also relates to security levels, but it may be difficult to determine the correct goal for different systems. Currently, the standard determines what to do but does not fully detail how to do it.

Finaly, it's worth notinf that the threat of cyberattack will remain a problem for IACS in the foreseeable future. Standards and normative documents of the IEC 62443 series create a basis that allows operators to enhance system security. The main first step in this process is the stage of evaluation, which allows end users to analyze its system and understand what threats should be considered primarily. Countermeasures must be implemented at the implementation stage. The general system is guided by the processes specified in the White Book. The main thing is to stop expectations and not to avoid the analysis, it is better to start implementing countermeasures and improve them with time than just to wait for the next attack.

4 FUNCTIONAL SAFETY REGULATION, ASSESSMENT AND INSURANCE

Safety assessment is a complicated and resource consuming process that is required be done so as to ensure the required safety level and comply to normative regulations. A lot of work have been performed in the field of application of different assessment methods and techniques, modifying them and using their combinations so as to provide unified approach in comprehensive safety assessment. Anyway, performed research have shown there are still challenges to overcome, including rationale and choice of the safety assessment method, verification of assessment results, choosing and applying techniques that support safety assessment process. These techniques can be rather simple or quite complicated to implement depending on the problems at hand. Generally, during safety assessment process the following challenges are met:

- complex fault-tolerant architecture;
- usage of multiversion technologies;
- large number of different components.

Also, there are many characteristics making the chemical and energy carriers industries different. For example, it is not enough to have only a safe installation, but it also has to be proved to the licensing authorities that the installation really is safe and meets all the necessary requirements.

Safety covers a set of measures aimed at preventing harm to people, environment and the loss of property in the event of an emergency (accident, etc.). Safety can be compromised due to hardware and software failures (reliability aspect), or due to unauthorized interventions, vulnerability exposures (information security and cybersecurity aspect). A high-level safety is provided when the safety function in emergency situations is implemented predictably and reliably. In industrial systems, for example, typical safety functions include such as emergency stop, boiler pressure control, emergency opening or closing of the valve, refraining from closing the sluice gate, and so on.

For example, to prevent the acceptable pressure level in the boiler from being exceeded, the opening of the pressure reducing valve is provided as a safety function. To do this, the appropriate sensors continuously monitor the pressure in the boiler. In case of reaching the unacceptable pressure level, the controller of the safety-related system must generate an appropriate alarm and issue an "Open" command to the valve actuator in order to reduce the pressure in the boiler to an acceptable level.

4.1 Regulation Framework

4.1.1 Standard IEC 61508

The basic safety standards of electrical, electronic and programmable electronic (E/E/PE) devices and systems are given in the series of IEC 61508 standards. A feature of the standards of this series is a risk-oriented approach to safety assessment. Depending on the damage that can be caused by man-made objects to human life, health or the environment, appropriate risk levels are set. To reduce the risk level, a set of measures is provided, which is regulated by a series of standards IEC 61508. Moreover, one of the tasks addressed by the IEC 61508 standards series is the requirements formation for the development of electrical, electronic and programmable electronic safety-related systems for industries where there are no relevant industry standards. The current version of the IEC 61508 standards series, which was put under operation in 2010, is the second generation and it repealed the first generation of standards from 1998 (Fig. 4.1-4.2).

The following definitions are given in IEC 61508-4 part:

- Equipment under control (EUC) – equipment, machine, apparatus or installation used for the production, processing, transportation, medical or other activities.
- EUC control system - a system that responds to input signals from the process and / or operator and generates output signals, determining the operation of the EUC as needed.
- E/E/PE system - a system based on one or more electrical and / or electronic and / or programmable electronic (E/E/PE) devices that performs control, protection or surveillance functions, including all elements of the system namely internal power supply, sensors and other input devices, data bus and other communication channels, actuators and other output devices.

Safety is a part of the general security related to the EUC and the EUC control system, and it depends on the correct E/E/PE systems functioning related to safety and other means of risk mitigation.

To achieve safety, two types of requirements must be implemented:

1. Safety functions requirements are the requirements for safety functions performed by the control system

2. Safety requirements integrity are the requirements for the probability of satisfactory performance of safety functions. These requirements can be formed after conducting the system's risk analysis.

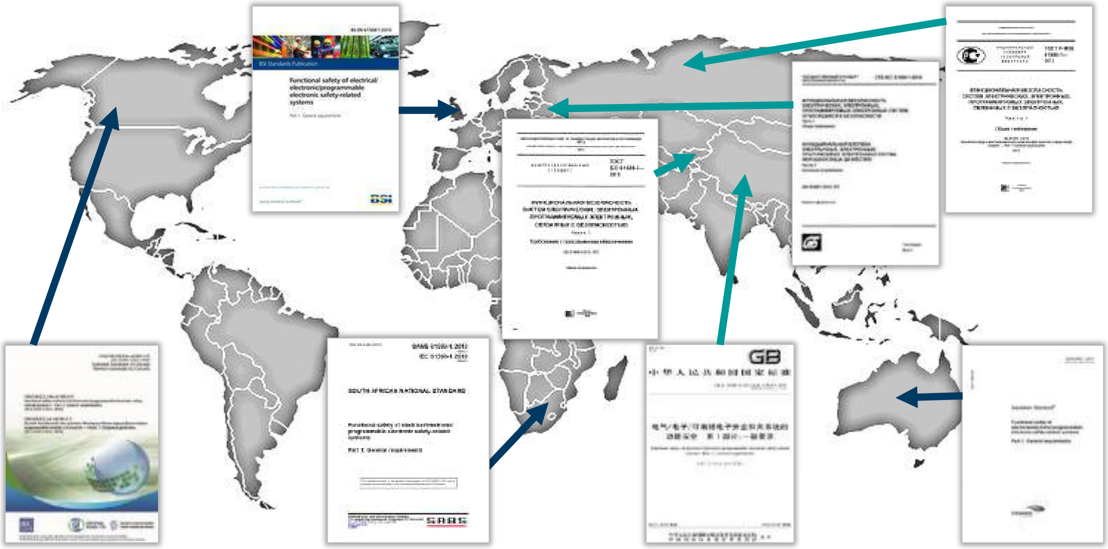
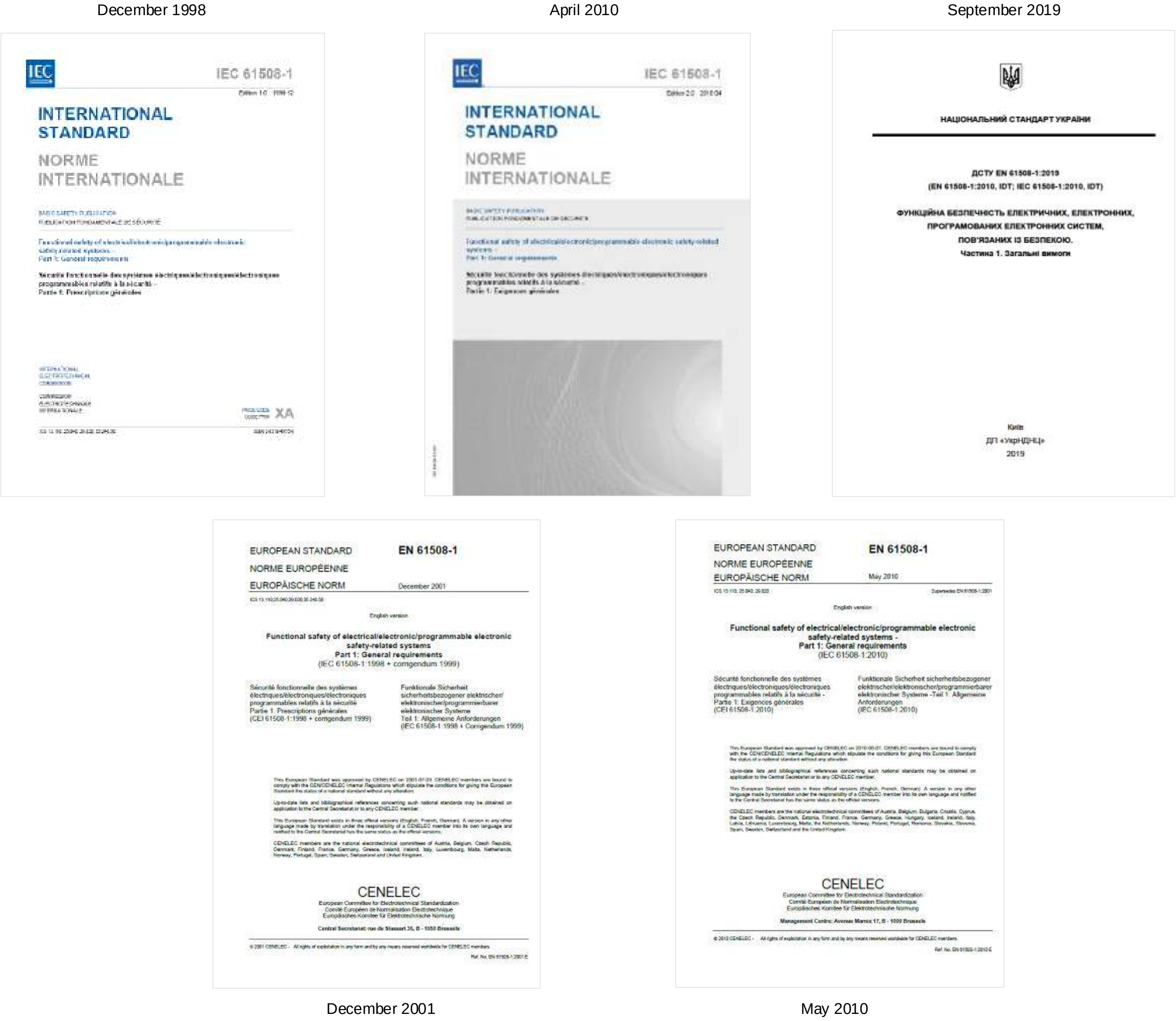

BS EN 61508-1:2010
BSI Standards Publication
Functional safety of electrical/electronic/programmable electronic safety-related systems
Part 1: General requirements
BSI
SOUTH AFRICAN NATIONAL STANDARD
SABS
GB
中华人民共和国国家标准

Figure 4.1 – IEC 61508 Geography



December 1998

IEC 61508-1

INTERNATIONAL STANDARD

NORME INTERNATIONALE

April 2010

IEC 61508-1

INTERNATIONAL STANDARD

NORME INTERNATIONALE

September 2019

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ДСТУ EN 61508-1:2019
(EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT)

ФУНКЦІЙНА БЕЗПЕЧНІСТЬ ЕЛЕКТРИЧНИХ, ЕЛЕКТРОННИХ,
ПРОГРАМОВАНИХ ЕЛЕКТРОННИХ СИСТЕМ,
ПОВ'ЯЗАНИХ ІЗ БЕЗПЕКОЮ.
Частина 1. Загальні вимоги

Київ
ДП «УкрНДНЦ»
2019

EUROPEAN STANDARD — EN 61508-1
NORME EUROPÉENNE
EUROPÄISCHE NORM — December 2001

English version

Functional safety of electrical/electronic/programmable electronic
safety-related systems
Part 1: General requirements
(IEC 61508-1:1998 + corrigendum 1999)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
Partie 1: Prescriptions générales
(CEI 61508-1:1998 + corrigendum 1999)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Teil 1: Allgemeine Anforderungen
(IEC 61508-1:1998 + Corrigendum 1999)

CENELEC

December 2001

EUROPEAN STANDARD — EN 61508-1
NORME EUROPÉENNE
EUROPÄISCHE NORM — May 2010

English version

Functional safety of electrical/electronic/programmable electronic
safety-related systems -
Part 1: General requirements
(IEC 61508-1:2010)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité -
Partie 1: Exigences générales
(CEI 61508-1:2010)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme -Teil 1: Allgemeine Anforderungen
(IEC 61508-1:2010)

CENELEC

May 2010

Figure 4.2 – IEC 61508 publication dates

As a safety metric IEC 61508 implements safety integrity level.

Safety integrity level (SIL) - a discrete level (one of the four possible) to determine the safety requirements to be applied to the safety functions performed by E/E/PE systems, where SIL 4 is the highest level, and SIL 1 is the lowest.

To establish the safety integrity level, it is necessary to calculate the failure rates and safe failure fraction.

Safe Failure Fraction (SFF) is a property of a safety-related element that is determined by the ratio of the average failure rates of safe and dangerous detected failures to safe and dangerous failures.

The calculation of the safe failure fraction involves the classification of failures (Figure 4). Failures that lead to loss of safety of the system and / or loss of its safe state are dangerous. Failures that lead to false shutdown of the output and stop of the controlled technological process (false positive) are considered to be safe).

The key definitions of terms and concepts used in the IEC 61508 standards series are considered in Figure 4.3.

Figure 4.3 – Key terms of IEC 61508

Failures classification according to the impact on safety and the detection possibility by diagnostic means in Figure 4.4.

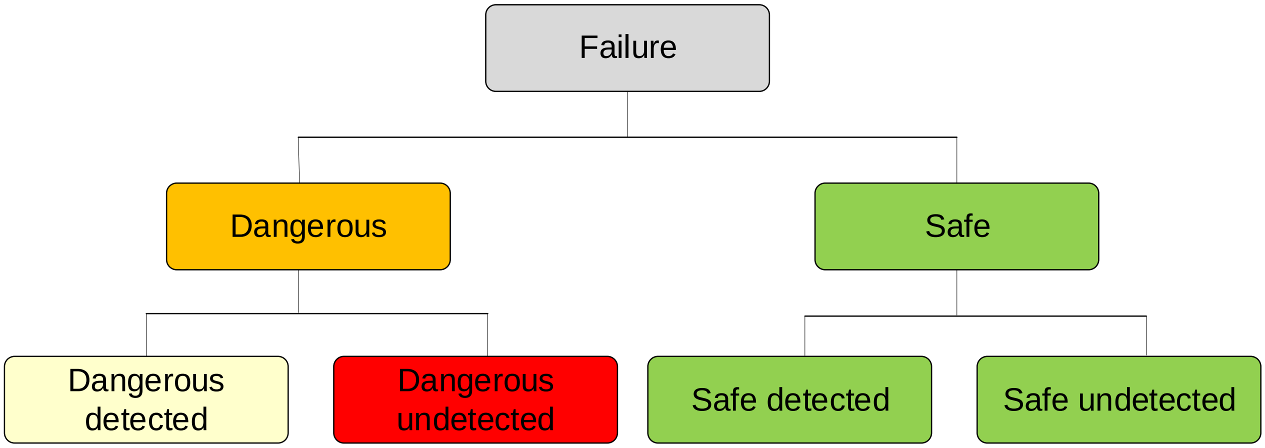


Figure 4.4 – Failures classification according to the impact on safety and the detection possibility by diagnostic means

Failures are also classified by nature (Fig. 4.5). Accidental hardware failures can be caused by overload (stress) or gradual aging of hardware materials, most often failures of this type are manifested in adverse operating conditions. Systematic failures may be due to defects introduced at the design stage of the system, or unforeseen interaction of the system with other systems, personnel, etc.

Diagnostic coverage in accordance with IEC 61508 is calculated based on the determination of the dangerous failures intensity. Diagnostic coverage is the ratio of the dangerous detected failures intensity to the dangerous failures intensity. Thus, the diagnostic coverage indicates the fraction of probability reducing for only dangerous failures by the built-in diagnostic tools.

The scheme for calculating the safe failure fraction is illustrated in Figure 4.6.

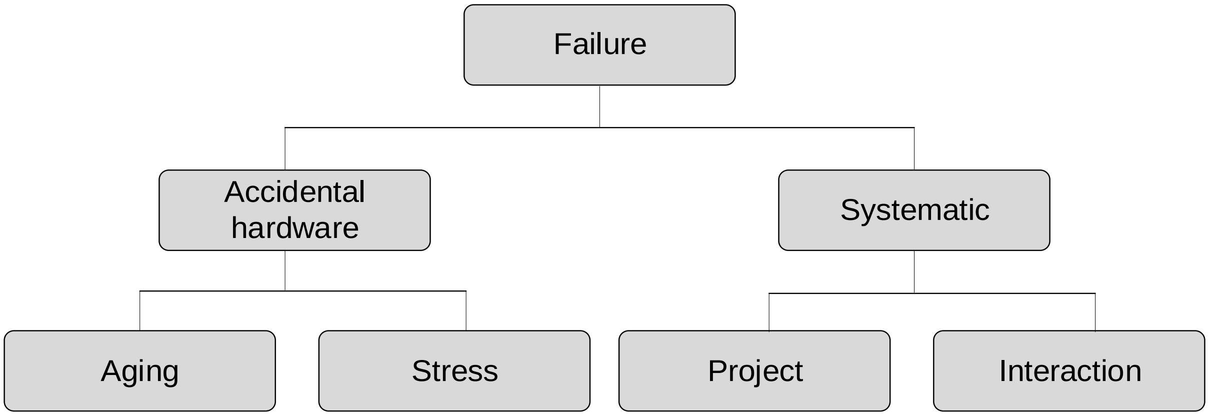
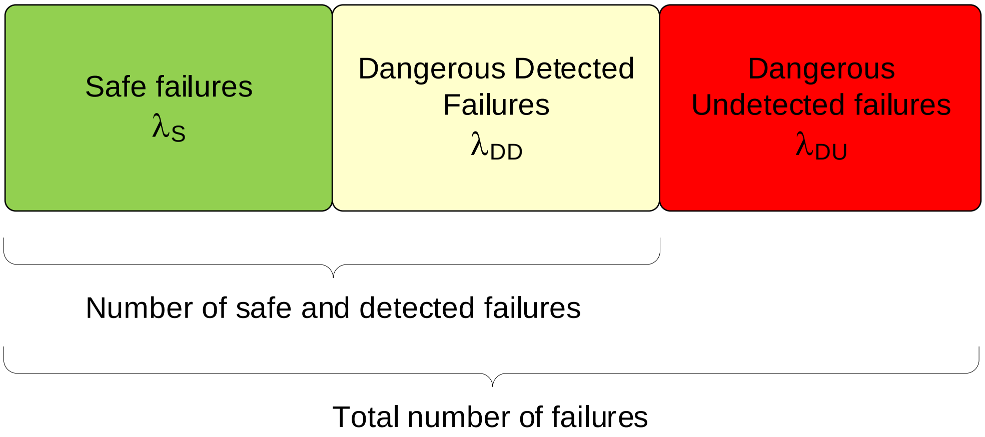


Figure 4.5 – Failure classification by nature


Safe failures
λ_S
Dangerous Detected Failures
λ_{DD}
Dangerous Undetected failures
λ_{DU}
Number of safe and detected failures
Total number of failures

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$$

Figure 4.6 – Safe failure fraction calculation

The IEC 61508 standard implies the need to develop safety functions to reduce the risk level down to acceptable one. Security functions are performed by a security-related system.

Acceptable risk is a risk that is acceptable in these circumstances on the basis of current society values. Residual risk is the risk that remains after the application of preventive measures (Fig. 4.7).

Safety function is a function that must be implemented by an E/E/PE safety-related system or by other risk mitigation means, designed to achieve or maintain a EUC safe state in a certain dangerous event.

Any hardware implementation of the safety function is a combination of a number of devices: software logic controllers, sensors, electromagnetic relays, actuators, etc. Each hardware features that ultimately make up a safety system has its own system reliability level, which can be estimated using the on-demand dangerous failure probability indicator.

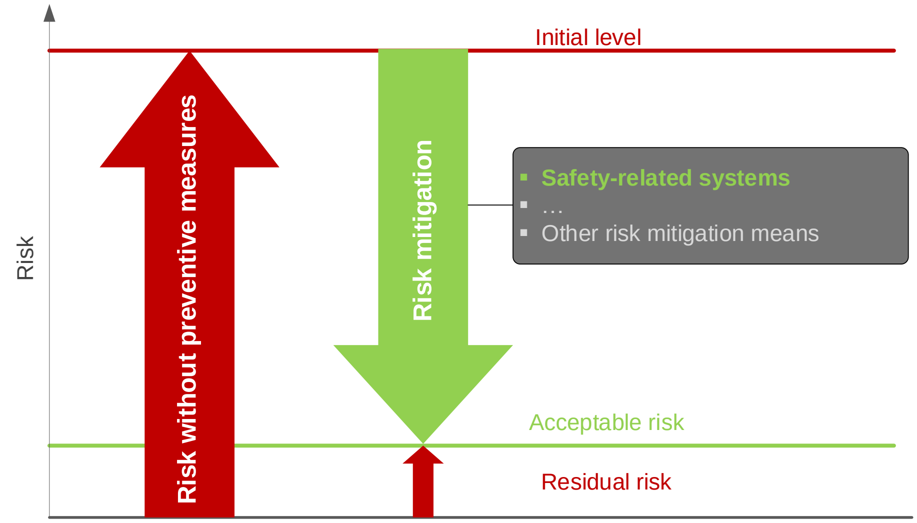


Figure 4.7 – Risk mitigation

Probability of dangerous on-demand failure is an unavailability of the safety-related E/E/PE system to perform a certain safety function when requested by the EUC or the EUC control system. From either quantitative or qualitative analysis using techniques recommended by IEC 61508, values of safety integrity level (SIL) are obtained. SIL could be treated as a requirement for the level of integrity required in the product architecture and as a measure of its fulfilment. SIL is defined based on a failure in time (FIT) rates for both low demand (Table 4.1) and high demand (Table 4.2) systems, which defines the operating life-cycle and in terms of the rate at which dangerous failures could be tolerated.

IEC 61508 determines four safety integrity levels (SIL) – SIL 1, SIL 2, SIL 3 та SIL 4.

Table 4.1 – Safety integrity levels – target failure measures for a safety function

Safety integrity level (SIL)	**Average probability of a dangerous failure on demand of the safety function (PFD$_{avg}$)**
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 4.2 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

The more dangerous the process or equipment, the higher the requirements for the reliability of safety functions are. SIL 4 meets the highest safety requirements and SIL 1 meets the lowest ones. For each level different failure probablilty stages are determined, which should not exceed the system's ability to perform security functions.

Qualitatively, SIL can be considered as a probable damage to personnel, enterprises and society in the event of a safety failure:

SIL 1 – insignificant protection of equipment and products is required;

SIL 2 – significant protection of equipment and products, protection from possible injuries of service personnel is required;

SIL 3 – protection of service personnel and society is required (non-catastrophic impact);

SIL 4 – protection from catastrophic impact on society is required.

The selection of the required SIL level for a specific production is a corporate decision, that should be based on a common sense and requirements for the safety level and acceptable risk level for the relevant industrial facility.

4.1.1.1 Standard Structure

IEC 61508 consists of 7 parts. Part 1 provides general requirements, part 4 contains terms and definitions. Parts 2 and 3 of the standard are key in the definition of the safety of a system. Part 2 focuses on hardware, that can be either programmable or not. Part 3 covers software topics in IEC 61508. Parts 6 and 7 give practical guidance on how to apply the processes in parts 2 and 3. Part 5 provides examples of methods for the determination of safety integrity levels

Overall safety lifecycle according to IEC 61508 shown in Figure 4.8 provides general workflow from the high-level requirements in the scope and concept phases to the hazard and risk analysis.

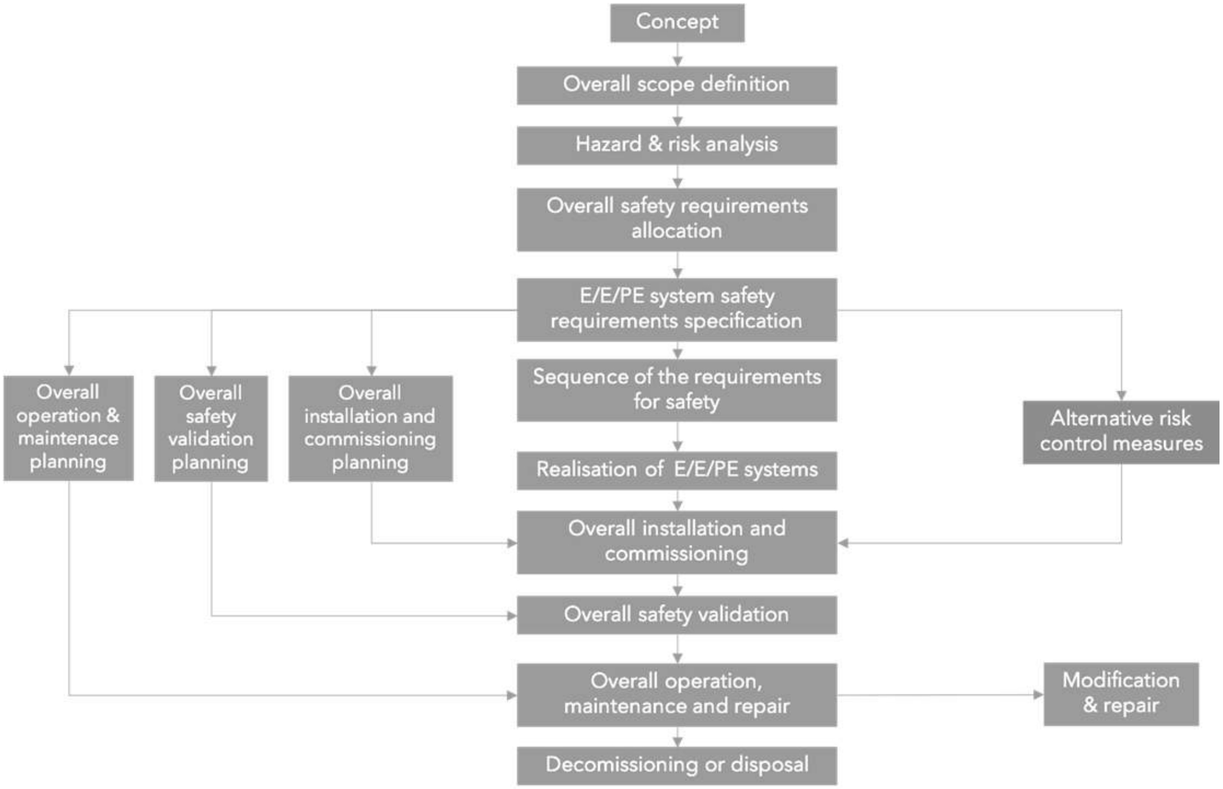

Concept
Overall scope definition
Hazard & risk analysis
Overall safety requirements allocation
E/E/PE system safety requirements specification
Overall operation & maintenace planning
Overall safety validation planning
Overall installation and commissioning planning
Sequence of the requirements for safety
Alternative risk control measures
Realisation of E/E/PE systems
Overall installation and commissioning
Overall safety validation
Overall operation, maintenance and repair
Modification & repair
Decomissioning or disposal

Figure 4.8 – Overall safety lifecycle according to IEC 61508

4.1.1.3 Safety Lifecycle

IEC 61508 represents the safety lifecycle (Figure 4.9). Each stage of the lifecycle lists the tasks and requirements that must be implemented.

For example, the tasks of the stage "Overall scope definition" are as follows:

– defining the scope of the EUC and the EUC control system;

– establishing the scope of hazard and risk analysis (eg process hazards, environmental hazards, etc).

The requirements for this stage are formulated as follows:

– EUC and EUC control system scope should be defined to include all equipment and systems (including people if appropriate) that are associated with relevant hazards and hazardous events;

– physical equipment, including the EUC and the EUC control system to be included in the scope of the hazard and risk analysis, should be defined;

– external events that will be taken into account in the analysis of hazards and risks must be defined;

– equipment and systems related to hazards and hazardous events must be defined;

– the types of initial events to be considered (e.g. component failures, procedural defects, human errors, dependent failure mechanisms that may cause dangerous events) should be defined;

– the information and results obtained in the above sub-paragraphs must be documented.

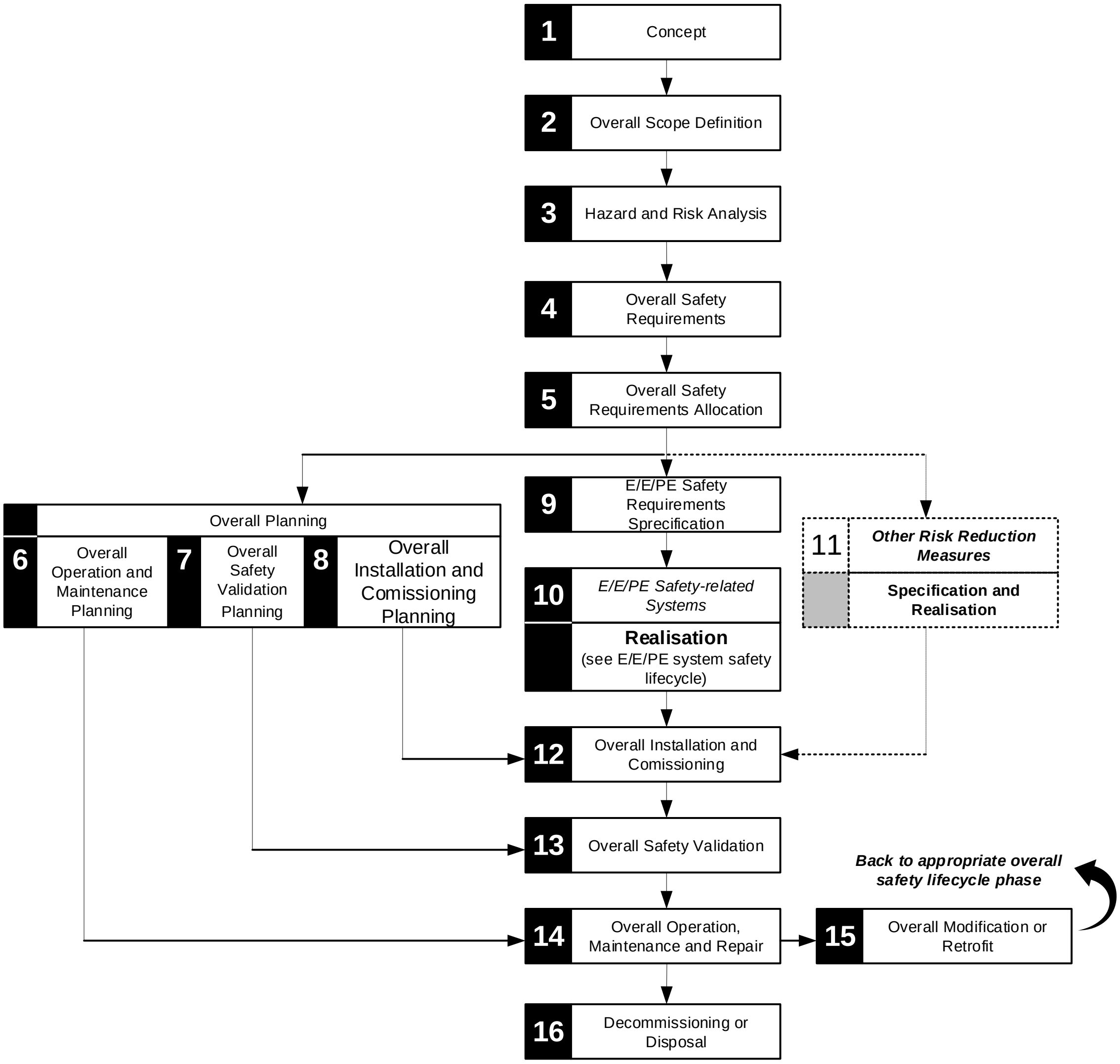

1
Concept
2
Overall Scope Definition
3
Hazard and Risk Analysis
4
Overall Safety Requirements
5
Overall Safety Requirements Allocation
Overall Planning
6
Overall Operation and Maintenance Planning
7
Overall Safety Validation Planning
8
Overall Installation and Comissioning Planning
9
E/E/PE Safety Requirements Sprecification
10
E/E/PE Safety-related Systems
Realisation
(see E/E/PE system safety lifecycle)
11
Other Risk Reduction Measures
Specification and Realisation
12
Overall Installation and Comissioning
13
Overall Safety Validation
Back to appropriate overall safety lifecycle phase
14
Overall Operation, Maintenance and Repair
15
Overall Modification or Retrofit
16
Decommissioning or Disposal

Figure 4.9 – Overall safety lifecycle

The peculiarity of the safety lifecycle is that at each stage it is necessary to analyze the hazards and risks. The implementation of such a requirement is possible only if careful planning, implementation, consistent monitoring and documentation of all processes occurring during the full safety lifecycle.

4.1.4 Target Audience

The advantages of using the 61508 standards series are the transparent proof of the required safety level and justification of using equipment or systems to solve critical problems possibility.

The target audience of the standard is:

- product used in hazardous industries (components of industrial systems) developers;
- integrators;
- industrial systems developers.

4.1.5 Application: practical steps

The following steps are required to assess safety:

1. Hazardous processes identification. The number of such processes significantly depends on production, but, as a rule, it is small. For example, basic operations of control modes that do not include safety functions are not considered.

2. Safety integrity level requirements identification. For each potentially hazardous process, anassessment of hazard degree and the damage level resulting from the failure is made. For this, IEC 61508 offers several risk-oriented approaches / tools, such as a risk graph or a criticality matrix. Depending on the danger degree and the probability of its occurrence, it is concluded whether the protection process requires a safety function, and which safety integrity level of such a function should be provided.

3. Necessary elements selection. To implement the security function with the safety integrity level, the necessary elements are selected. To simplify this step, lately manufacturers indicate the compliance of their products with different SIL-levels.

4. SIL requirements check. By analyzing the safety performance of the used devices, it is necessary to check whether the safety function ***provides*** the required SIL level. If not, then additional risk mitigation measures should be added (Fig. 4.10). The RadICS platform, developed by PJSC Radiy (Kropyvnytskyi, Ukraine), is a set of different types of electronic modules that provide the possibility of integration of various automated control systems for nuclear power plants on their basis. The RadICS platform is certified in accordance with the requirements of the international standard IEC 61508: 2010 (parts 1-7) and has a SIL3 category for single-channel architecture. Besides, this platform has been certified by US Nuclear Regulatory Committee.

4.1.6 Final Notes

IEC 61508 “Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems” is the umbrella functional safety standard used as source and basic reference for industry-specific standards. It provides Safety Integrity Level (SIL) and generic compliance tips. Main idea is to reduce risk to acceptable levels by implementing required activities during different lifecycle stages.

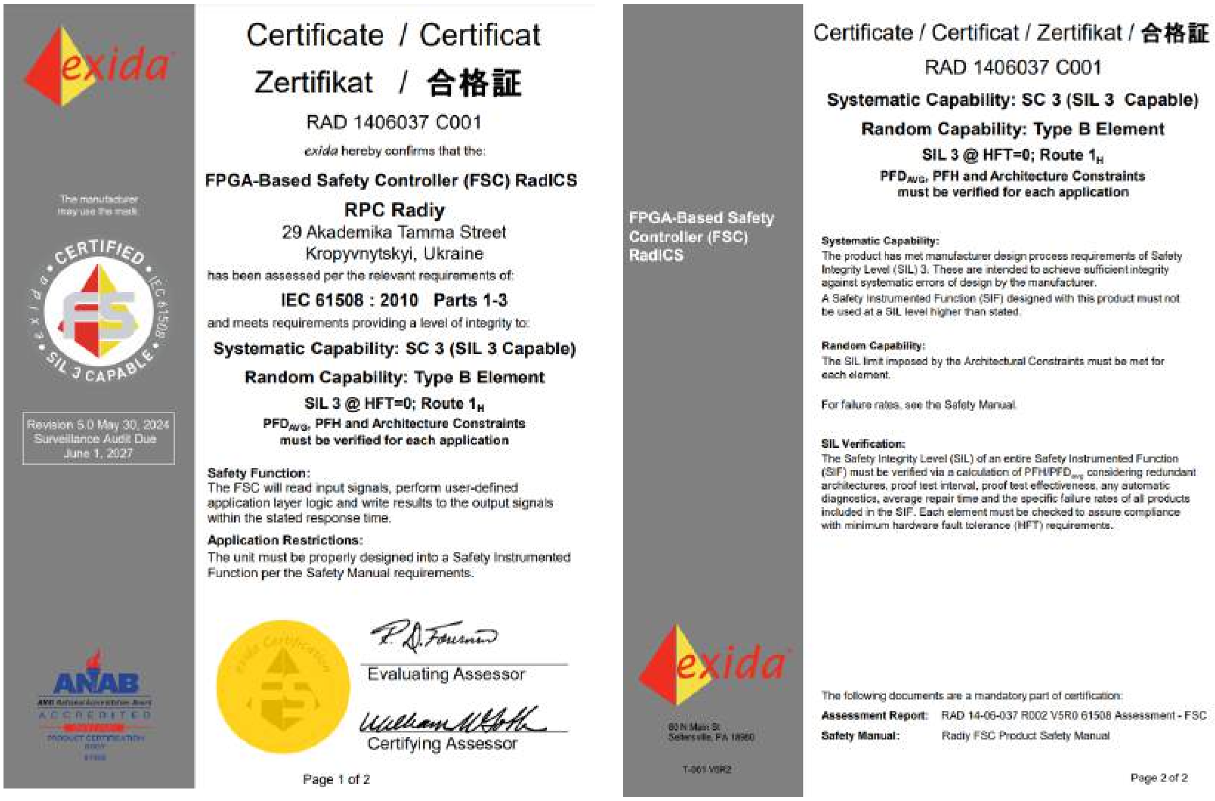
This standard applies to critical systems in different branches of industry, referring in such a manner to a wide class of systems, including the following types of components:

- electrical (E) (e.g., electromechanical devices);
- electronic (E) (e.g., nonprogrammable transistor devices);
- programmable (PE) (e.g., microprocessors, microcontrollers, programmable logic controllers, programmable platforms).

The definition of “functional safety” given in IEC 61508 states that it is a part of the overall safety relating to the equipment under control (EUC) and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures. EUC could be equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

In IEC 61508 it is emphasized that the EUC control system is separate and distinct from the EUC, and actually the main attention is paid to computer systems.

IEC 61508 requires that functional safety assessment is being performed for all parts of E/E/PE system at all lifecycle stages. This standard is a basic: it is not only used as an independent one in some branches of industry, but also forms a ground for development of branch standards like IEC 61511. Also, it is often the standard of choice if no other industry specific reference standard exists.



exida

The manufacturer may use the mark

CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida

Revision 5.0 May 30, 2024
Surveillance Audit Due
June 1, 2027

ANAB ACCREDITED PRODUCT CERTIFICATION

Certificate / Certificat
Zertifikat / 合格証

RAD 1406037 C001

exida hereby confirms that the:

FPGA-Based Safety Controller (FSC) RadICS

RPC Radiy
29 Akademika Tamma Street
Kropyvnytskyi, Ukraine

has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-3

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT=0; Route 1_H

PFD_{AVG}, PFH and Architecture Constraints must be verified for each application

Safety Function:
The FSC will read input signals, perform user-defined application layer logic and write results to the output signals within the stated response time.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

FPGA-Based Safety Controller (FSC) RadICS

exida
80 N Main St
Sellersville, PA 18960

T-001 V5R2

Certificate / Certificat / Zertifikat / 合格証

RAD 1406037 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT=0; Route 1_H

PFD_{AVG}, PFH and Architecture Constraints must be verified for each application

Systematic Capability:
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:
The SIL limit imposed by the Architectural Constraints must be met for each element.

For failure rates, see the Safety Manual.

SIL Verification:
The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report:	RAD 14-06-037 R002 V5R0 61508 Assessment - FSC
Safety Manual:	Radiy FSC Product Safety Manual

Page 2 of 2

Figure 4.10 – Certificate of SIL compliance of the RadICS platform (PJSC "Radiy", Ukraine)

One of the most essential parts of IEC 61508 are metrics that it provides: failure rates classified as safe/dangerous, detected/undetected, diagnostic coverage and safe failure fraction. Not all failures in a system will lead to a hazardous event, therefore such failures are treated as safe failures. Failures that result in a hazardous or potentially hazardous event are treated as dangerous failures. Diagnostic coverage provides assessment of whether failures are detectable or not.

4.1.2 Standard IEC 61511

IEC 61511 provides a framework for managing instrumented safety systems in the process industry sector in general, covering oil and gas in particular.

The first edition of IEC 61511 issued in 2003 defined the requirements associated with the use of safety integrity level (SIL) 4 and the limitations of going beyond this integrity level. It described the avoidance of such high integrity level requirements where reasonable practicable. Edition 2 of IEC 61511 issued in 2016 provides guidance on the techniques that can be used in order to avoid the use of high integrity level safety systems. In particular, it recommends a reconsideration of the application (e.g., process, other protection layers) to determine if any of the risk parameters can be modified so that requirement of going beyond SIL4 level is avoided, considering whether:

- the process or vessels/pipe work can be modified to remove or reduce hazards at the source;
- additional safety-related systems or other risk reduction means, not based on instrumentation, can be introduced;
- the severity of the consequence can be reduced, e.g., reducing the amount of hazardous material;
- the likelihood of the specified consequence can be reduced e.g., reducing the likelihood of the initiating source of the hazardous event.

IEC 61511 is mainly a guideline on how to use and develop a process safety application. Manufacturers and suppliers of safety related devices follow the IEC 61508 standard, while safety instrumented system designers, integrators and end users follow IEC 61511.

4.1.3 Other Standards under IEC 61508 Umbrella

Within automotive systems, the sector-specific standard ISO 26262 is used. EN 50129 is a European standard for safety related software in railway applications and is also derived from IEC 61508 (Fig. 4.11). The international standard IEC 62304 is a standard specifying life cycle requirements for the development of medical software and software within medical devices.

4.2 Functional Safety Audit

According to IEC 61508, Part 1, Clause 8.2.7, a functional safety assessment shall include assessment of the evidence that functional safety audit has been carried out. According to IEC 61511, Part 1, Clause 5.2.6.2.1, the purpose of such audit is to review information documents and records to determine whether the functional safety management system is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.

4.2.1 Functional Safety Audit Strategy

Set of documents is being audited against the functional safety management requirements of IEC 61508. This is done by a review of the completeness of the related requirements and then a spot inspection of certain requirements. The safety case is used to demonstrate the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed audit evaluates the compliance of the processes, procedures and techniques with IEC 61508.

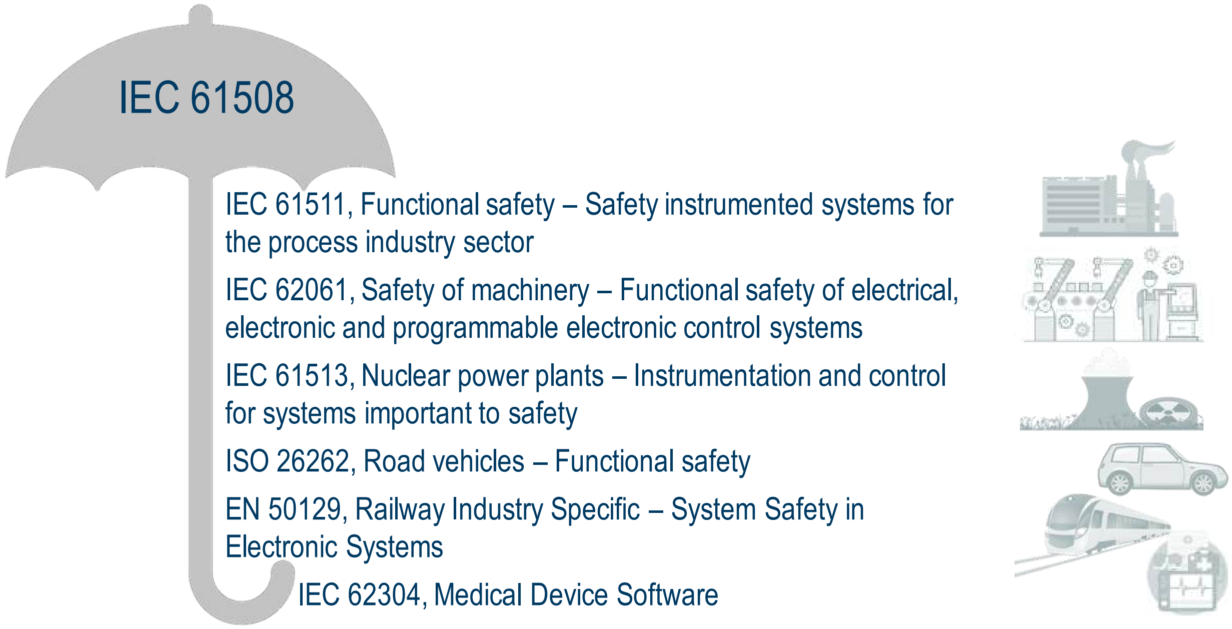

IEC 61508
IEC 61511, Functional safety – Safety instrumented systems for the process industry sector
IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems
IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety
ISO 26262, Road vehicles – Functional safety
EN 50129, Railway Industry Specific – System Safety in Electronic Systems
IEC 62304, Medical Device Software

Figure 4.11 – Standards derived from IEC 61508

4.2.2 Functional Safety Audit Program

The following objectives are subject to FS audit:

- Planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- System and hardware related V&V activities including documentation and verification
  - Integration and fault insertion test strategy
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

4.2.3 Functional Safety Audit Plan, Reporting Processes and Follow-up Mechanisms

Functional safety audit plan sets requirements for the functional safety management audits as the verification that the design teams are following the functional safety management plan and its derived plans and procedures. These audits can be performed periodically and also on the basis of the stage the design has reached.

The purpose of functional safety audits is to:

- detect problems in following the functional safety management plan early in the process while they are correctable at minimal cost;
- maximize the probability that the functional safety assessor will conclude that the functional safety management plan has been followed;
- uncover improvements in how the work could be done to make these processes more efficient and more likely to prevent design faults;
- ensure that the continuation of the design and development processes that led to a certified product.

4.3 Functional Safety Assessment

Functional safety assessment investigates the compliance with the requirements of the IEC 61508 standard, of the processes, procedures and techniques, used in product development. Normative references are IEC 61508, Part 1, Clause 8 and IEC 61511, Part 1, Clause 5.2.6

4.3.1 Functional Safety Assessment Scope

Functional Safety Assessments (FSAs) are independent assessments that cover the following process issues to ensure that the development process meets the requirements of IEC 61508:

- sufficiency of the functional safety management plan to address all the process requirements of IEC 61508;
- compliance with the functional safety management plan during the development process of the product.

The results of functional safety assessment used to confirm user confidence that sufficient attention has been given to systematic failures during the development process of the product

4.3.2 Functional Safety Assessment Plan

The following FSA planning items are considered:

- The scope of the FSA;
- Who is to participate in the FSA;
- The skills, responsibilities and authorities of the FSA team;
- The information that will be generated as a result of any FSA activity;

- The identity of any other safety bodies involved in the FSA;
- The resources required to complete the FSA activity;
- The level of independence of the FSA team;
- The methods by which the FSA will be revalidated after modifications

Normative reference is IEC 61511, Part 1, Clause 5.2.6.1.3

4.3.3 Techniques and tools

For safety and reliability assessment techniques, Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD) and Markov models are of particular importance.

4.3.3.1 Reliability Block Diagram

A reliability block diagram (RBD) is a graphical representation of a system's reliability. It shows the logical interconnection of (functioning) components required for successful operation of the system.

RBD allows performing system reliability (no-failure operation) calculation basing on known reliability of its elements.

Probability of no-failure operation in case of series reliability block diagram can be calculated as product of probabilities of no-failure operation of its elements:

$$P_{sys}(t) = \prod_{k=1}^{n} p_k(t) \quad , \tag{4.1}$$

where p_k – probability of no-failure operation of k -th element, n -number of elements in system.

The relation between failure rate and probability of no-failure operation is the following:

$$p(t_0, t) = e^{-\int_{t_0}^{t} \lambda(t)dt} \quad , \tag{4.2}$$

Basing on formulas (1) and (2) the following expression for failure rate can be obtained:

$$\lambda_{sys}(t) = \sum_{k=1}^{n} \lambda_k(t) \, , \tag{4.3}$$

where λ_k – failure rate of k -th element, n -number of elements in system.

4.3.3.2 Fault Tree Analysis

Fault tree analysis is a method to model the chain of causes that lead to an undesired event or effect.

An undesired event is chosen as the top event, e.g., a function event from the event tree. Situations or combination of events that could lead to the top event is connected by logical gates. These second level situations are in turn evaluated and their possible causes determined and connected by logical gates. In this way a tree is built between the top event and a number of basic events and every possible sequence that result in a failing top node is identified.

The basic events are not developed further, they are instead assigned appropriate probability measure that describe their failure probability.

FTA analysis provides both qualitative and quantitative results. Qualitative analysis can be obtained from identification of cut set. While the quantitative analysis of the calculation of failure probability of the system based on the failure probability of each component that compiled it. The qualitative analysis of FTA is based on the cut set that can be easily seen based on the number of components that compose them. Cut set that is only compiled by one component means that if that component failure, then will cause a certain failure on the entire system. While the cut set composed of two or more components implies that there is a redundancy so that the failure of one of them will only increase the failure probability but will not cause a failure of the entire system. Cut set that constructed by many components mean that they have better redundancy. While the quantitative analysis on the FTA is done by calculating the failure probability of the system and/or cut set based on the failure probability of each component by following Boolean algebra rules.

4.3.3.3 Failure Modes and Effects Analysis

FMEA (Failure Modes and Effects Analysis) is a structured, qualitative analysis of a system, subsystem, module, design or function, in order to identify potential failure modes, their causes and their effects on (system) operation, with the objective of improving the design. FMEA is widely used as reliability analysis technique in the initial stage of system development. There are some basic consent of FMEA, such as; how each part can conceivably fail, what mechanisms might produce those modes of failure, what is the effects of the failures, is the failure in the safe or unsafe condition, how the failure can be detected, and what inherent provisions are provided in the design to compensate for the failure. FMEA analysis is done through weighting and ranking. At the end of the analysis will be obtained which component has the greatest weight that means require greater attention and which components have a low weight which means no need to be prioritised.

4.3.3.4 Markov Models

Markov models provide memoryless modelling and a continuous time stochastic process. There are at less four kinds of Markov models used in different situations depending on sequential state observation and adjustment of the system on the observation, such as Markov chain, Hidden Markov model, Markov decision process, Partially observable Markov decision process. Those Markov models have been used widely for mechanical modelling, especially for reliability modelling. Markov models also very popular for maintenance purposes especially modelling for the single failure of a component. Markov models are very powerful because it can illustrate the failure of the process in detail to present a good quantitative analysis.

4.4 Product development safety life cycle

4.4.1 Development process

The following stages are described: product architecture design, hardware and software design, functional and integration testing.

According to safety life cycle, product design is typically partitioned into subsystems, and interfaces between subsystems are to be clearly defined and documented. The Product Architecture Design shall clearly identify the SIL capability of all components, including software components, in the design. If a component has a lower SIL capability than that associated with the safety function(s), then sufficient independence between the components are to be documented in a Failure Analysis. The Product Architecture Design shall describe the behavior of the device when a fault is detected is to annunciate the detected fault through the output interface.

During hardware architecture design, design reviews are to be used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are to be incorporated into the design. The design shall be reviewed by Failure Modes, Effects and Diagnostics Analysis (FMEDA). Required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test, are to be defined.

The Software Architecture Design shall contain a description of the software architecture. The design is typically partitioned into new, existing and/or reused components and modules, which are identified as such. A software criticality analysis and HAZOP is usually performed to list all components along with their criticality and their required systematic capability. Common cause failures are usually identified in the Software HAZOP as failures of one component that could affect an independent component and defensive measures are listed as safety measures. Semi-formal design notation like state/transition diagrams, sequence diagrams etc., is typically used in the design.

The Software Architecture Design shall describe what techniques are implemented to detect software faults. Program flow monitoring, data flow monitoring and CRCs on serial communications data are the examples of such techniques. The resulting behavior of the device due to a detected fault shall be specified.

Software verification could be accomplished through various means:

- review of Software Architecture Design;
- creation and execution of module tests;
- measuring, documenting and verifying of structural test coverage to ensure all code is tested at least once;
- inspection of all safety related Source Code Modules;
- creation of code review reports to ensure non-conformances are recorded and followed up;
- module testing for all safety related modules with indication whether tests pass or fail;

- static code analysis tools and code reviews to ensure that coding rules, documented in the coding standard, are followed;
- integration testing by running validation tests in development, using prototype hardware, prior to releasing code to quality assurance for final integration and validation with release candidate hardware;
- use of test management tools to manage the module and/or integration testing process.

4.4.2 Supporting processes

Importance of support processes is highlighted, including action tracking, requirements tracing, training, documentation etc.

Projects in the chemical and energy carriers industries typically generate a large number of recommendations from not only safety assessment but also multiple different technical, commercial, cyber security, and other studies, to which must be added actions and commitments arising from regulatory, planning approval, and other meetings. As a result, the project needs a system to prioritize, document decisions, and track progress of each recommendation and action. Action tracking systems are used to support solving of these issues.

Action tracking systems ensure that corrective actions are completed in a timely manner. The goal of action tracking is to ensure that all actions arose during implementation of project design activities are assigned to a specific person for action and are tracked to resolution. Corrective actions shall not be closed without effective resolution and employee feedback/review.

The following documents of FSC project may identified actions to be tracked and resolved:

- document review reports;
- compliance check lists;
- audits reports;
- test and analysis reports.

As for requirements tracing, it is required to:

- ensure that all requirements are implemented;
- ensure that all requirements are tested;
- ensure that only required features and functions are implemented.

IEC 61508 and derived standards require tracing of product requirements, while they typically do not require tracing of process or procedural requirements. Requirements tracing shall be used as a generic verification method, applicable to all the documents associated with tracing requirements.

Training is required to ensure necessary competence of engineers involved into safety related design and V&V decisions, such as:

- project manager;

- product manager;
- product safety system architect;
- project and functional safety coordinator;
- hardware and electronic design development manager;
- test team leader;
- product QA manager;
- product documentation manager;
- product validation and qualification manager;
- product verification manager.

4.4.3 Management of product failures

Random failures of a product are controlled by hardware safety integrity. Such failures occur at a reasonably constant rate and are completely independent of each other. They are not preventable and cannot be avoided or eliminated, but can be reduced by provided risk reduction measures.

Predictable systematic failures of a product are controlled by systematic safety integrity. Such failures could result from errors and shortcomings in the design, manufacture, installation, operation, maintenance and modification of the system.

4.5 Safety Manual

According to Annex D of IEC 61508-2, the purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of IEC 61508.

For every compliant item, the safety manual shall contain:

- a functional specification of the functions capable of being performed;
- identification of the hardware and/or software configuration of the compliant item to enable configuration management of the E/E/PE safety-related system;
- constraints on the use of the compliant item and/or assumptions on which analysis of the behaviour or failure rates of the item are based.
- For every function, the safety manual shall contain:
- the failure modes of the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the function and that are not detected by diagnostics internal to the compliant item;
- the failure modes of the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the function and that are detected by diagnostics internal to the compliant item;
- the failure modes of the diagnostics, internal to the compliant item (in terms of the behaviour of its outputs), due to random hardware failures, that result in a failure of the diagnostics to detect failures of the function.
- the hardware fault tolerance;

- the classification as type A or type B of that part of the compliant item that provides the function.

For every failure mode, an estimated failure rate must be provided. Also, the diagnostic test interval and the outputs of the compliant item initiated by the internal diagnostics are to be also specified for relevant failure modes.

For every function of the compliant item that is liable to systematic failure, the manual shall contain:

- the systematic capability of the compliant item or that part of the element that provides the function;
- any instructions or constraints relating to the application of the compliant item, relevant to the function, that should be observed in order to prevent systematic failures of the compliant item.

Established company safety culture should be treated as an investment in improving level of talent and expertise of company's employees. Their employee gains personal knowledge of the subject matter and brings that knowledge back to the company, confirming that safety is important.

4.6 Best practices

4.6.1 FPGA technology for safety/security critical systems

In FPGA-based systems, a high-level design is implemented with the configurable logic blocks made available by a given FPGA chip. In order to attain a realistic model and satisfactory accuracy of the analysis, it is possible to represent FPGA-based system at this implementation level. Also, different types of models and failure distribution can be considered. Furthermore, combinations of different assessment methods so as to increase assessment accuracy are discussed and presented.

There are two lines in contemporary programmable logic arrays: Complex Programmable Logic Devices (CPLD) and FPGA. CPLDs are a continuation of programmable matrix logic line, whereas FPGAs continue basic matrix crystal line. The desire to combine the advantages of both line led to development of combined architecture VLSIs. Still, all contemporary FPGAs possess such architecture.

CPLD architecture has its origins in Programmable Arrays Logic (PAL) preceded by Programmable Logic Arrays (PLA) and from Generic Arrays Logic (GAL). Its functional unit consists of microcells, each of them performing some combinatory and/or register functions. Functional logic within the block is a matrix of logic products (terms). A subset of terms may be accessed by each macrocell via term distribution diagram. Switch matrix commutates the signals coming from outputs of the functional unit and I/O unit. As distinct from FPGA (segmented connections), CPLDs have a continuous system of connections (completely commuted connections).

FPGA architecture topologically originates from channeled Gates Arrays (GA). In FPGA internal area a set of configurable logic units is disposed in a regular order with routing channels there between and I/O units at the periphery. Transistor couples, logic gates NAND, NOR (Simple Logic Cell), multiplexer-based logic modules, logic modules based on programmable Look-Up Tables (LUT) are used as configurable logic blocks. All those have segmented architecture of internal connections.

The application of FPGA technology could provide some benefits because of design simplicity and transparency. Unlike in microprocessor-based digital I&C systems, the safety function applications implemented by FPGAs are executed without running any system software or operating systems. This reduces the vulnerability of the designed system to cyber attacks or malicious acts. Simplicity gives a faster and more deterministic performance; the ability to execute logic functions and control algorithms in a parallel mode provides fast response times with known and fixed time delays. Similarly, the transparent and simple FPGA design allows the complexity of the verification and validation, and implementation processes to be reduced, making the end-product more reliable and error-free. Also, separation of FPGA functions can provide isolation between safety and non-safety systems maintaining functional independence.

Also, there are two important issues at the system's operating lifecycle: licensing and obsolescence. The licensing process of FPGA-based safety systems may be easier, due to the simplicity and transparency of the system's architecture and its design process. Evidence of meeting licensing requirements, such as independency, separation, redundancy and diversity, can be provided in an easier and more convincing way. As for obsolescence, FPGA-based applications have more resilience due to the portability of the HDL code between various versions of FPGA chips produced by the same or different manufacturers.

4.6.2 FPGA platform RadICS based decisions for safety critical I&C system

The FPGA-based platform RadICS is a logic based controller that provides a means for users to create safety function logic which the controller executes. The logic is based on existing function blocks, created by vendor, and logic created by the user, which is converted into an image appropriate for programming the FPGA device in the controller hardware. The device cannot be programmed while in operation as a safety device.

The basic configuration for the RadICS platform consists of an instrument rack containing a logic module, as well as other modules of any combinations of module types (for example, input/output (I/O) and fibre-optic communication modules). The basic set of I/O modules consists of analogue and digital input, and digital output modules. There are also special-purpose I/O boards designed for specific field detectors and devices, such as resistance temperature detectors, thermocouples, ultra-low-voltage AI boards for neutronic instrumentation, actuator controller modules, and fibre-optic communication modules to expand the I&C system to multiple chassis. It is also possible to provide interchannel communications between two, three or four channels via fibre-optic communications directly between logic modules.The logic modules gather input data from input modules, execute user-specific logic and update the value driving the output modules. Diagnostic modules gather diagnostic and general health information from all I/O modules and the logic module. The I/O modules provide interfaces with field devices (such as sensors, transmitters and actuators). The functionality of each module is driven by the logic implemented in the onboard FPGA(s).

The backplane of the RadICS platform provides external interfaces to power supply, process I/Os, communication links, and local inputs and indicators. The internal backplane interfaces provide connections to the modules that are installed within the chassis by means of a dedicated, isolated, point-to-point 'lowvoltage differential signalling' interface.

As for application development, the Radiy Product Configuration Toolset is used to configure the functional block library for the given NPP-specific applications. RadICS-based I&C systems also provide extensive online, self-surveillance and diagnostics at various levels, including self-diagnostic and defensive coding of electronic design components; self-monitoring of the FPGA circuit; and monitoring the performance of FPGA support circuits, I/O modules, communications units and power supplies.

The diagnostic functions are separated from the logic functions and are executed independently in a parallel mode. In case of fault detection, the diagnostic module provides a means to place the system in a safe state, defined for the detected fault.

Safety Life Cycle (LC) of the RadICS Platform is presented on Figure 4.12.

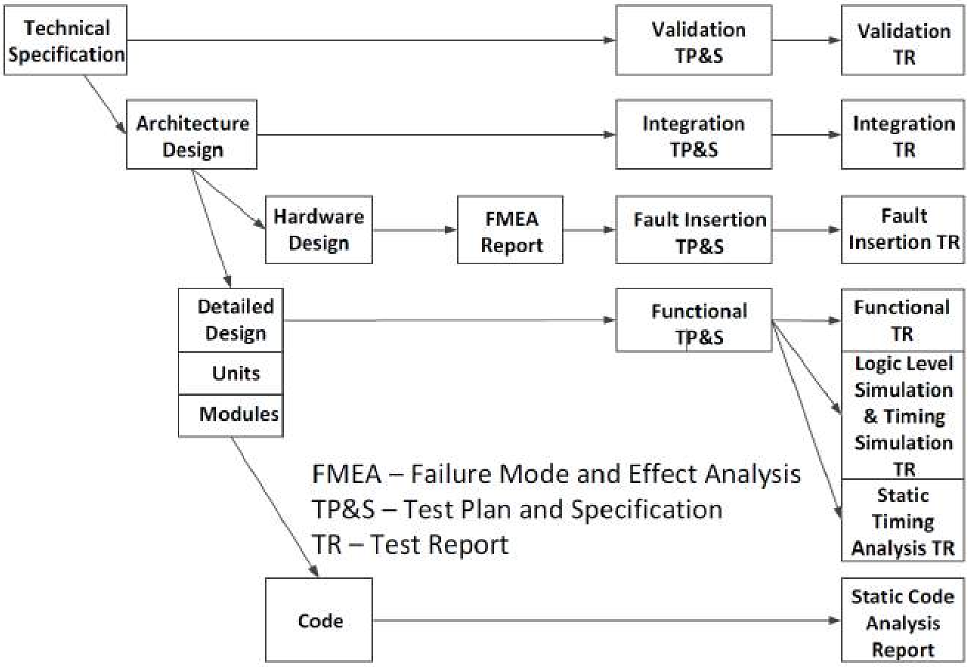


Figure 4.12 – RadICS Platform Safety Lifecycle

The RadICS Platform lifecycle implements specific stages of FPGA design development and verification. Specific technique of fault insertion testing has been performed for both hardware and software parts. This lifecycle complies with requirements traceability concept which requested the following:

- Every requirement has a child (either a lower level requirement or a solution);
- Every lower level requirement or solution has a higher level requirement (and opposite, an orphan represents unjustified functionality);
- Every requirement has been tested.

RadICS Platform that was certified by exida as an IEC 61508:2010 SIL 3 capable digital I&C platform intended for nuclear safety applications. RadICS achieved the SIL 3 rating in a single channel configuration. The redundancy typical of nuclear safety systems provides an additional level of risk reduction.

4.7 Implementation of Functional Safety Management System

Safety management is very similar to the classic Project Management. Consider a typical sequence of actions (Figure 4.13).

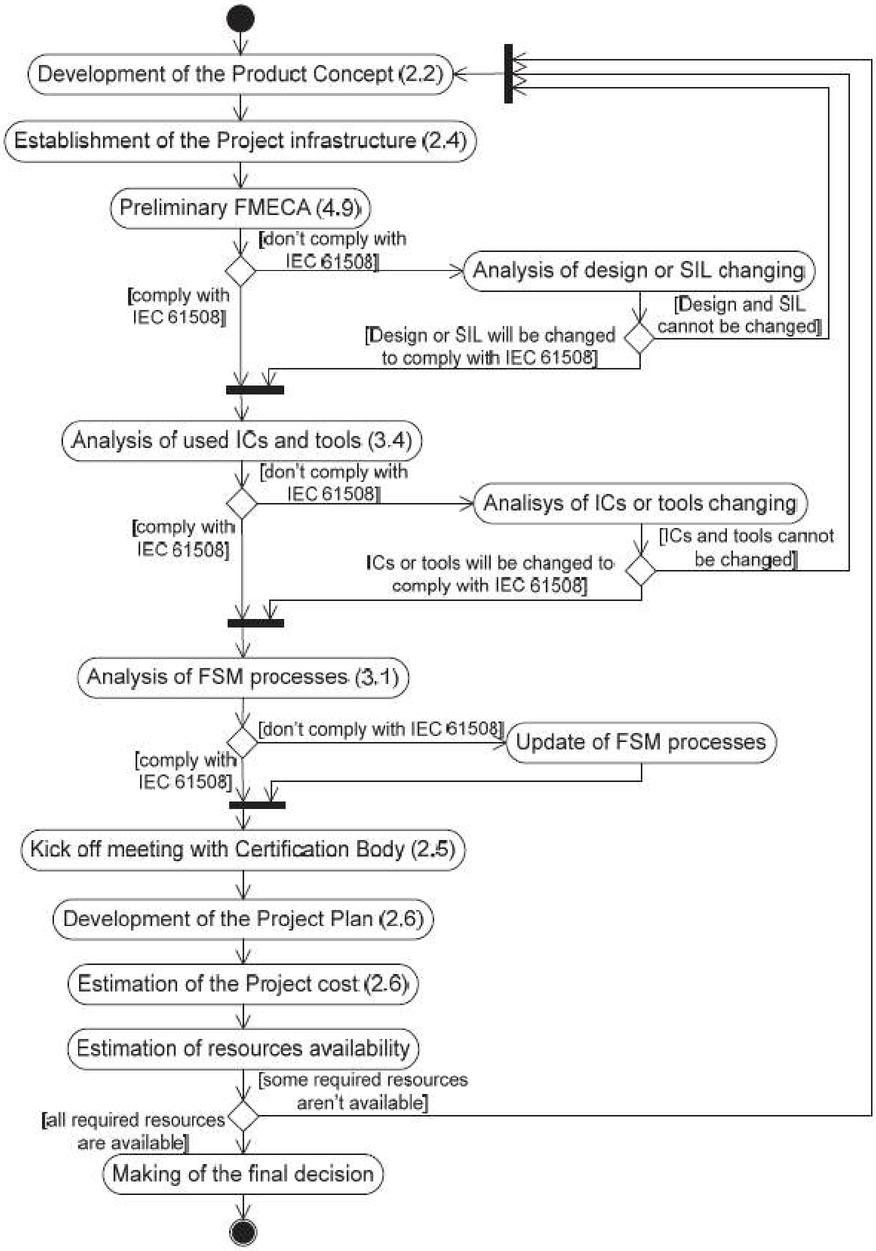

Development of the Product Concept (2.2)
Establishment of the Project infrastructure (2.4)
Preliminary FMECA (4.9)
[don't comply with IEC 61508]
Analysis of design or SIL changing
[comply with IEC 61508]
[Design and SIL cannot be changed]
[Design or SIL will be changed to comply with IEC 61508]
Analysis of used ICs and tools (3.4)
[don't comply with IEC 61508]
Analisys of ICs or tools changing
[comply with IEC 61508]
[ICs and tools cannot be changed]
ICs or tools will be changed to comply with IEC 61508]
Analysis of FSM processes (3.1)
[don't comply with IEC 61508]
Update of FSM processes
[comply with IEC 61508]
Kick off meeting with Certification Body (2.5)
Development of the Project Plan (2.6)
Estimation of the Project cost (2.6)
Estimation of resources availability
[some required resources aren't available]
[all required resources are available]
Making of the final decision

Figure 4.13 – Ensuring the compliance to IEC 61508 procedure

The figure shows next steps:

–**Development of the Product Concept** is a development of the product concept, during which the object of certification must be defined; the product concept also defines the safety integrity level (SIL), which determines the required values of safety indicators;

–**Establishment of the Project infrastructure** is the creation of project infrastructure, including the project organizational structure, as well as processes and tools of project management;

–**Preliminary FMECA** is the performing preliminary failure mode, effect and criticality analysis; using FMECA to determine the quantitative values of safety indicators specified in the IEC 61508 requirements; preliminary FMECA is called because in the preparatory work it is carried out to analyze the possibility of product certification in terms of reliability, safety and diagnostic coverage, which characterizes the degree of resistance to accidental hardware failures; if the conducted FMECA did not reveal deviations from the planned safety indicators, the transition to the next step is carried out; if the FMECA results show that the product does not meet the specified SIL level, then the analysis of design or SIL changing takes place; it may be found that the refinement will be so complex and expensive that it will be more effective to change the product concept, including in terms of reducing the specified SIL level; if a decision is made to refine the product, then proceeded to the next step;

–**Analysis of used integrated circuits (ICs) and tools** is an analysis of used programmable chips and development tools; IEC 61508-3 (7.4.4) requires full testing of code compiler outputs for defects in the final product made by the integrated curciuts; testing by commercial compiler is a time consuming task that calls into question the certification project success; however, in the last few years, with the increase in the market for security-critical systems, many leading developers of programmable components (Microprocessors and FPGAs) have released compilers certified in accordance with the safety requirements; such compilers can be used to develop program code without additional validation; a feature of certified compilers is that they can be applied only to a limited number of programmable chips, and not to all products in the line; another barrier is the high cost of many certified compilers (usually thousands of dollars); if the analysis of the used programmable components and integrated curcuits (IC) used for the development of PLCs and software did not reveal deviations from the IEC 61508 requirements, then proceed to the next step; if the results of the analysis show that the programmable components and ICs do not meet the requirements of IEC 61508, the analysis of ICs or tools changing is applied; it may turn out that the refinement will be so complex and expensive that it will be more effective to change the concept of the product; if a decision is made to refine the product, then proceed to the next step;

–**Analysis of Functional Safety Management (FSM) processes** is safety management processes analysis; IEC 61508 requires compliance with the requirements for safety management, as this method provides protection against systematic failures; if the analysis did not reveal deviations from the requirements of IEC 61508, then proceed to the next step; in case of discrepancies, corrective actions are required to bring the safety management processes in line with the requirements of IEC 61508;

–**Kick off meeting with Certification Body** initiates the meeting with the certification authority; in preparation for the launch of the certification project it is necessary to hold a meeting with the certification body, ie, with the organization that will assess compliance with the safety requirements and issue a certificate of compliance; at this meeting it is necessary to agree on the scope and content of the project;

– **Development of the Project Plan** is the development of project implementation;

– **Estimation of the Project cost** is the calculation of the project budget on the basis of the planned operations;

– **Estimation of resources availability**. After planning the costs of the project it is necessary to assess the availability of resources and their availability during the planned certification time; as already mentioned, certification is a costly measure, stretching over months and years, and it is difficult to expect "quick money"; it may be necessary to return to some preparatory actions to optimize costs before making a final decision on certification;

– **Making of the final decision** concerning the certification.

4.8 Functional Safety Management Plan

The safety management plan is a key document of the safety management processes. Consider a typical structure of a functional safety management plan.

When analyzing the requirements that should be reflected in the safety management plan, it is advisable to divide them into two parts. The first part includes requirements groups that require more tasks and, thus, result in independent management processes and require the development of separate plans. The second part includes "less global" requirements that do not need the development of separate plans, and which are sufficient to implement in the framework of the safety management plan.

Consider the processes set by the first part of the requirements. Such processes include:

– Human Resource Management;

– Configuration Management;

– Tools Selection and Evaluation;

– Verification and Validation;

– Requirements Tracing;

– Documentation Management;

– Functional Safety Assessment.

The peculiarity of taking into account and fulfilling the safety requirements is that, since each of the areas is quite large, dynamic and even partially autonomous from the other process, it is recommended to develop and maintain their own individual documents. In terms of safety management, it makes sense to leave the basic points without details. However, if the project is not large enough,all areas of planning for it, as well as the selection and evaluation of instrumented curcuits, can be included in the safety management plan.

A separate document is a requirements tracing report, as it can only be completed at the very end of the project. In addition, the safety management plan should include the following sections:

– Project Policy and Strategy is a declarative description of how and why the project goals will be achieved; as a matter of fact, this part summarizes the main provisions of the safety management plan;

– Project Management; Section 6 of IEC 61508-1 does not explicitly require the use of project management techniques, however, the requirements for project management are contained in IEC 61508-2 (Appendix B) as one of the methods of protection against systematic failures in the development of systems and hardware; therefore, consideration of the project management approach in terms of safety management is appropriate;

– Quality Management System; IEC 61508 requires suppliers to have a quality management system in place; if the organization and suppliers have an ISO 9001 certificate, then no issues arise; special attention is paid to interaction with product suppliers and services that affect the safety provision; this requirement also came from the quality management system (ISO 9001); in terms of Project Management analogue is "procurement management";

– Functional Safety Life Cycle should be described by stages in the safety management plan;

– Product Safety Manual is the main document that provides the user with a description of the product in terms of its use in compliance with all the safety requirements;

– Security; IEC 61508 has a very brief description of this important property, which, of course, does not mean that this aspect should not be paid attention to; how to confirm compliance with security requirements depends on the project specifics; if the cybersecurity management system (CSMS) is in place for the system development project, then, in this section of the safety management plan, it is sufficient to provide a reference to the relevant documents related to the security; if not - it is necessary to use the relevant documents (for example, IEC 62443 series).

4.9 Requirements Tracing

Requirements tracing is one of the processes of a broader field of knowledge called "Requirements Engineering". Requirements tracing is a method of changing requirements and related artefacts managing. Requirements tracing solves three main problems:

– ensures the implementation of all the requirements from the upper level at the lower level;

– prevents the appearance of undocumented functions at the lower level;

– provides and confirms coverage of all requirements by tests.

Specialized software is usually used to manage the requirements. One of the most famous such tools is IBM Rational DOORS. IBM claims that with the help of DOORS you can manage projects of any scale, respectively, the tool has serious functionality and analytics, and the cost of an annual license starts from a thousand dollars. At the same time, the basic functions of requirements management and tracing are to present requirements specifications in the form of a database, the records of which are components of the source document.

To perform the requirements tracing, the documents must be prepared for this process by placing requirements identifiers and tags that define the scope of the requirements. For example, in the Safety Requirements Specification, you must enter an identifier for each of the requirements, as well as specify a lower-level document where the requirements of the specification should be traced. For example, System Architecture Design. System Architecture Design must also be tagged. In addition, for each of the equirements, its source must be indicated in the top-level document, the so-called "parental requirement". Then each of the requirements of System Architecture Design is traced in Hardware Design and Software Design. The final results of the trace can be presented as a set of matrices that reflect the relationship between the requirements of the documents.

For the above mentioned example, the requirements tracing is performed amongthe design documents as follows. First, there is a direct requirements tracing from the Safety Requirements Specification to the System Architecture Design. Then, the requirements from System Architecture Design to the Safety Requirements Specification are traced back to make sure that System Architecture Design does not include redundant functionality that is not documented in the Safety Requirements Specification. After System Architecture Design, the design process is divided into two streams, Hardware Design and Software Design. For both documents, direct and reverse tracing is performed. Hardware Design mainly includes drawings in which it is problematic to place tags, so another document is marked under the trace, Hardware Design Review Report (Fig. 4.14).

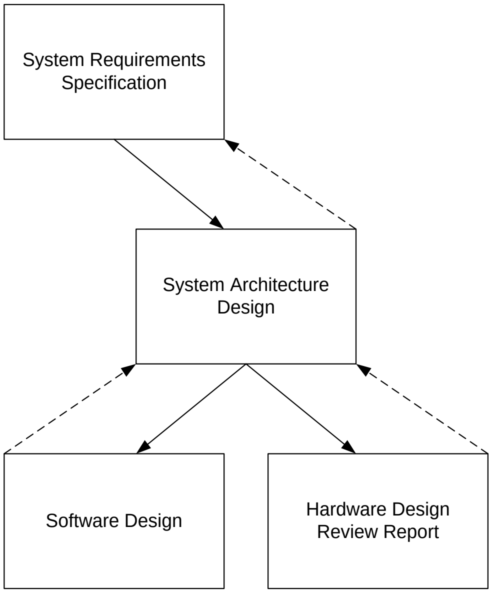

System Requirements Specification
System Architecture Design
Software Design
Hardware Design Review Report

Figure 4.14 – Tracing requirements for different stages of the life cycle

4.10 Configuration Management

Configuration management is the discipline of identifying the components of an evolving system to monitor changes in those components and maintain continuity and traceability throughout the lifecycle.

4.11 Tools Evaluation and Usage

The tools selection and evaluation activities are closely related to safety management, although the requirements are set out in a separate section of IEC 61508-3 (7.4.4 Requirements for Support Tools, including Programming Languages).

Depending on the degree of impact on the final product (system and software), tools are classified as follows:

– **T1 tools** do not generate outputs that directly affect the executed code; these include text and graphics editors, configuration management tools (those that do not directly generate code), action&bug trackers;

– **T2 tools** support testing and other types of verification and approval (e.g. static code analysis or test coverage integrity analysis); the direct effect on the executable code is not detected, however, the problem in the testing tools may lead to the fact that software errors may not be detected; this class should include not only software, but also software and hardware simulators of input / output signals; It should be noted that T2 tools may also include means of designing mechanical, electrical and electronic components (e/g. printed circuit boards);

– **T3 tools** generate outputs that directly affect the executed code, they include translators and compilers, which are part of integrated development environments (IDE & Software Development Kit, SDK), scripts to support build collections and SCADA in terms of configuration of the controller.

To ensure compliance with the safety requirements, it is advisable to develop a special the tools selection and evaluation report (TSER). It should include:

– a description of the stack of tools used (both software and hardware, both commercially available and in-house developed) used to develop the product, test it, and for the support processes (configuration management, set of text documents, project management, etc.); for each of the tools specify: type (which process is used to support), name, version number, vendor name, class (T1, T2 or T3), which outputs are generated in terms of configuration items;

– results of tools evaluation (analysis) according to a set of specified criteria, such as, for example: functions performed and their applicability in this project, experience, available documentation, information about the supplier, market reputation, quality management system, approach to configuration management and etc.), the impact on product safety, identified and eliminated errors, possible risks of use in terms of failure detection and risk management strategy, the availability on the market of compatible programmable chips (for software development and electronic projects).

In addition, the TSER should include the results of the tool compliance analysis specified in IEC 61508-3, such as:

– requirements specifications or user documentation must be available for T2 and T3 tools that clearly describe how the operation takes place;

– for T2 and T3 tools, the compliance with the requirements specification or user documentation must be documented, for example, in the form of a certificate;

– the used tools versions must be controlled, as the mentioned conditions may not be met for all the versions; all project participants must use the same version; the appropriate procedure must be used for transitions between versions;

– if the tools are used as a single technological complex (for example, code and tests are generated on the basis of the specification), their compatibility with each other should be tested.

The choice of programming tool is associated with the task of selecting programmable chips. The following criteria can be proposed as an approach to the chips selection:

- technology used: microprocessors, FPGA, signal processors, etc.;
- chip resources: memory, clock speed, etc.;
- physical parameters: size (form factor), frame type, number of input and output contacts, etc.;
- power supply parameters and power consumption;
- requirements for the chip surface mounting on the printed circuit board: soldering technology, requirements for the composition of the solders used, etc.;
- temperature and qualification level to the external factors influence: radiation, ultraviolet radiation, etc.;
- reliability indicators: failure rate, durability, shelf life, etc.;
- compatibility with development tools, including tools certified to meet safety requirements;
- availability of software libraries, including libraries certified for compliance with safety requirements;
- proven in safety-critical applications;
- time of availability on the market, both from the moment of issue and to the planned date of termination of release; the accelerated development of modern electronics is a serious challenge for conservative safety-related systems; the life cycle of the chip on the market does not exceed 10 years, which is too little for safety systems, because the chip must be tested and then certified based on the tested solution, and only this can be a total of up to 5 years; therefore, various solutions are offered to extend the service life (none of them is ideal): the purchase of a large number of chips used in the product "in stock" before their decommissioning, periodic transition to newer analogues, reverse engineering, when the existing program code is reproduced according to the design artifacts and adapted to the new programmable component;
- availability of errata sheets;
- the presence of manufacturer's documentation describing the mentioned above characteristics.

In addition, IEC 61508 requires selection and control of the application of coding rules, to use a limited secure set of programming language designs. To meet this requirement, coding guidelines (self-developed or borrowed from specialized companies) should be used in the certification project. Checking the compliance of the developed program code with the coding rules is one of the tasks of static analysis.

4.12 Documentation

Now consider what types of documents are developed in the draft certification for compliance with the safety requirements. Types of documents include:

- Safety planning documents;
- Safety Requirements Specification (SRS) and System Architecture Design (SAD);
- Hardware Design;
- Software Design;
- Verification and Validation documents;

– Equipment Qualification Testing for resistance to extreme influences; usually the levels of such influences as climatic (temperature and humidity), mechanical (shocks, resonance search, traffic shaking, seismic), electromagnetic are set;

– Documents related to tools (user manuals, requirements specifications, certificates confirming compliance, information on suppliers);

– Change Control;

– User-specified documentation for the delivered product including Product Safety Manual;

– Guidelines, procedures and instructions used in the project to organize the work; such documents may use company-accepted practices or may be designed specifically for a safety project;

– Safety evaluation documents.

The initial data can be obtained from databases of failure rates, datasheets, or calculated by structural reliability schemes.

4.13 Using Failure Modes, Effects, and Diagnostic Analysis

4.13.1 The sequence of reliability and safety analysis

According to the provisions of IEC 61508, Failure Modes, Effects, and Diagnostic Analysis (FMEDA) differs from other methods of reliability and safety analysis as it combines all the tasks of calculating safety indicators.

FMEDA is based on the developed and adopted standard IEC 60812: 2015 Methods of analyzing the systems reliability. Failure Analysis (FMEA) (IEC 60812: 2006, IDT), extending it with the failure diagnosis analysis.

The sequence of reliability and safety analysis using FMEDA includes the following steps:

– structure and system functions analysis;

– division of the system into constituent parts (elements), based on the influence of element failures on system failures and the detalization level;

– construction and analysis of the structural reliability scheme for system decomposition;

– failures types and system operation modes determination;

– determination of failures consequences and their criticality (influence on performance of safety functions; from the point of view of IACS safe condition is removal of data from analog and discrete outputs of the controller for the purpose of disconnection or inclusion (through intermediate relays) of executive mechanisms (so-called de-energize to trip). in addition, the type of failure is classified in terms of danger and diagnosability;

– failure reason determination;

– failure rate determination;

– definition of failures detection and compensation methods; for this purpose the approach to diagnosis of failure, both for hardware, and software failures is determined, also the size of a diagnosis coverage is defined;

– calculation and analysis of reliability indicators and safety; bottom-to-top analysis, i.e. nodes, modules, products and the system as a whole are "assembled" and analyzed from the components;

– the obtained safety values are compared with the IEC requirements for the specified SIL levels.

Different detalization levels can be used for these actions. Usually for safety systems, the analysis takes into account all electronic components, i.e. the level of resistors, capacitors, diodes, etc. is analyzed.

FMEDAs are performed for identified safety functions (in IEC 61508 terminology this is called Safety Instrumented Function) in terms of software and hardware (sensors, logic controller and actuators) involved in the functioning. For functions, dangerous failure states are defined and described.

The mode of operation for safety functions is considered, which can be with high and low intensity of requests, as well as continuous.

The results of the analysis are recorded in the form of FMEDA tables. Consider further stages of FMEDA, proceeding within the purposes of IEC 61508.

The presented FMEDA table (see table 4.3) contains examples of typical failures for PLC modules. Of course, this is only a small list, usually the FMEDA table for the electronic module contains dozens and hundreds of possible failures, up to the analysis of the simplest components (resistor, capacitor, etc.). For complex electronic components, such as a microprocessor, the number of types of failures can also be dozens, especially when performing FMEDA for software.

Table 4.3 – FMEDA table example for PLC module

Component	Failure type	Failure reason	Failure consequence	Failure safety impact	Failure diagnostics	Failure compensation	Failure rate
Power supply unit	Power loss	Short circuit	Module power loss	Dangerous	Voltage control circuit	Transition to a safe state	
CPU clock speed node	Frequency loss	Short circuit	Disabling the processor	Dangerous	Watchdog timer	Transition to a safe state	
Processor node	Lack of contact	Soldering defect	Disabling the processor	Dangerous	Сторожовий таймер	Transition to a safe state	
Processor node	Memory error	Chip defect	Inaccurate CPU performance	Dangerous	Memory test	Transition to a safe state	
Watchdog timer node	Lack of initial data	Voltage reduction	Lack of control	Dangerous	CPU software	Transition to a safe state	
Ethernet communication node	No connection to the workstation	Chip defect	Lack of data in SCADA	Safe	Workstation (external)	Backup channel connection	

When assessing the safety for compliance with the requirements of IEC 61508, FMEDA table is not the final, but only the source material, because it does not answer questions about the achieved level of SIL.

The next step is the formation of spreadsheets that relate to specific software and hardware (e.g., PLC) and are used to analyze the reliability and safety of systems developed on the basis of these tools (see Table 4.4).

Table 4.4 – A practical example of calculating safety indicators

PLC component	λSd	λSu	λDd	λDu	SFF	DC
Analog signal input module, common part	6E-7	9E-8	3,7E-7	1,2E-8	0,989	0,969
Analog signal input module, 1 input channel	1E-7	1E-9	1,1E-7	3E-9	0,986	0,973
Logical processing module	3,4E-6	1,2E-7	5,7E-7	4,1E-8	0,990	0,933
Discrete signal output module, common part	6,5E-7	1E-7	3,5E-7	1,2E-8	0,989	0,967
Discrete signal output module, 1 input channel	7E-8	1E-9	3E-8	2E-9	0,981	0,938
TOTAL	4,82E-6	3,12E-7	1,43E-6	7E-8	0,989	0,953

Table 5.4 includes the PLC modules required to implement the function of protecting the boiler from excess pressure, namely the module for input of analog signals, the module of logic processing and the module for output of discrete signals. For input and output modules, a common part and an input or output channel are selected. This is because the input and output modules have several ports for signal processing, and to implement the safety function you need to connect only one input and one output channels. Thus, the accuracy of calculation of safety indicators increases, excluding idle signal processing ports.

Differentiation of failure rates corresponds to the failure classification of IEC 61508. The rate of dangerous failures of PLC is $\lambda_D = \lambda_{Dd} + \lambda_{Du} = 1{,}5*10^{-6}$ 1 / hour.

The obtained SFF values for all components and for the PLC as a whole are in the range of 90% -99%, which corresponds in the non-reserved configuration to the SIL2 level. The value of the diagnostic coverage is also 90% ≤ DC <99%.

Assuming that the system is running in a low query mode. To determine the Proof Testing Interval (PTI), it is necessary to investigate the dependence of the probability of dangerous failures over time. The limit value corresponding to the level of SIL2 is PFD = 0,01.

This value is calculated as $PFD\ (t) = 1 - \exp\ (-\lambda_D \cdot t)$.

It should be remembered that in the IACS on the PLC accounts for 15% of failures, which is PFD_{PLC} = 0,0015.

$$PFD_{PLC} \text{ (1 month)} = 0{,}00103 <0{,}0015.$$

$$PFD_{PLC} \text{ (2 month)} = 0{,}00206> 0{,}0015.$$

Thus, for the SIL2 level, the interval between periodic testing should be PTI = 2 month.

The recommended recovery time in IEC 61508 can be set as the average recovery time after failure MTTR=8 hours.

4.13.2 Calculation of Safe Failure Fraction

Based on the classification of failures, the following relations can be obtained for failure rates:

- total failure rate: $\Lambda = \lambda_{Sd} + \lambda_{Su} + \lambda_{Dd} + \lambda_{Du}$;
- dangerous failure rate: $\lambda_D = \lambda_{Dd} + \lambda_{Du}$;
- safe failure rate: $\lambda_S = \lambda_{Sd} + \lambda_{Su}$;
- detected failure rate: $\lambda_d = \lambda_{Sd} + \lambda_{Dd}$;
- undetected failure rate: $\lambda_u = \lambda_{Su} + \lambda_{Du}$.

The above values of rates are the basis for determining the safety values specified in IEC 61508.

Safe Failure Fraction (SFF) is defined as the ratio of the of safe and dangerous diagnosed failures rate to the total failure rate:

$$SFF = (\lambda_S + \lambda_{Dd}) / \Lambda.$$

4.13.3 Calculation of Diagnostic Coverage

Diagnostic Coverage (DC) in IEC 61508 is determined only on the basis of the dangerous failures rate, this is the ratio of dangerous diagnosed failures rate to the rate of dangerous failures:

$$DCD = \lambda_{Dd} / \lambda_D.$$

In technical diagnostics, a more common approach is when the diagnostic coverage is defined as the ratio of the diagnosed failuresrate to the total failure rate:

$$DCD = \lambda_D / \Lambda.$$

However, IEC 61508 declares diagnostic coverage based on the fraction of reduction in the dangerous failures probability due to the built-in diagnostics.

4.13.4 Calculation of probability of failure on demand

For systems with low query frequencies, the target is the determined average probability of a dangerous failure to perform the on-demand safety function. For the completeness level of SIL1 safety, this value should not exceed 0.1. As the SIL increases, the probability of a dangerous failure should decrease 10 times each level. Thus, for the SIL4 security level, the probability of a dangerous failure should be from 10^{-5} to 10^{-4}.

The probability of dangerous failures is determined as follows:

$$PFD\ (t) = 1 - \exp\ (- \lambda_D\ t) = \exp\ (- (\lambda_{Dd} + \lambda_{Du})\ t).$$

4.13.5 Determination of Safety Integrity Level

The safety integrity level is a value that reflects the ability of the system to provide safety features. The required SIL level is calculated based on the risk graph assessment.

The initial data for the graph are given in the Table 4.5.

Table 4.5 – Risk graph input data

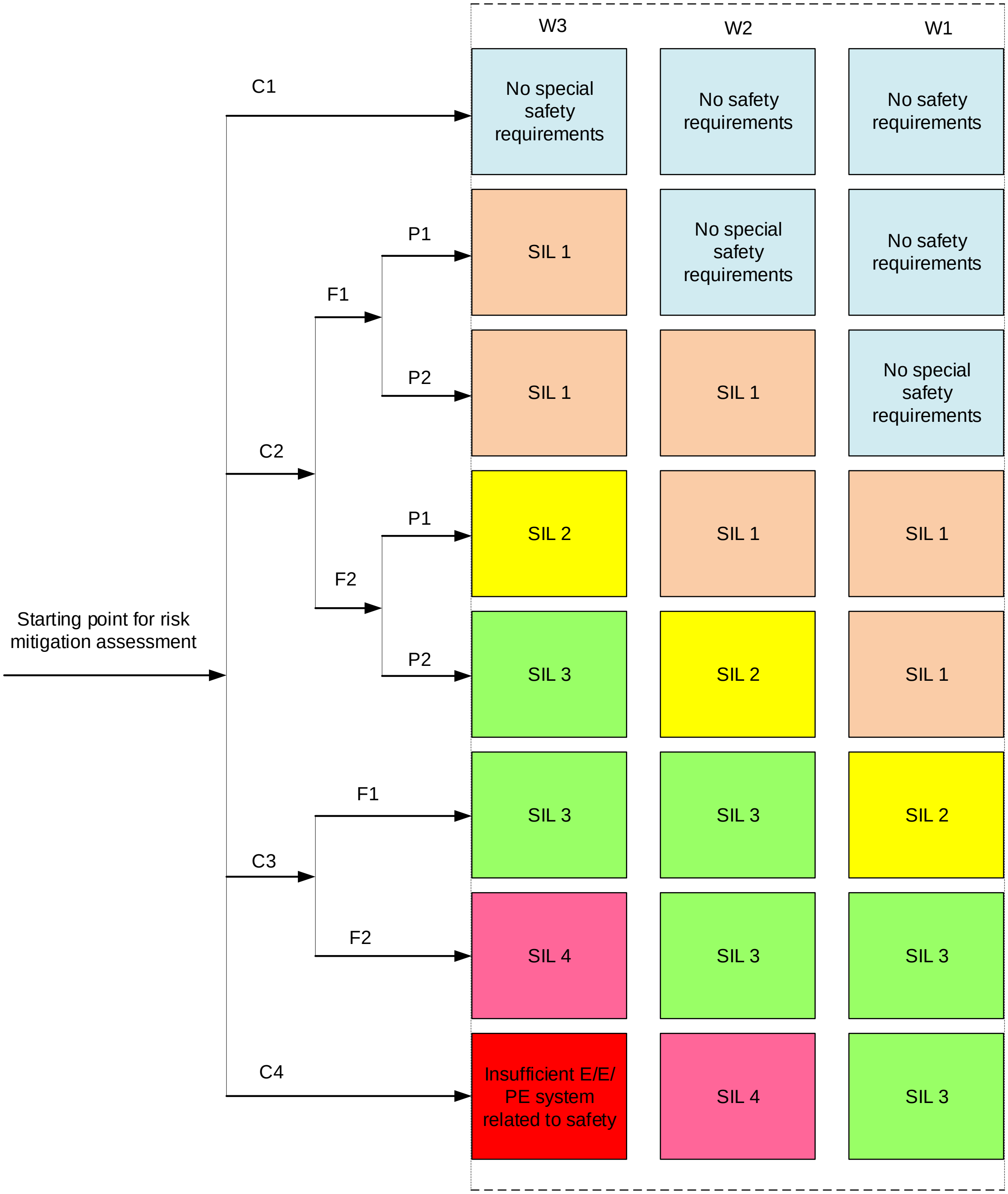
Risk parameter		Classification
Consequences of risk C	C1	A minor injury
	C2	Serious irreversible injury to one or more people
	C3	Death of several people
	C4	Death of a large number of people
Frequency and duration of stay in the danger zone F	F1	From rare to frequent stay in the danger zone
	F2	From frequent to prolonged stay in the danger zone
Ability to avoid a dangerous event P	P1	Probably under certain circumstances
	P2	Almost impossible
Probability of an undesirable event W	W1	Quite a small probability of an undesirable event, posibility of only a small number of such events
	W2	A small probability of an undesirable event, a small number of such events is possible
	W3	Relatively high probability of occurrence of an undesirable event, probable frequent recurrences of an undesirable event

4.14 Industrial-Process Measurement, Control and Automation – Framework for Functional Safety and Security

4.14.1 Security unity concept and security environment

For modern industrial systems it is important to apply methods aimed at providing both cybersecurity and safety. It should be noted that in the IEC 61508 series safety standards practically do not refer to cybersecurity, there are no approaches to provide it, but there is a link to the IEC 62443 standards series.

Safety concerns the correct functioning of systems, connected with safety. For systems where safety depends on security systems, security countermeasures contribute to safety functions. Complex of security countermeasures must create a secure environment to achieve this goal (Fig. 4.15).



W3	W2	W1
No special safety requirements	No safety requirements	No safety requirements
SIL 1	No special safety requirements	No safety requirements
SIL 1	SIL 1	No special safety requirements
SIL 2	SIL 1	SIL 1
SIL 3	SIL 2	SIL 1
SIL 3	SIL 3	SIL 2
SIL 4	SIL 3	SIL 3
Insufficient E/E/ PE system related to safety	SIL 4	SIL 3

Figure 4.15 – Risk graph

It is recommended to establish interaction between experts in the field of safety and information security in order to ensure general security. Specific implementation of interaction depends on the organization's policy. Overview of potential interactions shown in Figure 4.16 (IEC TR 63069).

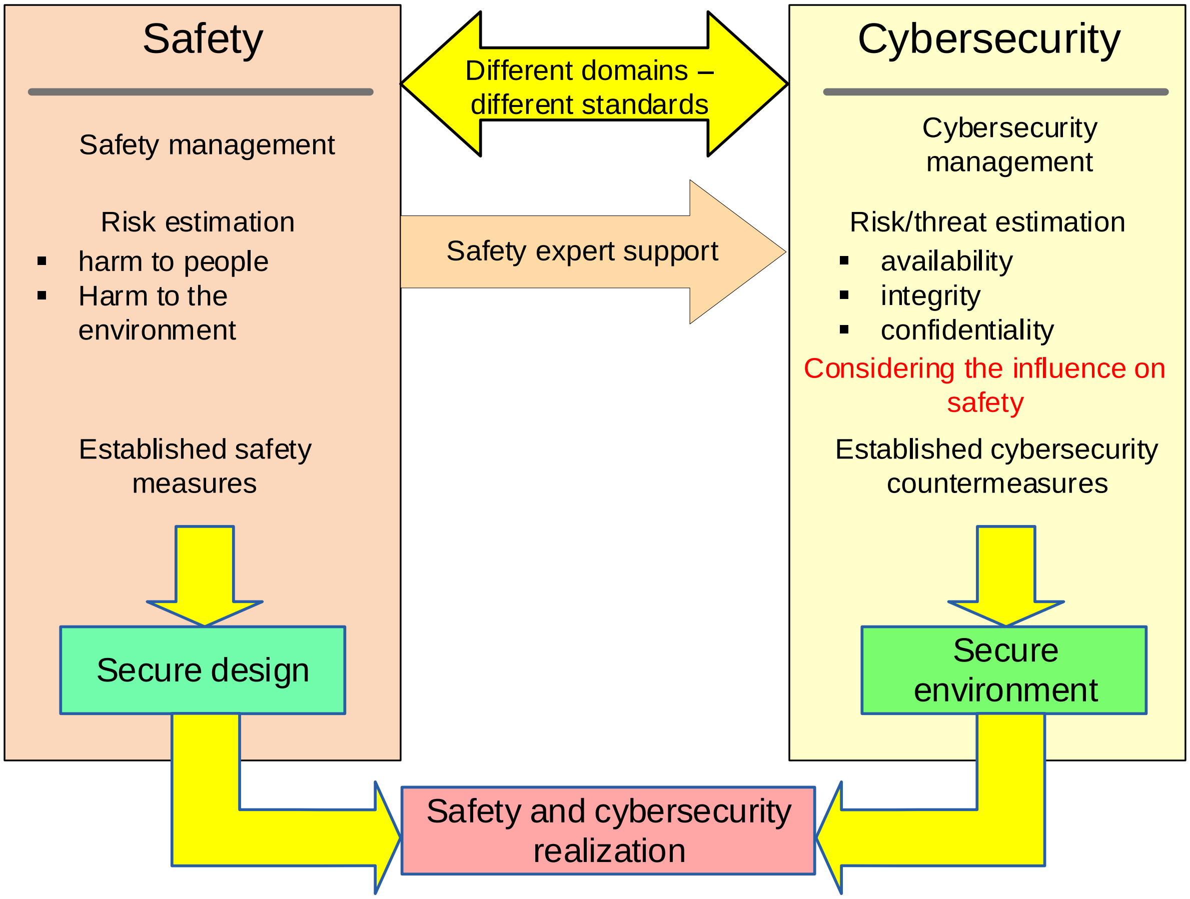


Figure 4.16 – Safety and cybersecurity interaction

The safety domain should be controlled in accordance with IEC 61508 (all parts). The cybersecurity domain must be controlled in accordance with IEC 62443 (all parts).

4.14.2 Managing Security Related Safety Aspects

When interacting between the domains of cybersecurity and security, as shown in Figure 10, the following is recommended.

1. Security aspects relating to safety should be guided by the personnel of the security domain and investigated during the threats and risk for security assessment.

NOTE «Guided by the personnel of the security domain» doesn’t mean that it should n=be operated only by security experts.

2. Potential security consequences that affect safety functions must be resolved by countermeasures defined for security environment.
3. Measures to implement safety and countermeasures for environment must meet guidelines to achieve the required risk reduction in both spheres.

Risk assessment for safety and threat assessment for cybersecurity should be based on the high-level risk assessment results.

When evaluating threats and security risks, security and safety experts investigate the potential impact on safety functions. Safety experts should provide a detailed description of the isafety implementation while intoducing safety functions, includinf the list of assets used to build the safety system and its data (for example, specifications and configuration). The security expert must be able to understand the safety precedents to identify the security risks that may affect safety.

Processes associated with safety or with a cybersecurity domain can be carried out separately by individual teams or by one common team. Safety and cybersecurity experts should try to reach the agreement. If arrangements are not achieved, a compromise analysis should be applied.

The interconnection between the introduction of safety and product cybersecurity (in the considered case it is an industrial automation and control system) is reflected in Figure 4.17. On the left of the main stages of the system's lifecycle there are the activities that are relevant to security. The system is considered an enterprise or organization, the product is an industrial automation and control system within the enterprise. The relevant normative documents on the domain of safety are delivered from the lifecycle stages. All activity on both domains (Safety and Security) are tied to certain stages of the lifecycle, outgoing from the established frameworks of their use.

4.15 Security and safety life cycle of Industrial Control Systems

As if was defined earlier, security and safety can be implemented in a fame of common life cycle. Typical ICS life cycle include four the main stages:

– ICS development, what is responsibility of ICS vendor;

– ICS installation and commissioning at the operation site, what is responsibility of a system integrator;

– ICS operation and maintenance, what is responsibility of an operator (assets owner);

– ICS decommissioning, what is also responsibility of an operator (assets owner).

From the point of security view, operation is the most important phase because security features are running and maintaining during ICS operation. However, the most complicated structure is implemented for ICS development, since in accordance with standards requirements this part of life cycle has to have a V-shape (see Fig. 4.18). Development phases are signed with usual lines and verification and validation phases are signed with dash-lines.

The main security features implementation for specified life cycle stages and phases are given below.

During concept phase, ICS security implementation includes the following activities:

– Recognize need for protection of property, assets, services, or personnel

– Start developing the security program

– Document assets, services, and personnel needing some level of protection

– Document potential internal and external threats to the enterprise

– Establish security mission, visions, and values;

– Develop security policies for industrial automation and control systems and equipment, information systems and personnel.

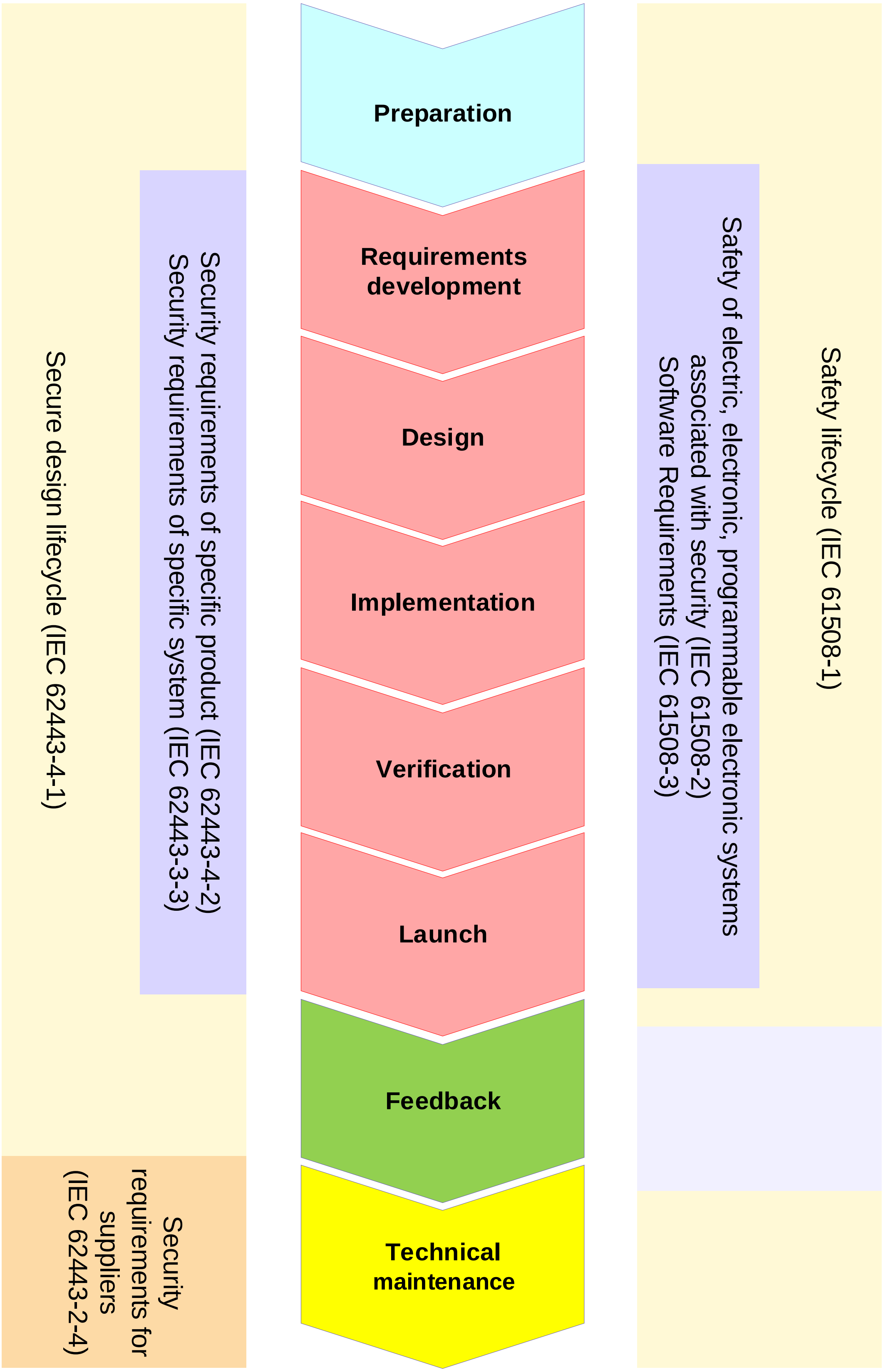

Preparation
Requirements development
Design
Implementation
Verification
Launch
Feedback
Technical maintenance
Secure design lifecycle (IEC 62443-4-1)
Security requirements of specific product (IEC 62443-4-2)
Security requirements of specific system (IEC 62443-3-3)
Security requirements for suppliers (IEC 62443-2-4)
Safety of electric, electronic, programmable electronic systems associated with security (IEC 61508-2)
Software Requirements (IEC 61508-3)
Safety lifecycle (IEC 61508-1)

Figure 4.17 – Applying safety standards during the lifecycle of product development

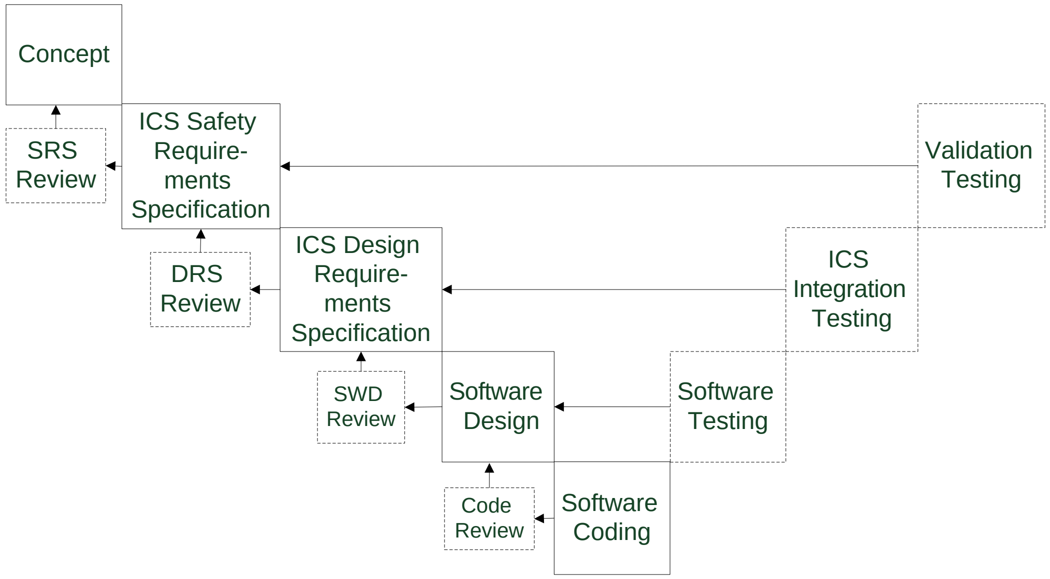


Figure 4.18 – V-shape security and safety life cycle (development stage)

The main issues of phase content and goals are given in Table 4.6.

Table 4.6 –Life cycle content (development stage)

Phase name	Activities
Concept	Developments of top-level conceptual document, which states recognition of needs for plants and processes automation including hazards, threats and risks analysis
SRS	Developments of ICS functional requirements specification (“black box”) including modes, timing, interfaces, signals, self-diagnostics and others
SRS Review	SRS verification against Concept requirements
DRS	Developments of ICS architecture requirements specification (“white box”) including detailed structure and behavior description
DRS Review	DRS verification against SRS requirements
Software Design	Developments of algorithms and data structure for every software module
Software Design Review	Software Design documents verification against DRS requirements
Software Coding	Writing a software source code in accordance with Software Design documents

Phase name	Activities
Code Review	Software code verification against Software Design documents requirements including Static Code Analysis
Software Testing	Functional and structural testing of software code against Software Design documents requirements
Integration Testing	Functional testing of integrated ICS components against DRS requirements
Validation Testing	Functional testing of ICS against SRS requirements

During SRS development phase, ICS security implementation includes the following activities:

– Continue developing the security program;

– Establish security functional requirements for ICS and equipment, production systems, information systems, and personnel;

– Perform vulnerability assessment of facilities and associated services against the list of potential threats;

– Discover and determine legal requirements for ICS;

– Perform a risk analysis of potential vulnerabilities and threats;

– Categorize risks, potential impacts to the enterprise, and potential mitigations;

– Segment security work into controllable tasks and modules for development of functional designs;

– Establish network functional definitions for security portions of ICS.

During DRS development phase, ICS security implementation includes the following activities:

– Development of the security program is completed in this phase

– Define functional security requirements for enterprise zones, plant zones, and control zones;

– Potential activities and events are defined and documented to perform the functional requirements and implement plans for a secured enterprise;

– Define functional security organization and structure;

– Define functions required in the implementation plan;

– Define and publish security zones, borders, and access control portals;

– Complete and issue security policies, and procedures;

– Design physical and logical systems to perform the functional requirements previously defined for security;

– Conduct training programs;

– Initiate asset management and change management programs;

– Design borders and access control portals for protected zones;

During software design and software coding phases, the designed before security features shall be implemented into the ICS components.

During installation and commissioning stage, ICS security implementation includes the following activities:

– Physical security equipment, logical applications, configurations, personnel procedures are installed to complete the secured zones and borders within the enterprise;

– Access control portal attributes are activated and maintained;

– Training programs are completed;

– Asset management and change management programs are functional and operating;

– Security system turnover packages are completed and ready for acceptance by operations and maintenance personnel.

During operation and maintenance stage, ICS security implementation includes the following activities:

– Security equipment, services, applications and configurations are completed and accepted by operations and maintenance;

– Personnel are trained, and continued training is provided on security matters;

– Maintenance monitors security portions of enterprise, plant, or control zones and keeps them functioning properly

– Asset management and change management is operational and maintained

– Risk reviews, internal and external audits are conducted.

During decommissioning stage, ICS security implementation includes the following activities:

– Obsolete security systems are properly disassembled and disposed of;

– Security borders are updated or recreated for zone protection;

– Access control portals are created, redefined, reconfigured, or closed;

– Personnel are briefed about changes in the security systems and items along with the impact to associated security systems;

– Intellectual property is properly collected, documented, and securely archived or destroyed.

Processes and management maturity issues are closely related with life cycle issues. It is possible to describe the relative maturity of a security program in terms of a life cycle that consists of several phases. Each of these phases consists of one or more steps. So company level should be implemented or maintained through ICS life cycle.

5 RISK MANAGEMENT AND SECURITY AUDITS OF OPERATION TECHNOLOGY SYSTEMS AND PROCESSES

5.1 Risk Management Standards and Guidelines

Cybersecurity procedures based on standards and properly implemented in companies help to manage risk by making systems more resistant to attacks. Also help reducing the impact that an attack can have on critical infrastructure. Organizations without security standards face several problems, including unaware of their security weaknesses and how they can be exploited by intruders.

Cybersecurity standards occur on several levels. International standards are those adopted by an international **Standards Development Organization (SDO)** and are publicly available, e.g. international **ISO standards**.

Standards at a regional level are adopted by several nations in a given geographical region, for example the **European Committee for Standardisation (Comité européen de normalisation - CEN)**. National standards are prepared for use in a country by a government or an SDO.

A national standard can also become an international standard for example, **the American National Standards Institute (ANSI)**, which is the technical standards setter in the USA, and the **British Standards Institution (BSI)**.

The Security Industry Association (SIA), on the other hand, is a standard adopted by companies.

American and international organizations have introduced good practices developed by the **National Institute of Standards and Technology (NIST)** as generally applicable organizational standards.

The International Organization for Standardization **ISO** is an organization of over 150 countries that prepares all international standards. The standards for the electrical and electronic engineering industry are developed by the **International Electrotechnical Commission (IEC)**. Therefore, ISO and IEC have created **Joint Technical Committee 1 (JTC1)**, which is an organization developing standards dedicated to the IT industry and those concerning system and information security.

Although **CEN**, whose members are national standards organizations from 30 European countries, develops its own standards for cyber-safety and in conjunction with other international, national and governmental standards.

The Association for Automatic Identification and Mobility (AIM) is a trade association for entities with an interest in AIDC (**Automatic Identification and Data Capture**) technologies. The AIM develops cybersecurity standards in areas such as barcodes, card technologies, electronic article surveillance, RFID (Radio-frequency identification), Real-Time Location Systems (RTLS), and other AIDC-related technologies.

The British Security Industry Association (BSIA) is the professional association for the security industry in the UK. BSIA develops standards, good practice, and technical documentation. The security areas covered by BSIA include access control, information destruction, physical protection equipment and security systems.

The Information Systems Audit and Control Association (ISACA) is an organization dedicated to ensuring information flow, security, and audit. It is particularly known for its information audit system and standards control. ISACA has developed Control Objectives for Information and related Technology (COBIT), a control framework covering several aspects of IT management including risk assessment. COBIT is based on various international standards and can be used to define appropriate reference standards during audits.

The Instrumentation, Systems, and Automation Society (ISA) is an association that develops standards for automation technology. For example, the SP99 working group develops safety standards for manufacturing and control systems, such as Supervisory Control and Data Acquisition Systems (SCADA) and Distributed Control Systems (DCS). Some of the ISA reports on the subject have become ANSI standards.

NIST develops security standards for US federal information systems. NIST FIPS systems have been made mandatory for federal use. An example of FIPS is FIPS 200, which sets minimum security requirements for federal information systems, FIPS 199 provides standards for categorizing the security of federal systems and FIPS 197 defines the Advanced Encryption Standard (AES). NIST also hosts **the National Center for Standards and Certification Information (NCSCI)**, an institution that provides information on U.S. standards and technical regulations.

In addition to the above- mentioned organizations, other cybersecurity standards are available. The **ICT Security Standards Roadmap** provides a summary of available and approved ICT security standards.

The guidelines for risk management related to cybersecurity are set out in the **Act of 2018 on the National Cyber Security System**. The legislator used international ISO standards when drafting the Act on the National Cybersafe System.

The effectiveness of a cybersecurity system depends on its integration with other management systems in the company. The areas of management that are worthy of attention, in terms of compliance with the National Cyber Security Act are risk assessment, identification, data collection, and one of the most important, i.e. incident reporting.

When preparing to implement a security system in a company, it is worth getting familiar with the following ISO standards:

- **ISO 22301:** this standard entered into force several years ago and complements the information security management system. It addresses issues related to ensuring the continuity of the organization’s operations.
- **ISO 27000:** provides a general overview and terminology used in ISO/IEC 27001:2005.
- **ISO 27001:** presents an information security management system, i.e. the security requirements and objectives identified in Annex A.
- **ISO 27002:** contains practical rules for information security, including a list of security features.
- **ISO 27005:** This standard cover information security risk management. It contains, among other things, a catalog of threats to be considered in risk analysis.
- **ISO 27035:** this standard contains information on the management of security incidents.
- **ISO 27041**: provides guidance on mechanisms to ensure that methods and processes used in the investigation of information security incidents are 'fit for purpose'.

- **ISO 27043:** provides guidance based on idealized models for common incident investigation processes in different investigation scenarios involving digital evidence.
- **ISO 31000:** the standard states that the selection and implementation of safeguards must be based on risk analysis.

5.2 Systems Security Audits

The security audit shall be carried out to check the security systems in terms of procedures and systems in the organization. Well performed audits indicate weaknesses in the security systems and their vulnerability to external attacks. It is important to remember that until recently, operational technology (OT) infrastructure had no contact with IT solutions and thus was exposed to fewer threats.

The audit should answer the following questions:

- Is the data safely stored?
- Is it possible to attack critical infrastructure?
- Are there procedures in place to respond to incidents?
- Are employees aware of the threats resulting from the connection between OT and IT?
- Is documentation securely stored?
- What should be improved in the future and what security procedures are implemented?
- What risks are there if current security measures are not improved?
- How not to make similar mistakes in future years?

Recommendations for the OT systems security audit:

- cyclical safety audits or control activities to confirm the facts with the assumed requirements. should be carried out not less frequently than once every two years
- Irregularities detected during the audit should be included in the post-audit report.
- It is recommended that cyclical security tests be conducted to verify the effectiveness of OT environment safeguards - they should be limited to verification of edge protections (e.g. firewall between IT/OT layers) and OT environment architecture, software version, operating system configuration on OT systems.
- It is not recommended to use network tools in the production environment. Vulnerability identification using active network tools should be performed in the laboratory environment or during the OT system deployment phase.

A security audit can be performed using the scenario described inTable 5.1.

Security audit requirements under the National Cyber Security Act:

1. Under the national law, the operator of key services is required to conduct a security audit of the information system used to provide the key service once every 2 years, with the first audit to be carried out within one year from the date of notification of the decision to consider a key service operator. A written audit report and documentation is kept by the operator and may be made available upon a reasoned request from the competent authority for cyber security, the Director of the Government Security Centre and the Head of the Internal Security Agency.

2. The Cyber Security Authority is authorized to supervise the key service operators in, for example, auditing, preventing cyber threats and reporting serious incidents. As part of the supervision, the competent authorities may carry out inspections as well as impose fines.

3. The key service provider may designate internal structures responsible for cyber security or enter into an agreement with the provider of such services.

4. The audit may be carried out by:

- A conformity assessment body accredited in accordance with the provisions of the Act of 13 April 2016 on conformity assessment and market surveillance systems.
- At least two auditors holding certificates specified in the regulations and at least three years' practice in the field of information systems security audit or two years' practice in the field of information systems security audit.
- Sectoral cybersecurity team

5. The auditor is obliged to keep confidential information obtained in connection with the audit. Based on the collected documents and evidence, he shall prepare a written report on the conducted audit and forward it to the key service provider together with the documentation.

Table 5.1 – Scenario of security audit

Operations	Description
Prediction	
Proactive threat analysis	Defining threats resulting from the company profile, e.g. checking which IT infrastructure solutions have been implemented
Prediction of attack	Checking how a production line can be attacked, for example. The answer to the question whether it is possible to access control systems from outside.
Primary systems	Check the vulnerability of the systems used.
Response	
Reacting to intrusion/change	Designing the process of how to deal with incidents or changes.
Designing changes	What changes need to be made to prevent intrusion, what procedures need to be followed. Training of employees in information security.
Undertake investigative action / white internet intelligence	Risk identification based on information collected from various publicly available sources.
Prevention	
Identifying and removal of vulnerable areas from the system and separating systems	Checking the actions to reduce vulnerability of systems to external attacks.
Distraction of attackers	
Prevention of incidents	
Detection	
Detection of incidents	Checking and stopping incidents.
Confirmation and prioritization of risks	
Incident prevention	

It is worth knowing that the key service provider with whom an internal audit of the information system for the provision of the key service in information security was conducted in a given year is not obliged to conduct the audit for 2 years.

5.3 Infrastructure Reliability

To increase the reliability of the infrastructure, companies use platforms for asset integrity management in single and complex installations. The software allows for central monitoring of the integrity and reliability of assets in refineries, chemical plants, LNG plants, offshore and onshore facilities around the world.

Maintenance and reliability in the context of OT infrastructure are defined as having assets and resources in good condition. Today, the software allows for more efficient management. The databases store information about the inspections carried out and, based on this data, a new inspection date can be set, with confidence that they will be in good condition. The Anglo-Saxon example illustrates the situation well, the company inspects the liquid tank every year. The inspection comes out fine and the data obtained from it are entered into the system. The analysis of data from the last three inspections clearly shows that an inspection every year is not necessary and can be postponed by half a year. Thus, the planned inspection is carried out on average every 1.5 years. The organization can save money in this way, as it does not have to close a part of the infrastructure for the duration of the inspection.

Additional advantages of using the asset management platform are:

- Reduction of downtime to 50%.
- Risk minimization using risk estimation methods (RBI).
- Defined list of work and tasks to be performed.
- Reliability and responsibility management.
- Extension of the operating time.
- Reduction of inspection costs up to 30%.

A system supporting the reliability of OT infrastructure is also historian data, whose highly scalable, open data infrastructure gives businesses the ability to operate in real- time, transforming operational data into useful knowledge. This is an opportunity to develop operational analysis in the organization.

Historian data provides access to critical data that is found in many incompatible systems across the enterprise. It discovers new ways to improve processes and make continuous improvements. The system allows for data collection, search, analysis and visualization. Each step leads to a deeper understanding of what has been done and what is happening now, enabling organizations to move from reactive to proactive decision-making. This is a process that never stops and that constantly discovers the possibility of finding new value through:

- Process optimization.
- Increase in production quality
- Increasing asset availability.
- Improvement of energy efficiency.
- Risk management and compliance.
- Improving safety performance.

With these and other key business solutions, companies are prepared to improve operational analysis and sustainability in a competitive environment.

Additionally, the data history system stores such data as:

- Analogue data, e.g. processor temperature, fan and other equipment revolutions, flow rate, fluid level and pressure.
- Digital readings such as valve positions, limit switches, discrete level sensors and whether motors are on or off.
- Quality assurance data, such as process, product and custom limits.
- Limit exceeding alerts and return to normal signals.
- Aggregate data such as average, standard deviation, process efficiency, moving average.

Asset integrity management platforms have built-in functionality that reads data from data historian. The advantages of this functionality are well illustrated by the following example, the device has a temperature set to -20°C and a maximum value of 40°C as the minimum value of the parameter. Thus, this device working in these parameters should be in good condition for at least 5 years. Nevertheless, there may be incidents, i.e. situations when the device will work outside the correct parameters. It is then important to know how long the device has been working outside the parameters and whether degradation has occurred. The device may work in other parameters due to technological processes or hacker attacks. It is worthwhile to monitor the device's operation because the IT system can penetrate the OT system and change the preemptive temperature from -10°C to 140°C from the computer level leading to its degradation. Platforms adapted to asset management show data on offences and allow for their constant monitoring.

5.4 Transformation of Operation Technologies Towards Industry 4.0

Since the industrial revolution, new industries have been created and developed: processes have become more efficient, the productivity of industrial processes has increased, and new services, tools and products have driven the development of all our societies. To monitor, manage and supervise these industrial processes, industrial control systems (ICS) and operating technology have been implemented to ensure that these industries operate day and night, constantly producing the services, media, fuel, chemicals and manufactured goods we need. Traditionally most OT companies have existed and operated in silos, isolated and not connected to each other or to the outside world. Industry 4.0 means the digital transition, i.e. the creation of networks between products, value chains and business models. It is also characterized by automation, which relates to data exchange and wide application of new technologies and ways of supervising production. The fourth industrial revolution is observed on two levels, namely:

- Horizontal integration - industry transforms and integrates processes within an organization such as purchasing and product development, manufacturing, logistics and services.
- Vertical integration - includes customers, suppliers and all key value chain partners. It is based on technology that enables the identification, tracking, integrated planning and execution of tasks in real- time.

The use of advanced algorithms and the loT Internet of things allows organizations to carry out the digital transformation towards industry 4.0. This transformation involves changing the processes of production planning, i.e. transferring the planning from people to computers that are equipped with DCS or SCADA control and control systems. The concept of the fourth-generation industry is related to the integration of areas that were previously disconnected, i.e. OT production systems with IT infrastructure. Within the 4.0. industry, huge amounts of data are taken from various devices and systems and then processed using advanced algorithms, data warehouses and high computing power. To gain a new perspective on production processes and business lines, production lines have been equipped with ultra-modern sensors (IoT). However, they were not designed to operate in cyberspace and this is one of the biggest challenges of the fourth-generation industry.

When planning the digital transition, it should be considered that production lines are vulnerable to external attacks and the number of detected vulnerabilities in production systems is constantly increasing. There is also a noticeable increase in security incidents. Manufacturing companies want to benefit from IT facilities and improvements, thus joining the IT world in terms of cyber threats. Thus, the implemented cyber security strategy should include mechanisms to protect production processes. Proper training of technical staff is equally important. So far, automation specialists have not been in contact with advanced malware, which, for example, can cause the production line to fail continuously. Preventive measures at the interface with the IT world and detection measures in the production sphere are also important in this area, so that they can detect and respond to an attack.

5.5 Case Studies of Cyber-Attack

Critical infrastructure and industrial systems remain prime targets for cyberattacks, with the energy sector being particularly vulnerable. Recent years have seen a significant increase in both the frequency and sophistication of attacks on industrial control systems (ICS) and OT networks. These incidents underscore the critical importance of robust industrial cybersecurity and reliability measures.

Colonial Pipeline Ransomware Attack (2021)

One of the most significant recent cyberattacks on industrial infrastructure occurred in May 2021, when Colonial Pipeline, the largest fuel pipeline in the United States, fell victim to a ransomware attack. This incident led to a six-day shutdown of the pipeline, causing fuel shortages across the southeastern United States and highlighting the vulnerabilities in critical infrastructure.

Key points:

1. The attack was carried out by DarkSide, a Russian-speaking hacking group.
2. It affected the company's billing system and internal business network, prompting a precautionary shutdown of pipeline operations.
3. Colonial Pipeline paid a $4.4 million ransom, though some was later recovered by authorities.
4. The incident led to panic buying, fuel shortages, and price spikes, demonstrating the far-reaching economic and social impacts of industrial cyberattacks.

Relevance to industrial cybersecurity and reliability: This attack highlighted the interconnectedness of IT and OT systems in modern industrial environments. It demonstrated how an attack on business systems could indirectly impact operational systems, emphasizing the need for comprehensive cybersecurity strategies that cover both IT and OT networks.

Oldsmar Water Treatment Facility Attack (2021)

In February 2021, a water treatment plant in Oldsmar, Florida, was targeted in a cyberattack that could have had severe public health consequences.

Key points:

1. An attacker gained unauthorized access to the plant's SCADA system.
2. The hacker attempted to increase the amount of sodium hydroxide (lye) in the water to dangerous levels.
3. The attack was quickly detected and thwarted by an alert operator.
4. Investigation revealed that the facility was using outdated Windows 7 systems and shared passwords for remote access software.

Relevance to industrial cybersecurity and reliability: This incident underscores the importance of basic cybersecurity practices in industrial settings, including timely software updates, strong access controls, and employee vigilance. It also highlights the potential for cyberattacks to have direct, life-threatening consequences in critical infrastructure.

CISA Alert on Ransomware Attacks Targeting Food and Agriculture Sector (2021)

In September 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about increasing ransomware attacks targeting the food and agriculture sector.

Key points:

1. Multiple ransomware attacks disrupted operations at meat processing plants and agricultural cooperatives.
2. One attack on a U.S. bakery company halted operations for a week, costing millions in lost revenue.
3. Another attack on a U.S. farm resulted in losses of approximately $9 million due to the temporary shutdown of farming operations.

Relevance to industrial cybersecurity and reliability: These incidents demonstrate the growing threat to the food and agriculture sector, an often overlooked but critical part of national infrastructure. They highlight the need for robust cybersecurity measures across all industrial sectors, not just traditional critical infrastructure.

Norsk Hydro Ransomware Attack (2019)

While slightly older, the 2019 cyberattack on Norsk Hydro, one of the world's largest aluminum producers, remains a significant case study in industrial cybersecurity.

Key points:

1. The attack used LockerGoga ransomware, forcing the company to halt production at several plants and switch to manual operations.
2. The total cost of the attack was estimated at $75 million.
3. Despite the severe impact, Norsk Hydro was praised for its transparent communication during the crisis.
4. The company's robust backup systems and preparedness allowed for a quicker recovery.

Relevance to industrial cybersecurity and reliability: This case demonstrates the importance of having comprehensive incident response plans, robust backup systems, and a strategy for transparent communication during cybersecurity crises. It also shows how cyber resilience can be a competitive advantage in the industrial sector.

Conclusions

These recent cases illustrate the evolving nature of cyber threats to industrial systems and critical infrastructure. They highlight several key points:

1. The increasing convergence of IT and OT systems creates new vulnerabilities that attackers are keen to exploit.
2. Ransomware has become a major threat to industrial operations, capable of causing significant economic damage and operational disruption.
3. Basic cybersecurity practices, including regular updates, strong access controls, and employee training, remain crucial in preventing attacks.
4. The potential impacts of industrial cyberattacks extend far beyond immediate financial losses, potentially affecting public safety, national security, and critical supply chains.
5. Preparedness, including robust backup systems and well-rehearsed incident response plans, is crucial for minimizing the impact of attacks and ensuring rapid recovery.

As industrial systems become more connected and digitalized, the importance of comprehensive, adaptive cybersecurity strategies that address both IT and OT vulnerabilities cannot be overstated. These incidents serve as stark reminders of the critical need for ongoing investment in industrial cybersecurity and reliability measures.

6 DIGITALIZATION OF ENERGY ASSETS FOR MEASURING RISK: ROADMAP FOR INSURANCE AND THE ROLE OF CYBERSECURITY AND RELIABILITY

The digital transformation of the energy sector has revolutionized how risk is measured and managed, particularly in the context of insurance. The integration of IoT technologies, artificial intelligence (AI), and advanced data analytics has facilitated a new era of risk assessment for energy assets. While data collection on energy asset safety has been ongoing for years, the rise of digital technologies has introduced new avenues for understanding and mitigating risks.

A critical component of this transformation is the focus on cybersecurity and operational reliability. As energy assets become increasingly connected and reliant on digital systems, they face evolving cyber threats and operational challenges that directly impact their insurability. The ability to manage and mitigate these risks not only improves operational resilience but also offers a tangible financial benefit in terms of reduced insurance premiums.

In today's landscape, whether an energy asset is using commercial insurance or opting for self-insurance, it can now be ranked based on the quality of its physical and digital assets. A "ranking" algorithm, enhanced with insights from operational data and cybersecurity posture, can generate a score ranging from "0" (worst practice) to "100" (best practice). This scoring is achieved using the Risk Control Advantage framework, ensuring that confidential and proprietary data of the asset remain secure and are not shared with third parties such as insurers or investors.

This comprehensive approach to digitalizing energy assets for risk measurement, emphases the crucial role of cybersecurity and reliability. It explores advanced methods of data collection, dynamic risk assessment, and innovative insurance models that reward robust cybersecurity and reliability practices. Recommendations are provided for both insurers and energy asset operators to adopt this integrated approach effectively.

6.1 Enhanced Data Collection and Integration

Modern energy assets are now equipped with a network of sensors and smart devices that continuously collect data on various operational parameters, including real-time performance, equipment health, environmental conditions, and cybersecurity status. This data is crucial for assessing risks and determining an asset's reliability.

The integration of 5G technology further enhances data transmission, enabling real-time monitoring and analysis. Data quality and frequency directly influence an asset's risk rating, with high-quality, frequently updated data contributing to more accurate risk assessments.

- Equipment Manufacturer: Coordinating data feeds with equipment manufacturers allows energy assets to receive updates on operational health, maintenance records, and firmware status. This information is vital for understanding asset reliability and evaluating risks.
- SCADA Systems: Secure measurement data, product quality metrics, and event logs provided through SCADA systems offer a unified view of asset health. Modern SCADA systems now integrate constant data feeds from cathodic protection (to prevent corrosion), leak detection, fire protection, and cybersecurity events.

6.2 Advanced Analytics and AI for Risk Measurement

AI and machine learning have become integral to analyzing the complex data sets generated by energy assets. These technologies enable:

- Predictive Maintenance: AI analyzes trends in sensor data to predict equipment failures before they occur. This proactive approach minimizes downtime, enhances reliability, and contributes to a more favorable risk profile for insurance purposes.
- Anomaly Detection: Machine learning algorithms identify unusual patterns that may indicate increased risks, such as signs of impending equipment failure or cybersecurity threats. Anomalies trigger early intervention, reducing the likelihood of operational disruptions and costly incidents.
- Dynamic Risk Scoring: AI-driven analytics develop real-time, dynamic risk profiles for assets, adjusting scores based on changes in the asset's condition, usage patterns, and cybersecurity posture. This allows insurers to assess risks more accurately and price policies accordingly.

6.3 Digital Twins and Scenario Testing

Digital twins—virtual replicas of physical assets—is an innovative tool in the energy sector for risk management:

- Scenario Testing: Digital twins allow operators to simulate various risk scenarios, including cyber threats and physical disruptions, without affecting real-world operations. This testing helps identify vulnerabilities and refine protective measures.
- Lifecycle Management: By tracking assets throughout their lifecycle, digital twins provide insights into maintenance history, component wear, and firmware updates. This comprehensive view of asset health informs long-term risk assessments and insurance pricing.

6.4 Blockchain for Data Integrity

Blockchain technology is increasingly used to enhance the security and integrity of data for risk assessment:

- Immutable Records: Blockchain creates an unalterable record of asset data, including operational history and cybersecurity events. This immutability builds trust in the data used for insurance purposes.
- Transparent Data Trails: Blockchain's decentralized nature provides transparent, auditable data trails, supporting insurers in verifying asset reliability and security practices.

6.5 Cybersecurity Risk Integration

Given the growing interconnectivity of energy assets, cybersecurity is now a central component of risk assessment:

- Real-Time Cybersecurity Posture: Unified platforms integrate real-time monitoring of cybersecurity events, including threat detection, vulnerability scanning, and incident response capabilities. These measures contribute to a robust risk profile, indicating to insurers that an asset is actively managing potential cyber threats.

- Historical Cyber Event Data: The availability of historical cybersecurity data provides insights into past vulnerabilities and resolutions. The frequency and severity of past incidents influence the overall risk rating, guiding insurers in setting premiums.

6.6 Regulatory Compliance and Digital Standards

Adopting cybersecurity and reliability standards is crucial for managing digital risks. Governments play a role in encouraging the adoption of both de jure standards (legally mandated) and de facto standards (best practices). By incorporating these standards into regulatory frameworks, the industry can achieve:

- Improved Market Compatibility: Common standards facilitate compatibility among different products and systems, simplifying the integration of cybersecurity solutions within energy assets.
- Reduced Developmental Stress: Standards streamline digital operations, making it easier to implement comprehensive cybersecurity measures across the industry.

6.7 Dynamic Pricing Models for Insurance

The use of real-time data has enabled insurers to develop more dynamic pricing models:

- Usage-Based Insurance (UBI): Premiums are adjusted based on the asset's real-time operation and usage patterns. Assets demonstrating adherence to cybersecurity best practices, such as regular patching, network segmentation, and incident response readiness, receive lower premiums.
- Parametric Insurance: IoT sensors and smart contracts enable automatic payouts based on predefined events, such as system failures or breaches. By incorporating cybersecurity and reliability data into this model, assets can prevent payouts by proactively mitigating risks, resulting in lower insurance costs.

6.8 Roadmap for Insurance and Risk Control

As digitalization reshapes the energy sector, insurers are leveraging sophisticated analytics to measure risk. This approach considers:

1. Asset Usage Patterns: Evaluating the frequency and intensity of asset usage, along with real-time reliability metrics.
2. Real-Time Health Data: Incorporating data on component health, predictive maintenance activities, and cybersecurity status.
3. Cybersecurity Integration: Assessing the implementation of cybersecurity measures, including firmware updates, security patches, and incident response capabilities.
4. Environmental Performance: Factoring in sustainability practices, which align with Environmental, Social, and Governance (ESG) considerations.

6.9 Incorporating Resilience and Emerging Risks

Modern risk assessment models now account for the resilience of energy assets to emerging risks:

- Climate Change Impact Modeling: Assessing the risk of climate-induced disruptions and integrating adaptive strategies.
- Geopolitical Risk Assessment: Evaluating the impact of geopolitical events on operations, supply chains, and cybersecurity.
- Supply Chain Disruption Scenarios: Analyzing the cybersecurity practices of suppliers to identify vulnerabilities in the supply chain.

6.10 Innovative Insurance Models Based on Cybersecurity and Reliability

6.10.1 Linking Cybersecurity and Reliability to Risk Reduction

Incorporating cybersecurity and reliability measures into daily operations offers advantages that directly affect risk assessment:

1. Minimized Operational Downtime: Robust cybersecurity practices prevent disruptions caused by cyber-attacks, resulting in lower downtime risks and reduced premiums.
2. Predictable Maintenance: Reliable assets that utilize predictive maintenance have fewer unexpected failures, enhancing stability and favorably impacting insurance costs.
3. Enhanced Data Integrity: Secure data management practices ensure data integrity, enabling more precise risk assessments and better insurance pricing.
4. Resilience to Cyber Threats: Defense-in-depth strategies demonstrate an asset's resilience, making it a lower-risk investment for insurers.

6.10.2 Recommendations for Insurers and Energy Asset Operators

6.10.2.1 For Insurers:

- Develop Risk Scoring Models: Incorporate cybersecurity and reliability metrics into risk assessment algorithms to align premiums with actual risk levels.
- Offer Premium Discounts for Cybersecurity Compliance: Incentivize operators to adopt cybersecurity standards (ISO/IEC 27001, IEC 62443) by offering reduced premiums.
- Implement Real-Time Risk Monitoring: Integrate systems with operators' monitoring platforms for flexible premium adjustments based on current risk posture.

6.10.2.2 For Energy Asset Operators:

- Invest in Comprehensive Cybersecurity Measures: Adopt a multi-layered cybersecurity strategy, including endpoint security, network segmentation, and real-time monitoring.
- Prioritize Predictive Maintenance: Use digital twins and predictive maintenance tools to minimize equipment failures, providing insurers with favorable risk data.
- Adopt Secure-by-Design Principles: Incorporate cybersecurity into asset design to demonstrate a lower risk profile and qualify for reduced premiums.

6.11 Summary

The digitalization of energy assets has transformed risk measurement and insurance in the energy sector. By integrating comprehensive cybersecurity and reliability practices, energy asset operators can significantly lower their risk profiles. This innovative approach aligns insurance costs with actual risk levels, offering financial incentives for robust cybersecurity and reliability measures.

For insurers, adopting dynamic pricing models based on real-time data and risk scoring algorithms allows for more accurate risk assessments. Meanwhile, energy asset operators that invest in predictive maintenance, secure data management, and defense-in-depth cybersecurity strategies can enjoy tangible benefits in terms of lower insurance premiums.

As the energy sector continues to evolve, the combined focus on cybersecurity, operational reliability, and digital innovation will be key to achieving a more secure, resilient, and cost-effective future in risk management.

7 DEVELOPING COMPETENCIES AND TRAINING IN INDUSTRIAL CYBERSECURITY AND RELIABILITY

7.1 Cybersecurity and Reliability Management in the Industrial Sector

This chapter has explored the critical importance of developing competencies and training programs in reliability and cybersecurity management for the industrial sector. It began by examining the unique challenges faced by the industrial sector in the era of Industry 4.0, including the convergence

The chapter also made a strong case for the need to introduce professional competencies in industrial cybersecurity as an important element of overall cybersecurity strategy. We explored the various benefits of these competencies, from bridging the skills gap to enhancing organizational resilience and driving innovation. Finally, we looked at future directions and emerging trends in industrial cybersecurity competencies, considering the impact of technologies like AI, IoT, and quantum computing on the future skill requirements for industrial cybersecurity professionals.

7.1.1 The Evolving Cybersecurity Landscape in Industry 4.0

The fourth industrial revolution, characterized by the fusion of advanced technologies, is reshaping the very fabric of industrial operations. This transformation, while offering immense potential for increased efficiency and innovation, also introduces a new spectrum of cybersecurity risks that demand our attention and expertise.

The integration of Operational Technology (OT) with Information Technology (IT) marks a significant shift in how industrial operations are conducted. OT, which includes hardware and software that monitors and controls physical devices and processes, has traditionally been isolated from IT systems. However, the advent of Industry 4.0 has blurred these lines, leading to a more interconnected and interdependent environment. This convergence brings several benefits, including improved efficiency, reduced operational costs, and enhanced data analysis capabilities. Nevertheless, it also introduces a range of cybersecurity challenges that must be addressed.

One of the fundamental challenges in integrating OT with IT is the difference in their operational objectives and design philosophies. OT systems are typically designed with a primary focus on reliability, safety, and real-time responsiveness. In contrast, IT systems prioritize data integrity, confidentiality, and availability. This divergence in priorities can lead to vulnerabilities when the two systems interact. For instance, the real-time operational requirement of OT systems often means that they cannot afford downtime for updates or patches, a standard security practice in IT systems. This discrepancy can leave OT systems exposed to cyber threats.

Moreover, the increased connectivity in industrial environments expands the attack surface for potential cyber threats. Traditional isolated OT systems had limited exposure to external threats, but now, as they become more integrated with IT networks, they are more susceptible to a wide range of cyberattacks. These attacks can have severe consequences, not just in terms of data loss or theft but also in physical damage to equipment and disruptions to critical industrial processes.

The proliferation of Internet of Things (IoT) devices and Industrial Internet of Things (IIoT) sensors further compounds this challenge. These devices, often deployed in vast numbers across industrial facilities, create a multitude of potential vulnerabilities if not properly secured. The ability to remotely access and control industrial systems, while operationally beneficial, introduces additional risks that must be carefully managed.

Addressing these evolving challenges requires a new breed of cybersecurity professional – one who understands not only the intricacies of digital security but also the unique operational demands of industrial environments. This emerging field demands a blend of skills that bridges the gap between IT and OT, combining traditional cybersecurity knowledge with a deep understanding of industrial processes and control systems.

7.1.2 Legal and Regulatory Framework

Integrated Qualification System

In response to these evolving needs, Poland has developed the Integrated Qualification System, a framework that standardizes and recognizes professional qualifications across various sectors, including industrial cybersecurity. This system aims to ensure consistency in competency levels among cybersecurity professionals and supports the development of targeted training programs to meet the sector's growing demands.

Poland's Integrated Qualification System (IQS) represents an innovative approach to standardizing and recognizing professional qualifications across various sectors, including cybersecurity. Established by the Act on the Integrated Qualification System of 22 December 2015, the IQS aims to improve the quality and effectiveness of qualifications in Poland, aligning them with the European Qualifications Framework.

Key aspects of the IQS

Key aspects of the IQS relevant to industrial cybersecurity include:

1. Standardization of Qualifications: The IQS provides a unified framework for describing, assessing, and certifying qualifications, ensuring consistency across different sectors and professions.
2. Market Qualifications: The system allows for the inclusion of "market qualifications" - skills and knowledge sets that respond to current market needs, including emerging fields like industrial cybersecurity.
3. Validation and Quality Assurance: The IQS includes mechanisms for validating qualifications and ensuring the quality of education and training programs.
4. Lifelong Learning Support: By recognizing various forms of learning, including non-formal and informal education, the IQS supports continuous professional development - a crucial aspect in the rapidly evolving field of cybersecurity.
5. Transparency and Comparability: The system enhances the transparency and comparability of qualifications, both within Poland and across the European Union.

For industrial cybersecurity, the IQS plays a vital role in defining and standardizing the competencies required for professionals in this field. It provides a framework for developing targeted training programs and certifications, ensuring that the workforce is equipped with the skills necessary to address the unique cybersecurity challenges of industrial environments.

7.1.3 NIS 2 Directive: Reshaping Industrial Cybersecurity and Reliability

The Network and Information Systems Security 2 (NIS 2) Directive, adopted by the European Union in January 2023, marks a significant evolution in the EU's approach to cybersecurity. As a successor to the original NIS Directive of 2016, NIS 2 addresses the rapidly changing digital landscape and the increasing interconnectedness of industrial systems. This directive has far-reaching implications for industrial cybersecurity and reliability, setting new standards and expectations for organizations across the EU.

The transition from NIS to NIS 2 reflects the EU's recognition of the evolving threat landscape and the critical role of cybersecurity in maintaining economic stability and public safety. While the original NIS Directive laid the groundwork for a coordinated EU approach to cybersecurity, NIS 2 significantly expands its scope and introduces more stringent requirements. This evolution is particularly relevant for industrial sectors, where the convergence of Information Technology (IT) and Operational Technology (OT) has created new vulnerabilities and increased the potential impact of cyber incidents.

Key features of NIS 2 and their impact on industrial cybersecurity and reliability are the following.

1. Broader Sector Coverage

NIS 2 expands its scope to include additional sectors deemed critical for the economy and society. This expansion is particularly significant for industrial cybersecurity, as it now encompasses:

- Manufacturing of critical products (e.g., pharmaceuticals, medical devices, semiconductors)
- Chemical industry
- Food production and distribution
- Waste management
- Digital infrastructure providers

Implication for Industry: This broader coverage means that many industrial organizations previously outside the scope of NIS now fall under stringent cybersecurity regulations. These organizations must rapidly develop or enhance their cybersecurity capabilities to ensure compliance and protect their operations.

2. Strengthened Security Requirements

NIS 2 introduces more prescriptive and detailed security requirements, moving beyond the high-level guidelines of its predecessor. For industrial organizations, this includes:

- Mandatory implementation of state-of-the-art technical and organizational measures
- Regular cybersecurity risk assessments
- Supply chain security measures
- Encryption and multi-factor authentication implementation
- Comprehensive incident response plans

Implication for Industry: Industrial organizations must now adopt a more structured and comprehensive approach to cybersecurity. This may require significant investments in technology, processes, and personnel to meet these enhanced requirements.

3. More Stringent Supervisory Measures

The directive grants national authorities enhanced powers to supervise and enforce compliance. This includes:

- The ability to conduct security audits
- Request information and evidence of effective implementation of security policies
- Issue binding instructions to remedy identified deficiencies

Implication for Industry: Industrial organizations must be prepared for more frequent and thorough regulatory scrutiny. This necessitates maintaining detailed documentation of security practices and being ready to demonstrate compliance at any time.

4. Stricter Enforcement Requirements

NIS 2 introduces harmonized sanctions across the EU, including significant administrative fines. The maximum penalties can reach €10 million or 2% of global annual turnover, whichever is higher.

Implication for Industry: The potential for severe financial penalties elevates cybersecurity from an IT issue to a board-level concern. Industrial organizations must prioritize cybersecurity investments and ensure ongoing compliance to avoid these substantial fines.

5. Enhanced Cooperation and Information Exchange

The directive promotes increased cooperation and information sharing between member states, including the establishment of the European Cyber Crises Liaison Organisation Network (EU-CyCLONe).

Implication for Industry: Industrial organizations can benefit from improved threat intelligence and best practices shared across the EU. However, they must also be prepared to participate actively in information sharing initiatives, which may require changes to internal policies and procedures.

6. Supply Chain Security

NIS 2 explicitly addresses the security of supply chains and supplier relationships, recognizing their critical role in overall organizational security.

Implication for Industry: Industrial organizations must extend their cybersecurity considerations beyond their immediate operations to include their entire supply chain. This requires developing new processes for vendor assessment, ongoing monitoring, and collaborative security efforts with suppliers.

7. Streamlined Reporting Obligations

The directive aims to eliminate divergence in incident reporting requirements, establishing more uniform reporting obligations across the EU.

Implication for Industry: While this streamlining may simplify compliance in the long term, industrial organizations must adapt their incident response and reporting processes to meet these new, unified standards.

7.1.4 Relevance to Industrial Cybersecurity and Reliability

The NIS 2 Directive's requirements have profound implications for both cybersecurity and reliability in industrial settings:

1. **Integrated Approach to Security and Reliability**

NIS 2 implicitly recognizes the intrinsic link between cybersecurity and reliability in industrial environments. By mandating comprehensive risk assessments and security measures, the directive drives organizations to consider how cyber incidents could impact operational reliability.

Industrial organizations must now develop integrated strategies that address both cybersecurity threats and reliability concerns simultaneously. This might involve:

- Conducting joint cybersecurity and reliability risk assessments
- Implementing security measures that enhance both cyber resilience and operational reliability
- Developing incident response plans that address both cyber incidents and their potential impact on operational continuity

2. **Emphasis on Operational Technology (OT) Security**

While not explicitly mentioned, NIS 2's broader scope inherently places greater emphasis on OT security. This is crucial for industrial organizations where OT systems are critical for operations.

Industrial entities must now:

- Implement security measures specifically designed for OT environments
- Ensure the security of industrial control systems (ICS) and SCADA systems
- Address the unique challenges of securing legacy OT systems that may not have been designed with modern cybersecurity in mind

3. **Resilience and Business Continuity**

NIS 2's requirements for incident response planning and risk management inherently promote operational resilience and business continuity. Industrial organizations must now:

- Develop comprehensive business continuity plans that account for cyber incidents
- Implement redundancy and failover mechanisms to ensure operational continuity in the face of cyber attacks
- Regularly test and update these plans to ensure their effectiveness

4. **Skills Development and Workforce Implications**

The directive's stringent requirements create a significant demand for cybersecurity skills in industrial settings. Organizations must:

- Invest in training and development programs to upskill existing staff
- Recruit specialists with expertise in both cybersecurity and industrial operations
- Develop a culture of security awareness across all levels of the organization

5. **Technology Investment and Innovation**

To meet NIS 2 requirements, industrial organizations will need to invest in advanced cybersecurity technologies. This may drive innovation in areas such as:

- OT-specific security solutions
- AI and machine learning for threat detection in industrial environments
- Secure-by-design ICS and SCADA systems

6. Standardization and Interoperability

The directive's push for harmonized approaches across the EU may lead to greater standardization in industrial cybersecurity practices. This could result in:

- Development of EU-wide standards for industrial cybersecurity
- Improved interoperability between security solutions
- Easier collaboration and information sharing across borders

In conclusion, the NIS 2 Directive represents a significant step forward in the EU's approach to cybersecurity, with far-reaching implications for industrial organizations. By setting stringent requirements and promoting a harmonized approach across member states, NIS 2 is set to reshape the landscape of industrial cybersecurity and reliability.

For industrial organizations, compliance with NIS 2 is not just a regulatory obligation but an opportunity to enhance their overall security posture and operational resilience. As cyber threats continue to evolve and industrial systems become increasingly interconnected, the principles enshrined in NIS 2 will be crucial in safeguarding Europe's industrial infrastructure.

Moving forward, organizations must view NIS 2 compliance as part of a broader strategy to integrate cybersecurity and reliability considerations into every aspect of their operations. This holistic approach will not only ensure regulatory compliance but also position industrial organizations to thrive in an increasingly digital and interconnected world.

7.2 Management of Reliability and Cybersecurity for Industrial Devices

7.2.1 General statement

As industrial devices become increasingly interconnected and integrated into broader networks, the task of managing their reliability and cybersecurity grows ever more critical and complex. These devices, ranging from simple sensors to sophisticated control systems, form the backbone of modern industrial operations. Ensuring their security and reliability is paramount not only for operational continuity but also for safety, data integrity, and regulatory compliance.

The stakes in industrial cybersecurity are exceptionally high. A successful cyber attack or a significant reliability issue can lead to production downtime, resulting in substantial financial losses. More critically, compromised industrial devices can pose serious safety risks to personnel and the environment. The integrity of industrial data, crucial for informed decision-making and regulatory compliance, relies heavily on the security and reliability of these devices. Furthermore, in an age where brand reputation can be irreparably damaged by a single security breach, the importance of robust cybersecurity measures cannot be overstated.

7.2.2 Importance of Cybersecurity and Reliability in Industrial Devices

In the era of Industry 4.0, industrial devices have become the cornerstone of modern manufacturing and process control. These devices, ranging from simple sensors to complex Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCS), form an intricate network that drives production, ensures quality, and maintains safety in industrial environments. As these systems become increasingly interconnected and digitized, the importance of their cybersecurity and reliability has grown exponentially. This section delves into the multifaceted reasons why ensuring the cybersecurity and reliability of industrial devices is paramount in today's industrial landscape.

1. **Operational Continuity and Economic Impact.** The primary function of industrial devices is to ensure smooth, efficient, and continuous operations. Any disruption to these devices, whether due to a cyber attack or a reliability issue, can have severe economic consequences. In industries such as oil and gas, chemical processing, or power generation, even a few minutes of downtime can result in losses amounting to millions of dollars. For instance, a 2017 cyber attack on a petrochemical plant in Saudi Arabia was specifically designed to sabotage operations and trigger an explosion. While the attack was thwarted, it highlighted the potential for massive economic and human costs.

Moreover, in today's globalized supply chains, a disruption in one facility can have far-reaching consequences. The 2021 Colonial Pipeline ransomware attack in the United States demonstrated how a cyber incident affecting industrial control systems could lead to fuel shortages across multiple states, impacting various sectors of the economy. This interconnectedness means that the reliability and security of industrial devices are not just a concern for individual companies but can have national and even global economic implications.

2. **Safety and Environmental Concerns.** Industrial devices often control processes that, if compromised, could pose serious risks to human life and the environment. This is particularly true in industries dealing with hazardous materials or high-energy processes. For example:

- In a chemical plant, compromised control systems could lead to uncontrolled reactions, potentially resulting in toxic releases or explosions.
- In a nuclear power plant, a breach in the safety systems could have catastrophic consequences, as evidenced by historical incidents like Chernobyl or more recent events like the cyber attacks on Ukrainian power grids.
- In water treatment facilities, manipulation of industrial controls could lead to the release of untreated water, posing significant public health risks.

The Stuxnet worm, discovered in 2010, demonstrated the potential for cyber attacks to cause physical damage to industrial equipment, specifically targeting nuclear centrifuges. This case underscored how compromised industrial devices could lead to not just operational disruptions but also potential environmental and safety disasters.

3. **Data Integrity and Decision-Making.** In modern industrial environments, data is as valuable as the physical products. Industrial devices generate, process, and transmit vast amounts of data that inform critical decision-making processes. This data is used for:

- Quality control and assurance
- Predictive maintenance
- Resource allocation and optimization
- Compliance reporting
- Research and development

The integrity of this data is crucial. If compromised, it could lead to:

- Production of faulty or substandard goods
- Missed maintenance leading to equipment failure
- Inefficient resource utilization

- Regulatory non-compliance and associated penalties
- Misguided strategic decisions based on corrupted data

For instance, in the pharmaceutical industry, data integrity is crucial for ensuring drug safety and efficacy. A cyber attack that compromises the integrity of manufacturing data could lead to the production of ineffective or even harmful medications, with severe consequences for public health and the company's reputation.

4. **Brand Reputation and Customer Trust.** In an age of heightened cybersecurity awareness, a single security breach can have long-lasting impacts on a company's reputation. The costs associated with reputational damage often far exceed the immediate financial losses from an incident. Consider the following aspects:

- Media Coverage: Cybersecurity incidents, especially those affecting critical infrastructure or consumer data, often receive extensive media coverage, amplifying reputational damage.
- Customer Trust: In B2B relationships, a cybersecurity incident can lead to a loss of trust from clients who rely on the security and reliability of their suppliers' systems.
- Market Value: Public companies often see significant drops in stock prices following the disclosure of major cyber incidents, reflecting investor concerns about the company's risk management capabilities.
- Competitive Disadvantage: In highly competitive industries, a cybersecurity incident can be exploited by competitors to gain market share.

The Norsk Hydro ransomware attack in 2019 serves as a case study in both the potential damage and the importance of transparent incident response. While the company faced significant operational disruptions and financial losses, its transparent and proactive communication strategy helped maintain stakeholder trust.

5. **Regulatory Compliance and Legal Implications**. The regulatory landscape surrounding industrial cybersecurity is becoming increasingly complex and stringent. Various sectors are subject to specific regulations:

- Energy Sector: Regulations like NERC CIP in North America set cybersecurity standards for the power grid.
- Chemical Industry: Regulations such as CFATS in the US mandate specific security measures for high-risk chemical facilities.
- Healthcare and Pharmaceuticals: Regulations like FDA 21 CFR Part 11 govern electronic records and signatures in drug manufacturing.
- Critical Infrastructure: The EU's NIS Directive and its successor, NIS2, set cybersecurity standards across various critical sectors.

Non-compliance with these regulations can result in:

- Substantial fines and penalties
- Mandatory third-party audits
- Operational restrictions or shutdowns
- Criminal liability for executives in extreme cases

Moreover, the legal landscape is evolving to place greater responsibility on organizations for maintaining the security and reliability of their systems. This includes potential liability for damages caused by cyber incidents, especially if negligence in maintaining adequate security measures can be demonstrated.

6. Technological Innovation and Competitive Advantage. Secure and reliable industrial devices are not just about risk mitigation; they also enable technological innovation and can provide a competitive advantage. Organizations with robust cybersecurity and reliability measures are better positioned to:

- Adopt new technologies like AI, machine learning, and advanced analytics
- Implement more efficient and flexible manufacturing processes
- Offer innovative products and services that leverage interconnected industrial systems
- Collaborate securely with partners and suppliers in digital ecosystems

For example, companies implementing secure Industrial Internet of Things (IIoT) solutions can achieve higher levels of operational efficiency, predictive maintenance, and quality control, giving them an edge over competitors.

7. National Security Considerations: In an era of increasing geopolitical tensions and cyber warfare, the security of industrial devices takes on national security implications. Critical infrastructure sectors like energy, water, transportation, and defense industrial base are potential targets for nation-state actors. Compromised industrial systems could be used to:

- Disrupt essential services
- Cause economic damage
- Create public panic
- Serve as leverage in international conflicts

The NotPetya malware attack in 2017, which significantly impacted global shipping giant Maersk among others, demonstrated how cyber attacks on industrial systems could have widespread, cross-border impacts.

Conclusion: The importance of cybersecurity and reliability in industrial devices cannot be overstated. These systems form the operational backbone of modern industry and critical infrastructure. Their compromise can lead to far-reaching consequences that extend beyond immediate operational disruptions to impact public safety, environmental integrity, economic stability, and even national security. As industrial systems become more interconnected and digitally dependent, ensuring their security and reliability becomes not just a technical challenge but a fundamental business imperative and a matter of societal importance.

7.3. The Need for Professional Competencies in Industrial Cybersecurity

The rapidly evolving landscape of industrial cybersecurity, driven by the convergence of IT and OT systems and the increasing sophistication of cyber threats, has created an urgent need for specialized professional competencies. This section explores the multifaceted reasons why developing these competencies is crucial for the future of industrial sectors.

7.3.1 Bridging the Skills Gap

The industrial sector faces a significant shortage of cybersecurity professionals with the specialized knowledge required to protect complex industrial environments. This skills gap is not just a matter of quantity, but also of quality – many IT security professionals lack the specific understanding of industrial processes and control systems necessary to effectively secure OT environments.

The gap is exacerbated by several factors:

1. Rapid digital transformation of industries outpacing the development of relevant cybersecurity skills.
2. The unique requirements of OT security, which often differ significantly from traditional IT security approaches.
3. An aging workforce in many industrial sectors, leading to a loss of institutional knowledge about legacy systems.

To bridge this gap, industries must:

1. Invest in specialized training programs that combine IT security knowledge with OT-specific skills.
2. Collaborate with educational institutions to develop curricula that address the unique needs of industrial cybersecurity.
3. Implement mentorship programs to facilitate knowledge transfer from experienced professionals to newcomers.
4. Encourage cross-training between IT and OT teams to foster a more holistic understanding of industrial cybersecurity challenges.

7.3.2 Adapting to Evolving Threats

The threat landscape in industrial cybersecurity is constantly evolving, with new vulnerabilities and attack vectors emerging regularly. This dynamic environment requires professionals who can not only understand current threats but also anticipate and prepare for future challenges.

Key aspects of this adaptability include:

1. Continuous threat intelligence gathering and analysis specific to industrial environments.
2. Understanding of emerging technologies like AI, 5G, and quantum computing, and their potential impact on industrial cybersecurity.
3. Ability to develop and implement adaptive defense strategies that can evolve with the threat landscape.
4. Skills in conducting regular risk assessments to identify new vulnerabilities in industrial systems.

Professionals must be equipped with the skills to:

1. Interpret and act on threat intelligence in the context of industrial operations.
2. Implement and manage advanced threat detection and response systems tailored to OT environments.
3. Conduct penetration testing and vulnerability assessments on industrial control systems.
4. Develop and update incident response plans that address the unique challenges of cyber-physical systems.

7.3.3 Enhancing Organizational Resilience

Cybersecurity competencies play a crucial role in enhancing the overall resilience of industrial organizations. This goes beyond merely preventing cyber attacks to ensuring that organizations can maintain critical functions and recover quickly in the face of disruptions.

Key areas where cybersecurity competencies contribute to organizational resilience include:

1. Business Continuity Planning: Integrating cybersecurity considerations into broader business continuity and disaster recovery plans.
2. Incident Response: Developing and implementing effective incident response strategies that minimize operational disruptions.
3. Supply Chain Security: Understanding and mitigating cybersecurity risks throughout the industrial supply chain.
4. Cyber-Physical Systems Protection: Ensuring the security and reliability of systems where digital and physical components intersect.

Professionals need to develop skills in:

1. Conducting business impact analyses that consider both cyber and physical risks.
2. Designing and implementing resilient industrial control systems that can withstand or quickly recover from cyber attacks.
3. Developing and testing comprehensive incident response plans that address both cybersecurity and operational continuity.
4. Implementing secure-by-design principles in the development and deployment of industrial systems.

7.3.4 Supporting Digital Transformation

As industries undergo digital transformation, cybersecurity competencies become crucial enablers of innovation and growth. Secure digitalization is not just about protecting against threats, but about creating a foundation for the safe adoption of new technologies and business models.

Key areas where cybersecurity competencies support digital transformation include:

1. Industrial Internet of Things (IIoT): Ensuring the secure implementation and operation of connected devices and sensors.
2. Cloud Integration: Enabling the secure use of cloud services in industrial environments.
3. Data Analytics and AI: Protecting the integrity and confidentiality of data used in advanced analytics and AI applications.
4. Remote Operations: Securing systems for remote monitoring and control of industrial processes.

Professionals need to develop competencies in:

1. Secure architecture design for IIoT deployments.
2. Cloud security strategies tailored to industrial data and applications.
3. Data protection and privacy in the context of big data analytics and AI.
4. Secure implementation of remote access technologies for industrial control systems.

7.3.5 Driving Economic Growth and Innovation

Strong industrial cybersecurity competencies can be a significant driver of economic growth and innovation. By enabling the secure adoption of new technologies and business models, these competencies can help industrial organizations:

1. Improve operational efficiency and productivity through secure digitalization.
2. Develop new products and services that leverage connected technologies.
3. Enter new markets with confidence in the security of their digital infrastructure.
4. Build trust with customers and partners through demonstrated cybersecurity capabilities.

Moreover, the development of industrial cybersecurity competencies can itself become a source of economic growth by:

1. Creating new job opportunities in the field of industrial cybersecurity.
2. Fostering the development of cybersecurity products and services tailored to industrial needs.
3. Enhancing the competitiveness of national industries in the global market.
4. Attracting investment in secure industrial technologies and infrastructure.

To realize these benefits, professionals need to develop competencies that blend cybersecurity expertise with business acumen, including:

1. Understanding of the economic impact of cybersecurity measures on industrial operations.
2. Ability to articulate the business case for cybersecurity investments.
3. Skills in identifying and developing new business opportunities enabled by secure industrial technologies.
4. Knowledge of global industrial cybersecurity trends and their implications for competitiveness.

In conclusion, the development of professional competencies in industrial cybersecurity is not just a technical necessity but a strategic imperative for the future of industrial sectors. These competencies are crucial for bridging the current skills gap, adapting to evolving threats, enhancing organizational resilience, supporting digital transformation, and driving economic growth and innovation. As industries continue to evolve in the digital age, investing in these competencies will be key to ensuring not only the security but also the prosperity of industrial organizations in an increasingly interconnected world.

7.4 Developing Professional Competencies and Training Programs

The evolving landscape of industrial cybersecurity demands a workforce equipped with specialized skills and knowledge. This section outlines three key qualifications that have been developed to address the growing need for expertise in this field.

7.4.1 Key Qualifications for Industrial Cybersecurity

Three qualifications have been developed for professionals seeking to navigate the complex intersection of cybersecurity, industrial processes, and regulatory compliance. These qualifications, designed to meet the growing demands of Industry 4.0 and align with frameworks such as NIS 2, offer a comprehensive approach to developing expertise in industrial cybersecurity and reliability.

These qualifications encompass a broad range of competencies, including:

1. Technical Knowledge:
   - Deep understanding of industrial devices and systems
   - Knowledge of device design, operation, and potential vulnerabilities
   - Familiarity with industrial control systems and their architectures
   - Understanding of industrial communication protocols and their security implications
2. Cybersecurity Skills:
   - Proficiency in cybersecurity principles and practices specific to industrial contexts
   - Knowledge of cybersecurity frameworks (e.g., NIST Cybersecurity Framework, IEC 62443)
   - Skills in threat detection and incident response
   - Ability to implement and manage security measures in OT environments
3. Risk Management:
   - Ability to conduct comprehensive risk assessments for industrial devices
   - Skills in developing and implementing risk mitigation strategies
   - Understanding of risk quantification methodologies for industrial environments
   - Knowledge of risk communication techniques for various stakeholders
4. Legal and Regulatory Compliance:
   - Familiarity with relevant legal and regulatory requirements (e.g., National Cybersecurity System Act)
   - Understanding of industry-specific regulations and standards
   - Ability to ensure compliance of cybersecurity measures with legal standards
   - Knowledge of international cybersecurity regulations affecting industrial sectors
5. Problem-Solving and Analytical Skills:
   - Capacity to analyze complex cybersecurity problems in industrial settings
   - Ability to troubleshoot device malfunctions and security incidents
   - Skills in root cause analysis for cybersecurity events
   - Proficiency in using analytical tools for security assessments
6. Communication and Training:
   - Skills in communicating complex cybersecurity and reliability concepts to non-technical audiences
   - Ability to develop and deliver effective cybersecurity training programs
   - Proficiency in creating awareness campaigns for industrial cybersecurity
   - Capacity to facilitate cross-functional collaboration on cybersecurity initiatives

7.4.1.1 Shaping Reliability and Cybersecurity Policy in Industry

This qualification is tailored for senior managers, policy makers, and strategists within industrial organizations. It is particularly relevant for those responsible for developing and implementing cybersecurity and reliability policies at an organizational level. This includes Chief Information Security Officers (CISOs), IT Directors, and Operations Managers in industrial settings who need to align cybersecurity strategies with business objectives and regulatory requirements.

The qualification recognizes that effective cybersecurity in industrial environments requires a holistic approach that balances technical knowledge with strategic thinking. It equips professionals with the skills to develop comprehensive policies that address the unique challenges of securing industrial control systems while ensuring operational reliability.

Competencies and curriculum focus:

1. Industrial Process Understanding: In-depth knowledge of industrial processes and control systems, including their vulnerabilities and critical points.
2. Regulatory Compliance: Comprehensive understanding of relevant cybersecurity standards, regulations, and frameworks, including NIS 2, ISO 27001, and IEC 62443.
3. Risk Assessment and Management: Advanced skills in conducting risk assessments specific to industrial environments and developing mitigation strategies.
4. Policy Development: Ability to craft comprehensive cybersecurity policies that align with business objectives and regulatory requirements.
5. Stakeholder Management: Skills in communicating complex cybersecurity concepts to various stakeholders and gaining buy-in for security initiatives.
6. Incident Response Planning: Expertise in developing and implementing incident response plans tailored to industrial settings.
7. Security Awareness Program Development: Capability to design and implement effective security awareness programs for industrial personnel.

Key learning outcomes:

Upon completion of this qualification, professionals will be able to:

1. Develop comprehensive, industry-specific cybersecurity policies that align with both organizational goals and regulatory requirements.
2. Conduct thorough risk assessments of industrial environments, identifying potential vulnerabilities in both IT and OT systems.
3. Create and implement strategic plans for enhancing the overall cybersecurity posture of industrial organizations.
4. Design and manage security awareness programs tailored to the unique needs of industrial settings.
5. Effectively communicate cybersecurity risks and strategies to both technical and non-technical stakeholders.
6. Develop and oversee the implementation of incident response plans that address the specific challenges of industrial cyber incidents.

This qualification provides immense value to both the individual and the organization. For professionals, it offers a pathway to senior leadership roles in industrial cybersecurity, enhancing their ability to influence organizational strategy and drive security initiatives. For organizations, it ensures that their cybersecurity policies are not only robust and compliant but also aligned with business objectives and operational realities. This alignment is crucial for maintaining a strong security posture without compromising on productivity or innovation, ultimately contributing to the overall resilience and competitiveness of the organization in an increasingly digital industrial landscape.

7.4.1.2 Management of Reliability and Cybersecurity in the Scope of Devices and Technology in Industry

This qualification is designed for technical specialists, system architects, and operational technology (OT) security professionals working directly with industrial control systems and devices. It is particularly relevant for automation engineers, ICS security specialists, and IT professionals transitioning into OT environments who need to understand and implement security measures at the device and system level.

The qualification addresses the unique challenges of securing industrial devices and technologies, recognizing that traditional IT security approaches often fall short in OT environments. It provides professionals with the technical expertise to secure industrial control systems while maintaining their operational integrity and reliability.

Competencies and curriculum focus:

1. Industrial Control Systems (ICS) Security: In-depth knowledge of ICS architectures, protocols, and security considerations.
2. Network Security: Advanced understanding of industrial network protocols and security measures, including segmentation and firewalls.
3. Vulnerability Assessment: Skills in identifying and assessing vulnerabilities in industrial devices and systems.
4. Secure System Design: Ability to apply secure-by-design principles to industrial systems and architectures.
5. Patch Management: Expertise in developing and implementing patch management strategies for industrial environments.
6. Industrial IoT Security: Understanding of security implications and best practices for Industrial Internet of Things (IIoT) deployments.
7. Operational Technology (OT) Security Monitoring: Skills in implementing and managing security monitoring solutions for OT environments.

Key learning outcomes:

Upon completion of this qualification, professionals will be able to:

1. Design and implement secure architectures for industrial control systems that balance security with operational requirements.
2. Conduct comprehensive vulnerability assessments of industrial devices and networks, identifying potential weaknesses and proposing mitigation strategies.
3. Develop and manage effective patch management processes for industrial systems, ensuring security without compromising operational stability.
4. Implement and manage security monitoring solutions tailored to OT environments, enabling early detection of potential security incidents.
5. Apply secure-by-design principles to new and existing industrial systems, enhancing their overall security posture.
6. Develop and implement security strategies for IIoT deployments, addressing the unique challenges of securing distributed and often resource-constrained devices.

This qualification is invaluable for organizations looking to enhance the security of their industrial devices and systems. It ensures that technical professionals have the specialized knowledge needed to secure complex OT environments, reducing the risk of cyber incidents that could impact production, safety, or environmental integrity. For individuals, it offers a path to becoming highly sought-after specialists in the growing field of industrial cybersecurity, bridging the gap between IT security and OT operational requirements.

7.4.1.3 Management of Reliability and Cybersecurity in Industry

This qualification is aimed at senior cybersecurity managers, operations executives, and strategic decision-makers responsible for overseeing cybersecurity and reliability across entire industrial organizations or sectors. It is particularly suited for professionals moving into leadership roles who need to understand how to integrate cybersecurity considerations into broader business strategies and operations.

The qualification takes a holistic view of industrial cybersecurity, focusing on how to manage security and reliability at an organizational level. It emphasizes the integration of cybersecurity with business continuity, operational resilience, and strategic planning.

Competencies and curriculum focus:

1. Cybersecurity Strategy Development: Ability to develop comprehensive, long-term cybersecurity strategies aligned with business objectives.
2. Operational Resilience: Understanding of how to integrate cybersecurity measures with broader operational resilience and business continuity planning.
3. Supply Chain Security: Knowledge of supply chain security risks and mitigation strategies in industrial contexts.
4. Cyber-Physical Systems Security: Understanding of the unique security challenges posed by cyber-physical systems in industrial environments.
5. Compliance Management: Expertise in managing compliance with various cybersecurity regulations and standards relevant to industry.
6. Security Metrics and Reporting: Skills in developing and tracking meaningful security metrics and creating effective reports for various stakeholders.
7. Emerging Technologies: Understanding of the security implications of emerging technologies like AI, machine learning, and 5G in industrial settings.

Key learning outcomes:

Upon completion of this qualification, professionals will be able to:

1. Develop and implement comprehensive cybersecurity strategies that align with an organization's overall business strategy and risk appetite.
2. Integrate cybersecurity considerations into broader operational resilience and business continuity planning efforts.
3. Manage supply chain security risks effectively, implementing robust vendor assessment and monitoring processes.
4. Oversee the secure implementation of emerging technologies in industrial environments, balancing innovation with security requirements.
5. Develop and manage compliance programs that address the requirements of various cybersecurity regulations and standards.
6. Create and maintain a set of meaningful security metrics, using these to drive continuous improvement in the organization's security posture.

7. Lead cross-functional teams in addressing complex cybersecurity challenges, fostering collaboration between IT, OT, and business units.

This qualification is crucial for organizations seeking to elevate their cybersecurity management to a strategic level. It ensures that senior leaders have the comprehensive understanding needed to make informed decisions about cybersecurity investments, risk management, and technology adoption. For individuals, it provides the skills and knowledge necessary to take on high-level leadership roles in industrial cybersecurity, positioning them as key strategic assets within their organizations.

7.4.2 Implementation of NIS 2 and CER Directives by these 3 qualifications

The three key qualifications outlined in this chapter play a crucial role in meeting the requirements of the NIS 2 (Network and Information Systems) Directive and the Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 (CER Directive). Both directives emphasize the need for robust cybersecurity measures across various sectors, including industry. By aligning the competencies with these regulations, organizations can proactively strengthen their cybersecurity posture and compliance strategies.

NIS 2 Directive Implementation

1. **Risk Management**: NIS 2 underscores the importance of a risk-based approach to cybersecurity. The qualifications focus on advanced risk management skills, equipping professionals to identify vulnerabilities in both IT and OT environments and develop comprehensive mitigation strategies.
2. **Incident Reporting**: A core requirement of NIS 2 is prompt incident notification. The qualifications provide in-depth training on incident response and reporting procedures, enabling professionals to quickly address cyber incidents and fulfill regulatory obligations.
3. **Supply Chain Security**: Recognizing the interconnected nature of industrial environments, NIS 2 emphasizes securing the supply chain. These qualifications address the assessment and management of supply chain security, ensuring professionals can identify and mitigate risks associated with third-party vendors.
4. **Cybersecurity Measures**: All three qualifications provide the knowledge required to implement technical and organizational measures aligned with NIS 2 standards. This includes network segmentation, access controls, and intrusion detection systems tailored for OT environments.
5. **Governance**: The "Shaping Reliability and Cybersecurity Policy in Industry" qualification specifically addresses governance, ensuring that cybersecurity strategies receive appropriate management oversight, as required by NIS 2.

CER Directive Implementation

1. **Secure-by-Design Principles**: The CER Directive emphasizes built-in security for products and systems. The "Management of Reliability and Cybersecurity in the Scope of Devices and Technology in Industry" qualification teaches secure-by-design principles, guiding professionals in embedding security features from the early stages of product development.
2. **Vulnerability Management**: Continuous vulnerability management is a key requirement of the CER Directive. The qualifications cover aspects such as regular assessments,

patch management, and risk mitigation, ensuring that security is maintained throughout a product's lifecycle.

3. **Incident Handling**: The qualifications provide training on developing incident response strategies specific to industrial settings, aligning with CER's emphasis on manufacturers' responsibilities in addressing vulnerabilities.

4. **Compliance**: Professionals trained in these qualifications are equipped to ensure their organization's compliance with the CER Directive, incorporating legal and regulatory knowledge into security practices.

By aligning these qualifications with the NIS 2 Directive and CER Directive, organizations can ensure they are not only compliant but are also actively enhancing their cybersecurity defenses.

7.5 Developing Professional Competencies and Training Programs

The effective implementation of the key qualifications outlined above requires a thoughtful approach to training and competency development. This section explores strategies for integrating these qualifications into comprehensive training programs, balancing theoretical knowledge with practical application, fostering continuous learning, and addressing the challenges and opportunities in implementation.

7.5.1 Integration into Training Programs

To successfully integrate industrial cybersecurity qualifications into existing training programs, organizations should consider the following approaches:

1. Skills Gap Analysis: Conduct a thorough assessment of current competencies within the organization to identify areas where skills fall short of the requirements outlined in the qualifications.
2. Tailored Training Pathways: Develop customized training pathways that align with the structure of the qualifications while considering the specific needs and roles within the organization.
3. Modular Curriculum Design: Create a modular curriculum that allows learners to focus on areas most relevant to their roles while still providing a comprehensive understanding of industrial cybersecurity.
4. Cross-functional Training Initiatives: Develop training programs that bring together IT, OT, and business teams to foster a holistic understanding of cybersecurity challenges and solutions in industrial settings.
5. Partnerships with Educational Institutions: Collaborate with universities, technical colleges, and industry bodies to develop accredited courses that align with the qualifications and meet industry needs.
6. Mentorship Programs: Establish mentorship programs that pair experienced professionals with those developing their skills, facilitating knowledge transfer and practical application of learned concepts.

7. Simulation and Scenario-based Learning: Incorporate realistic simulations and scenario-based exercises that reflect the complex, interdependent nature of industrial cybersecurity challenges.

7.5.2 Theoretical and Practical Balance

Achieving the right balance between theoretical knowledge and practical application is crucial for effective industrial cybersecurity training. Consider the following approaches:

1. Blended Learning Approach: Combine traditional classroom or online learning for theoretical concepts with hands-on laboratory exercises using simulated industrial control systems.
2. Case Study Analysis: Incorporate real-world case studies of industrial cybersecurity incidents, allowing learners to analyze and discuss actual scenarios.
3. Hands-on Labs: Develop specialized labs that replicate industrial environments, allowing trainees to practice implementing security measures, detecting threats, and responding to incidents in a safe, controlled setting.
4. Industry Partnerships: Collaborate with industrial organizations to provide trainees with opportunities for on-site learning experiences, internships, or job shadowing.
5. Virtual and Augmented Reality: Utilize VR and AR technologies to create immersive training experiences that simulate complex industrial environments and cybersecurity scenarios.
6. Cyber Ranges: Implement industrial cyber ranges – controlled, virtual environments that simulate a wide range of industrial systems and cyber threats – for realistic training and assessment.
7. Project-Based Learning: Assign practical projects that require trainees to apply their knowledge to solve real-world industrial cybersecurity challenges.

7.5.3 Continuous Learning and Adaptation

Given the rapidly evolving nature of cyber threats and industrial technologies, fostering a culture of continuous learning is essential:

1. Regular Refresher Courses: Implement mandatory periodic refresher courses to keep professionals updated on the latest threats, technologies, and best practices.
2. Micro-Learning Modules: Develop bite-sized learning modules that professionals can easily access for just-in-time learning on specific topics.
3. Professional Development Plans: Create individualized professional development plans that outline ongoing learning objectives and pathways for career advancement.
4. Industry Conferences and Workshops: Encourage and support attendance at relevant industry conferences, workshops, and webinars to stay abreast of emerging trends.
5. Internal Knowledge Sharing: Establish platforms and processes for internal knowledge sharing, such as regular tech talks or a company wiki for sharing insights and best practices.
6. Certification Programs: Partner with industry certification bodies to offer relevant certifications, and provide support for employees to obtain and maintain these certifications.

7. Threat Intelligence Integration: Incorporate current threat intelligence into training materials to ensure learning is always relevant to the current threat landscape.

7.5.4 Challenges and Opportunities in Implementation

Implementing comprehensive training programs for industrial cybersecurity presents both challenges and opportunities:

Challenges:

1. Rapid Technological Change: Keeping training content up-to-date with fast-paced technological advancements.
2. Resource Constraints: Securing adequate funding and resources for ongoing training and development.
3. Diverse Workforce: Designing programs that cater to a workforce with varying levels of technical expertise and backgrounds.
4. Operational Demands: Balancing training needs with the continuous operational requirements of industrial environments.
5. Measuring Effectiveness: Developing meaningful metrics to assess the impact of training on actual cybersecurity outcomes.

Opportunities:

1. Enhanced Organizational Resilience: Well-trained staff significantly improve an organization's ability to prevent, detect, and respond to cyber threats.
2. Competitive Advantage: Organizations with strong cybersecurity competencies are better positioned to adopt new technologies securely, potentially gaining a competitive edge.
3. Regulatory Compliance: Structured training programs can help ensure compliance with evolving cybersecurity regulations.
4. Talent Attraction and Retention: Offering high-quality training and development opportunities can help attract and retain top cybersecurity talent.
5. Innovation Driver: A skilled workforce can drive innovation in industrial cybersecurity practices and technologies.

7.6 The Need for Professional Competencies in Industrial Cybersecurity

7.6.1 Bridging the Skills Gap

The industrial sector faces a significant shortage of cybersecurity professionals with the specialized knowledge required to protect complex industrial environments. To address this gap:

1. Develop specialized training programs that combine IT security knowledge with OT-specific skills.
2. Collaborate with educational institutions to develop curricula that address the unique needs of industrial cybersecurity.
3. Implement mentorship programs to facilitate knowledge transfer from experienced professionals to newcomers.

4. Encourage cross-training between IT and OT teams to foster a more holistic understanding of industrial cybersecurity challenges.

7.6.2 Adapting to Evolving Threats

The threat landscape in industrial cybersecurity is constantly evolving, requiring professionals to:

1. Engage in continuous threat intelligence gathering and analysis specific to industrial environments.
2. Develop skills in implementing and managing advanced threat detection and response systems tailored to OT environments.
3. Conduct regular penetration testing and vulnerability assessments on industrial control systems.
4. Develop and update incident response plans that address the unique challenges of cyber-physical systems.

7.6.3 Enhancing Organizational Resilience

Cybersecurity competencies play a crucial role in enhancing the overall resilience of industrial organizations:

1. Integrate cybersecurity considerations into business continuity and disaster recovery plans.
2. Develop skills in designing resilient industrial control systems that can withstand or quickly recover from cyber attacks.
3. Implement secure-by-design principles in the development and deployment of industrial systems.

7.6.4 Supporting Digital Transformation

As industries undergo digital transformation, cybersecurity competencies become crucial enablers of innovation and growth:

1. Develop expertise in securing Industrial Internet of Things (IIoT) deployments.
2. Acquire skills in implementing cloud security strategies tailored to industrial data and applications.
3. Understand data protection and privacy implications in the context of big data analytics and AI in industrial settings.

7.6.5 Driving Economic Growth and Innovation

Strong industrial cybersecurity competencies can be a significant driver of economic growth and innovation:

1. Create new job opportunities in the field of industrial cybersecurity.
2. Foster the development of cybersecurity products and services tailored to industrial needs.
3. Enhance the competitiveness of national industries in the global market.
4. Attract investment in secure industrial technologies and infrastructure.

7.7 Future Directions and Emerging Trends

7.7.1 Artificial Intelligence and Machine Learning

1. Develop skills in implementing AI-driven threat detection systems for industrial environments.
2. Understand the ethical implications and potential vulnerabilities of AI in industrial cybersecurity.

7.7.2 Internet of Things (IoT) and Industrial Internet of Things (IIoT)

1. Acquire expertise in securing diverse IoT devices and their communication protocols.
2. Develop skills in implementing edge computing security measures.

7.7.3 Cloud Security for Industrial Systems

1. Design secure cloud architectures tailored for industrial applications.
2. Develop competencies in managing security across multiple cloud platforms used in industrial settings.

7.7.4 5G and Advanced Networking

1. Implement security measures specific to 5G networks in industrial environments.
2. Develop skills in securing network slicing for different industrial applications.

7.7.5 Quantum Computing and Cryptography

1. Understand and implement quantum-resistant cryptographic methods.
2. Develop strategies for transitioning to post-quantum security measures in industrial systems.

7.7.6 Advanced Persistent Threats (APTs) and Nation-State Actors

1. Enhance skills in detecting and mitigating sophisticated, long-term cyber campaigns targeting industrial infrastructure.
2. Develop competencies in cyber threat intelligence specific to industrial sectors.

7.7.7 Human-Machine Interaction Security

1. Implement security measures for human-machine interfaces in industrial settings.
2. Develop skills in using behavioral analytics to detect insider threats and unusual operator actions.

7.8 Integration of Cybersecurity Competencies into Broader Industrial Skills

1. Incorporate cybersecurity principles into process engineering and automation roles.

2. Develop cybersecurity awareness and basic skills across all levels of industrial organizations.

7.9 Global Standardization of Industrial Cybersecurity Competencies

1. Contribute to the development of internationally recognized certification programs for industrial cybersecurity.
2. Participate in global initiatives to standardize industrial cybersecurity practices and competencies.

7.10 Ethical Considerations in Industrial Cybersecurity

1. Develop frameworks for ethical decision-making in industrial cybersecurity contexts.
2. Understand privacy implications of cybersecurity measures in industrial environments.

7.11 Interdisciplinary Approach to Cybersecurity Education

1. Promote collaboration between IT, OT, and engineering disciplines in cybersecurity education.
2. Develop curricula that integrate cybersecurity with industrial process knowledge and operational priorities.

7.11 Conclusions and Future Outlook

The development of professional competencies in industrial cybersecurity is a strategic imperative for the future of industrial sectors. As industries continue to evolve in the digital age, investing in these competencies will be key to ensuring not only the security but also the prosperity of industrial organizations in an increasingly interconnected world. The future of industrial cybersecurity lies in a workforce that can adapt to emerging threats, leverage new technologies securely, and balance security requirements with operational needs. Continuous learning, interdisciplinary collaboration, and a commitment to ethical practices will be crucial in shaping the next generation of industrial cybersecurity professionals.

8 INNOVATIVE INSURANCE MODELS BASED ON CYBERSECURITY AND RELIABILITY

8.1 OT, ET, and ICS Systems—Insurance Implications

Operational Technology systems (including operation technology OT, engineering technology ET, and industrial control systems ICS) play a pivotal role in the functioning of industrial environments, particularly in sectors such as oil and gas, utilities, and manufacturing. These systems are responsible for controlling physical processes, making them essential to the safety and reliability of industrial facilities. However, OT, ET, and ICS, ET, and ICS systems also present a unique set of cybersecurity challenges. As more industrial environments become interconnected and digitized, OT, ET, and ICS, ET, and ICS systems are increasingly vulnerable to cyberattacks that could disrupt operations, damage physical equipment, or even endanger lives.

The Stuxnet attack on Iran's nuclear facility, which inflicted an estimated **$2 to $5 billion** in damage, serves as a stark reminder of the potential vulnerabilities faced by every asset owner operating critical infrastructure. With development costs of the malware itself estimated between **$500 million and $1 billion**, Stuxnet demonstrated how a targeted cyberattack could cause damage many times greater than the initial investment, highlighting the asymmetry between the cost of launching an attack and the cost of recovery. For asset owners, the lesson is clear: failing to invest in robust cybersecurity measures can result in catastrophic losses. In contrast, the relative cost of improving security—such as through real-time monitoring, regular vulnerability assessments, and adopting advanced AI-driven defense systems—pales in comparison to the potential damages of a successful cyberattack. Strengthening cybersecurity isn't just a technological safeguard; it is a financial imperative.

For insurance providers, understanding how companies manage these risks is critical to offering appropriate coverage. Traditional risk assessments and security audits for IT systems are not enough for OT, ET, and ICS environments, as OT, ET, and ICS, ET, and ICS systems operate under different constraints and require specialized approaches. Insurers need to evaluate how well companies mitigate OT, ET, and ICS-related cyber risks, as this directly impacts the underwriting process and the structure of insurance policies. A failure to address OT, ET, and ICS risks adequately can lead to significant operational disruptions and costly insurance claims, while companies with strong OT, ET, and ICS risk management practices can benefit from more favorable premiums and coverage.

8.1.1 Adapting Risk Assessments for OT, ET, and ICS Environments

The unique nature of OT, ET, and ICS, ET, and ICS systems requires a specialized approach to risk assessment. Unlike traditional IT systems, OT, ET, and ICS, ET, and ICS systems are often designed to run continuously, and their real-time requirements mean that any downtime can result in severe consequences. In addition, OT, ET, and ICS, ET, and ICS systems are deeply integrated with physical processes, meaning a cyberattack on an OT, ET, and ICS system could cause physical harm, disrupt production, or even lead to safety hazards. These characteristics make OT, ET, and ICS, ET, and ICS systems especially critical from an insurance perspective.

8.1.1.1 Understanding OT, ET, and ICS Specifics

To fully assess the risks, insurers must understand the distinct characteristics of OT, ET, and ICS, ET, and ICS systems. For instance, the real-time operational needs of OT, ET, and ICS, ET, and ICS systems mean that they cannot afford prolonged downtime, as even short disruptions can lead to significant operational losses or safety incidents. The potential for physical harm also distinguishes OT, ET, and ICS, ET, and ICS systems from IT, as cyberattacks on OT, ET, and ICS, ET, and ICS systems can result in equipment malfunctions or safety system failures. Insurers should ensure that companies recognize these differences and have appropriate measures in place to protect their OT, ET, and ICS, ET, and ICS systems from cyber threats.

8.1.1.2 Asset Inventory

Maintaining a complete and up-to-date inventory of all OT, ET, and ICS assets is essential for both risk management and insurance underwriting. This inventory should include detailed information about each asset, such as its configuration, software version, and security features. By requiring companies to maintain accurate OT, ET, and ICS asset inventories, insurers can gain a clearer understanding of the scope of risk exposure. An updated inventory allows insurers to assess which assets are vulnerable and what the potential impacts might be in the event of a cyber incident.

8.1.1.3 Vulnerability Assessments

Regular vulnerability assessments are a key component of OT, ET, and ICS risk management. OT, ET, and ICS, ET, and ICS systems often run on legacy or unpatched software, which increases the likelihood of cyberattacks. Insurers should require companies to conduct frequent vulnerability assessments to identify and address weak points in their OT, ET, and ICS, ET, and ICS systems. Companies that consistently identify and patch vulnerabilities demonstrate a proactive approach to cybersecurity, which may translate into lower insurance premiums. Conversely, companies that fail to address vulnerabilities may face higher premiums, as they represent a greater risk of experiencing a costly cyber incident.

8.1.2 Security Audit Best Practices

Security audits are a critical tool for evaluating the effectiveness of a company's cybersecurity controls, particularly in OT, ET, and ICS environments where risks are high and the potential consequences of a cyberattack are severe. Insurers should prioritize companies that conduct regular, comprehensive security audits, as these audits help ensure that cybersecurity measures are functioning as intended and that any gaps are identified and addressed.

8.1.2.1 Regular Audits

Insurance providers should require companies to conduct periodic security audits of their OT, ET, and ICS, ET, and ICS systems. These audits provide valuable insights into the effectiveness of a company's cybersecurity controls, including access management, network configurations, and incident response capabilities. Regular audits ensure that companies stay ahead of emerging threats and remain in compliance with industry standards. Companies that conduct audits regularly—and act on the findings—are generally at lower risk of cyber incidents, making them more attractive to insurers and potentially eligible for lower premiums.

8.1.2.2 Compliance Checks

Adherence to industry standards, such as IEC 62443 (security for industrial automation and control systems) and NIST SP 800-82 (guidelines for securing OT, ET, and ICS, ET, and ICS systems), is another crucial factor in the underwriting process. Compliance with these standards demonstrates that a company is following best practices in OT, ET, and ICS security, which can significantly reduce its risk profile. Insurers should assess a company's level of compliance as part of their underwriting process and reward companies that consistently meet or exceed these standards with more favorable insurance terms. In addition to reducing cyber risk, compliance helps ensure that a company is well-prepared to address regulatory requirements in the event of an incident.

8.1.2.3 Third-Party Assessments

Independent, third-party assessments provide an unbiased evaluation of a company's OT, ET, and ICS security posture. Engaging external experts for these evaluations helps ensure that no internal biases or oversights affect the results. Third-party assessments are especially valuable for insurers, as they provide an objective view of the company's cybersecurity efforts. Insurance providers may offer better coverage options or lower premiums to companies that engage in regular third-party assessments, as these demonstrate a commitment to maintaining high cybersecurity standards.

8.1.3 Case Study: Cyber-Attack on an Industrial Facility

- Background: A petrochemical plant experienced a targeted cyberattack that compromised its OT, ET, and ICS, ET, and ICS systems. The attackers manipulated critical safety mechanisms, resulting in a complete shutdown of operations. The incident caused significant financial losses and raised serious safety concerns.
- Impact: The shutdown resulted in millions of dollars in lost revenue due to halted production. Insurance coverage for business interruption helped offset some of these losses, but the company's premiums increased significantly after the incident. In addition to the financial losses, the attack compromised the plant's safety systems, creating the potential for dangerous chemical leaks and equipment failure. The severity of this risk factored into the insurer's reassessment of the company's liability coverage, leading to higher premiums for liability insurance.

Lessons Learned: The incident highlighted the need for integrating cybersecurity with safety protocols. Insurers should ensure that companies have seamless integration between their OT, ET, and ICS security and safety management systems. Continuous monitoring and a well-defined incident response plan could have mitigated the impact of the attack. The lack of these capabilities left the company vulnerable, emphasizing the importance of real-time monitoring and rapid response for OT, ET, and ICS, ET, and ICS systems. Regular security audits could have identified the vulnerabilities that the attackers exploited. The company had not conducted a comprehensive audit of its OT, ET, and ICS, ET, and ICS systems in over a year, which contributed to the severity of the attack.

8.1.4 Insurance Implications for OT, ET, and ICS Risk Management

Insurers must adopt a specialized approach to underwriting and policy development for OT, ET, and ICS, ET, and ICS systems due to their unique risk profile. Offering standard IT-based cyber insurance policies is insufficient in environments where real-time operational needs, physical processes, and safety concerns are paramount. As industrial companies increase their reliance on OT, ET, and ICS, ET, and ICS systems, insurers should adapt their coverage models to reflect these new realities.

8.1.4.1 Customized Coverage for OT, ET, and ICS Systems

Given the unique risks associated with OT, ET, and ICS, ET, and ICS systems, insurers should offer customized policies specifically designed to address OT, ET, and ICS-related cyber risks. These policies should account for the potential for physical damage, safety incidents, and operational disruptions. By offering tailored coverage options, insurers can ensure that clients are adequately protected while also managing their own risk exposure.

8.1.4.2 Audit-Based Premium Adjustments

Insurers should consider adjusting premiums based on the results of regular security audits and vulnerability assessments. Companies that demonstrate strong cybersecurity practices through regular audits and rapid vulnerability patching should be rewarded with lower premiums, while those that neglect these activities may face higher costs. This dynamic pricing approach encourages continuous improvement in cybersecurity practices, benefiting both the insured and the insurer.

8.1.4.3 Incentives for Continuous Improvement

To further incentivize companies to adopt better cybersecurity practices, insurers can offer rewards for continuous monitoring, compliance with industry standards, and engagement with third-party security experts. These rewards may include premium reductions, expanded coverage options, or additional services such as incident response support.

By aligning insurance offerings with robust OT, ET, and ICS risk management practices, insurers can help industrial clients reduce the likelihood of cyber incidents while providing more competitive and comprehensive coverage. This mutually beneficial approach supports stronger cybersecurity in industrial environments, helping to minimize operational disruptions and protect against costly cyberattacks.

8.2 New Insurance Models

In an era where cyber threats are evolving rapidly, the traditional models of insurance for industrial clients are no longer sufficient to address the complex risks posed by cybersecurity challenges. Industrial sectors, particularly those that rely heavily on operational technology (OT, ET, and ICS) and industrial control systems (ICS), require insurance models that reflect the dynamic nature of modern cyber risks. As companies in the energy, oil and gas, and chemical industries become more digitalized, insurance providers are developing innovative ways to assess and price these risks.

8.2.1 Transition to Dynamic Pricing Models

One of the most promising shifts in the insurance industry is the move toward dynamic pricing models. Historically, insurance premiums were based on static assessments, which often failed to account for the ongoing and real-time changes in a company's cybersecurity posture. Today, the use of real-time risk assessment has revolutionized this approach. By leveraging advanced data analytics, insurers can continuously monitor a company's risk profile and adjust premiums accordingly. For example, companies that demonstrate strong cybersecurity defenses, such as regularly updated software, secure network configurations, and proactive threat detection measures, may benefit from reduced premiums. On the other hand, companies that are slow to implement cybersecurity best practices or fail to address vulnerabilities might see higher insurance costs.

This model does more than just improve the accuracy of premium pricing; it actively incentivizes security investments. Companies that adopt robust cybersecurity measures—such as multi-layered defense strategies, continuous monitoring, and incident response planning—are rewarded with lower insurance premiums. This financial incentive encourages businesses to prioritize cybersecurity not only as a means of risk reduction but also as a cost-saving strategy. In industries where margins are tight and downtime is costly, the potential savings from lower premiums can significantly impact operational budgets.

8.2.2 Risk Scoring Models Incorporating Cybersecurity Metrics

To facilitate dynamic pricing and create a fair, transparent assessment system, insurers are developing risk scoring models that incorporate key cybersecurity metrics. These models evaluate a company's security posture based on various factors, such as its exposure to external threats, the effectiveness of its mitigation measures, and the potential impact of a cyber incident on its operations.

A critical tool in this assessment process is the use of cybersecurity scorecards. These scorecards provide a comprehensive evaluation of a company's defenses, allowing insurers to quantify the effectiveness of its cybersecurity program. Metrics such as the implementation of firewalls, encryption protocols, employee training, and incident response capabilities are consistently measured. This systematic approach ensures that all companies are evaluated on a level playing field, using standardized metrics that align with industry best practices.

The standardized approach also benefits industrial companies by providing a clear framework for improvement. With cybersecurity scorecards, companies can see where they stand compared to industry benchmarks, identify areas of vulnerability, and prioritize upgrades or improvements to their security infrastructure. By doing so, they not only reduce their risk exposure but also position themselves to benefit from more favorable insurance terms.

8.2.3 Recommendations for Insurers and Energy Asset Operators

For insurers and energy asset operators alike, there are several key strategies to adopt in order to better align with the evolving cyber threat landscape.

For Insurers

- Develop Specialized Policies for OT, ET, and ICS and ICS Risks: Traditional cyber insurance models often focus on IT systems, leaving operational technology (OT, ET, and ICS) and industrial control systems (ICS) underinsured. Insurers must develop tailored policies that specifically address the unique risks associated with these critical systems. OT, ET, and ICS and ICS risks are inherently different from IT risks because they involve real-time control of physical processes, and a breach can result in physical damage, safety risks, and regulatory fines. Specialized policies should reflect the severity and complexity of these threats.
- Incorporate Cybersecurity Assessments into Underwriting Processes: The underwriting process should evolve to include thorough cybersecurity assessments. Rather than relying solely on historical data or industry averages, insurers need to incorporate real-time cybersecurity assessments into their underwriting criteria. This could involve evaluating a company's adherence to cybersecurity standards such as ISO/IEC 27001 or IEC 62443, conducting audits of security practices, or analyzing the company's incident response history.

For Energy/Industrial Asset Operators

- Invest in Multi-Layered Defense Strategies: Energy asset operators must invest in comprehensive, multi-layered cybersecurity strategies. A single line of defense is not enough in today's threat environment. Operators should implement a combination of firewalls, intrusion detection systems, encryption, and access controls, all of which work together to create a robust security perimeter. In addition, the use of advanced technologies such as artificial intelligence (AI) for threat detection and machine learning for anomaly identification can significantly enhance defensive capabilities.
- Engage in Regular Security Audits and Improvements: Cybersecurity is not a one-time investment; it requires continuous attention. Energy asset operators should engage in regular security audits to identify weaknesses and ensure compliance with industry standards. These audits can be conducted internally or through third-party assessments, but the goal should be the same: to continuously monitor and improve cybersecurity measures as threats evolve. Additionally, companies should implement a continuous improvement process, where findings from audits are used to update and upgrade cybersecurity systems proactively, rather than reactively.

By embracing these innovative insurance models and risk scoring systems, both insurers and energy asset operators can mitigate cyber risks more effectively. Insurers will benefit from a more accurate understanding of risk, enabling them to offer customized policies that reflect a company's true exposure. Meanwhile, companies in industrial sectors will gain a financial incentive to prioritize cybersecurity investments, leading to safer, more resilient operations in the face of growing cyber threats. This synergy between insurance and cybersecurity will help build a more secure and reliable industrial landscape, where both financial and operational risks are reduced through proactive measures.

8.2.4 Integrated Dashboards

Both asset owners and underwriters benefit significantly from having access to integrated dashboards that provide real-time visibility into the status of OT, ET, and ICS, ET, and ICS units. These dashboards, which detail system age, update status, versioning, history, and security posture, allow asset owners to manage their infrastructure proactively, ensuring timely updates and identifying vulnerabilities before they become critical. This level of insight not only strengthens operational security but also positions asset owners to minimize downtime and disruptions by maintaining a consistently high level of preparedness.

A key component of these dashboards is AI-powered traffic analysis, which monitors the flow of data between systems to detect suspicious activity or anomalies in real time. By continuously scanning for unusual patterns, AI tools can flag potential cyber threats, enabling asset owners to respond before significant damage occurs. From an insurance perspective, this capability provides underwriters with crucial, up-to-the-minute data on a client's risk profile. This real-time assessment can lead to more precise risk evaluations and dynamic adjustments to coverage, reflecting the current state of system security rather than relying on static, outdated assessments.

This continuous flow of data strengthens the relationship between asset owners and underwriters, allowing both parties to make informed decisions. Underwriters, with access to real-time security metrics, can more accurately assess risk and offer tailored premiums based on the actual cybersecurity practices in place. At the same time, asset owners are incentivized to maintain robust cybersecurity defenses, knowing that their efforts will be reflected in their insurance terms. This data-driven approach encourages a culture of continuous improvement and reduces the overall risk of costly incidents, benefiting both insurers and insured parties in the long term.

Dashboards that provide real-time visibility into the status of OT, ET, and ICS, ET, and ICS systems have a direct impact on premium rates by enabling insurers to base their assessments on dynamic, up-to-date information rather than static or periodic reviews. With access to real-time data on system updates, patch status, and potential vulnerabilities, underwriters can evaluate a company's cybersecurity posture more accurately. Companies that maintain well-updated, secure systems, and show proactive risk management are often seen as lower-risk clients, which can lead to reduced premiums. This level of transparency allows insurers to adjust premiums in a way that truly reflects the ongoing risk profile of the client.

Additionally, dashboards equipped with AI-powered traffic monitoring can further lower premium rates by detecting and mitigating suspicious activity early. The ability to spot threats before they lead to major incidents reduces the likelihood of expensive claims, thus making the client a more attractive candidate for favorable insurance terms. Insurers can reward companies that invest in advanced monitoring and quick-response systems, as these measures significantly reduce the potential for large-scale losses due to cyberattacks or operational failures. As a result, companies that utilize these dashboards are more likely to secure better premium rates because their risk exposure is continuously monitored and managed.

For underwriters, these dashboards also offer the ability to dynamically adjust premium rates based on real-time changes in a company's security posture. As systems age or vulnerabilities are discovered and patched, insurers can adjust premiums to reflect the current risk accurately. This flexibility benefits both insurers, who can align premiums more closely with actual risk, and asset owners, who can actively manage their premiums by maintaining strong cybersecurity practices. This data-driven, transparent approach to risk assessment creates a more fair and responsive insurance pricing model.

The following metrics could help insurers assess the robustness of a company's cybersecurity posture and the effectiveness of its risk management practices. Key metrics might include:

- **System Age and Update Status:** Regularly updated systems with the latest security patches have a lower risk of being compromised. Keeping OT, ET, and ICS and ICS software up to date reduces the likelihood of vulnerabilities being exploited. A proactive approach to patch management and upgrading aging systems signals strong cybersecurity hygiene, improving the overall risk score.
- **Vulnerability Management:** The frequency and effectiveness of vulnerability assessments play a significant role in determining risk scores. Companies that regularly scan for and promptly address vulnerabilities demonstrate an active commitment to mitigating risks. Automated vulnerability detection systems and timely patching of identified risks contribute to better scores, as they minimize the window of exposure to potential threats.
- **Network Traffic Monitoring and Anomaly Detection:** Continuous monitoring of network traffic through AI-powered tools helps detect and respond to suspicious activities before they escalate into major incidents. Metrics like the number of anomalies detected, response times, and the effectiveness of threat mitigation actions are crucial in showing an organization's capacity to manage cyber threats. A company with a strong anomaly detection and response system will have a more favorable risk profile.
- **Incident Response and Recovery Capabilities:** A well-documented and tested incident response plan, coupled with metrics on response times, recovery procedures, and the frequency of incident simulations (such as cyber drills), improves a company's risk score. Insurers look for companies that can demonstrate their ability to contain and recover from incidents swiftly, thereby reducing the potential impact of cyberattacks.
- **Compliance with Industry Standards:** Adherence to recognized cybersecurity frameworks such as IEC 62443 for industrial control systems or NIST standards improves risk scores. Compliance with these standards indicates that the company follows best practices for securing OT, ET, and ICS environments, making it a lower-risk client from an insurance perspective.
- **Asset Inventory and Control:** A complete, regularly updated inventory of all OT, ET, and ICS, ET, and ICS assets, along with strict access controls, shows that a company maintains full visibility and governance over its systems. Metrics tracking the management of assets, access control policies, and device authentication help insurers gauge how well a company manages its infrastructure, leading to better risk scores.
- **Security Awareness and Training:** The level of employee training and awareness around cybersecurity threats, particularly in environments where human error can lead to breaches, significantly influences risk scores. Companies that conduct regular training sessions, phishing simulations, and cybersecurity education programs have a workforce better equipped to avoid or mitigate risks, leading to a more favorable assessment from insurers.

8.3 Understanding Cyber Risk in Industry: Vectors and End Goals

In industrial environments such as oil and gas, chemical, and utilities sectors, cybersecurity risks are multi-faceted, with both digital and physical components. For insurance purposes, it is important to distinguish between attack vectors—the methods by which attackers gain access to systems—the end goals they aim to achieve, and the victims—first or third party. This distinction helps to better assess risks, develop mitigation strategies, and structure insurance policies that adequately cover potential losses.

This chapter provides a comprehensive breakdown of cyber risks faced by industrial organizations, categorized into attack vectors and end goals.

8.3.1 End Goals: What Cyberattacks Aim to Achieve

While the vectors describe how attackers gain access to a system, the end goals reveal their ultimate objectives. These can range from financial extortion to sabotage and theft, each posing unique risks to industrial organizations.

8.3.1.1 Ransom

- Description: Attackers use ransomware to encrypt files or systems, demanding payment (usually in cryptocurrency) in exchange for restoring access. In industrial environments, ransomware can halt production by targeting OT, ET, and ICS, ET, and ICS systems.
- Example: The Colonial Pipeline attack, where ransomware forced the shutdown of one of the largest fuel pipelines in the U.S., leading to fuel shortages and financial losses.

8.3.1.2 Vandalism/Sabotage (e.g., Stuxnet)

- Description: Cyber vandalism or sabotage involves deliberately disrupting, damaging, or destroying industrial systems. The goal is to cause operational failures or physical damage, often targeting critical infrastructure or safety systems.
- Example: The Stuxnet malware was designed to sabotage Iran’s nuclear program by manipulating centrifuge speeds, causing physical damage to the equipment.

8.3.1.3 Data Theft (Intellectual Property or Personal Data)

- Description: Data theft involves stealing sensitive information, including intellectual property (IP), trade secrets, or personal identifiable information (PII). For industrial companies, the theft of IP can lead to significant competitive disadvantages.
- Example: A hacking group targeting a manufacturing company’s R&D department, stealing proprietary blueprints for a new technology, resulting in loss of market advantage.

8.3.1.4 Surveillance and Espionage

- Description: Surveillance and espionage attacks focus on gaining unauthorized access to monitor network traffic or industrial processes. These attacks are often carried out by nation-state actors seeking strategic information about critical infrastructure.

- Example: State-sponsored cyber actors gaining access to an energy company’s control systems, silently monitoring power distribution to understand vulnerabilities or prepare for potential sabotage.

8.3.1.5 Cryptojacking

- Description: Cryptojacking involves hijacking a company’s computing resources to mine cryptocurrency. While it does not typically disrupt operations directly, it can consume resources and slow down essential systems, impacting performance.
- Example: An industrial company unknowingly having cryptojacking malware installed on its IT systems, leading to reduced operational efficiency and higher energy consumption.

8.3.1.6 Business Disruption

- Description: Some attacks are designed purely to cause operational disruptions, whether through ransomware, DoS attacks, or sabotage. The goal is to interrupt business processes, leading to financial losses and reputational damage.
- Example: A DDoS attack against a manufacturing plant’s control systems, halting production for several days and causing substantial revenue loss due to missed deadlines and contractual penalties.

8.3.2 Attack Vectors: How Cyberattacks Occur

These are the methods or pathways that attackers use to infiltrate industrial systems. Understanding these vectors is crucial for identifying potential entry points and implementing appropriate defenses.

8.3.2.1 Advanced Persistent Threats (APTs)

- Description: APTs involve highly sophisticated, long-term cyberattacks carried out by state-sponsored actors or well-resourced criminal organizations. Attackers maintain undetected access to a system over an extended period, using techniques like spear-phishing, zero-day vulnerabilities, or compromised credentials.
- Example: APT33, linked to state-sponsored cyber espionage in the energy sector, conducted prolonged campaigns against companies in the U.S. and Saudi Arabia.

8.3.2.2 Supply Chain Attacks (Third-Party Risk)

- Description: Attackers exploit weaknesses in third-party vendors or suppliers to breach a target’s network. In industrial environments, this often occurs via software or hardware components provided by vendors, creating a broader attack surface.
- Example: The SolarWinds hack, in which attackers compromised software updates from a widely used IT management vendor, leading to breaches in multiple critical infrastructure organizations.

8.3.2.3 Phishing and Social Engineering

- Description: Phishing involves deceptive emails or messages designed to trick employees into divulging sensitive information or downloading malicious software. Social engineering exploits human error or trust to gain access to systems.
- Example: An industrial employee being deceived by a phishing email and inadvertently installing ransomware on an operational control system.

8.3.2.4 Insider Threats

- Description: Insider threats occur when employees, contractors, or business partners with legitimate access to systems intentionally or unintentionally compromise cybersecurity. Insiders have privileged access, making their actions potentially more damaging.
- Example: A former employee at a utility company disabling critical safety systems before leaving, causing significant operational disruptions.

8.3.2.5 Denial of Service (DoS/DDoS)

- Description: DoS or DDoS attacks involve overwhelming a network, server, or system with traffic, rendering it unavailable. In industrial environments, this can disrupt control systems, leading to loss of monitoring and control capabilities over critical infrastructure.
- Example: A DDoS attack on a smart grid management system could prevent utility operators from controlling power distribution.

8.3.2.6 Physical-Digital Convergence Attacks

- Description: With the integration of physical and digital systems in industrial environments, attackers can exploit weaknesses in industrial control systems (ICS) or IoT devices to cause disruptions in the physical world.
- Example: A cyberattack on a water treatment plant that manipulates physical processes, leading to hazardous chemical levels being released.

8.3.3 Mapping Vectors to End Goals

It is important to understand the relationship between attack vectors and end goals. While some vectors can lead to multiple end goals, insurance clients need to prepare for the most likely scenarios based on the unique nature of their operations and assets. Below is an example of how vectors can map to end goals (Table 8.1).

8.3.4 Implications for Industrial Insurance

Insurance policies for industrial clients must consider both the attack vectors and end goals to offer comprehensive coverage. A well-rounded policy should:

- Cover Ransomware and Business Disruption: Given the growing frequency and impact of ransomware attacks, insurance should provide coverage for ransom payments, recovery costs, and losses from business disruption.

- Include Data Breach and Theft Protections: Policies must cover the legal liabilities and financial penalties associated with data breaches, particularly for intellectual property theft or loss of personal identifiable information.
- Protect Against Vandalism and Sabotage: In industries where physical safety and operational reliability are critical, policies should cover damages resulting from cyber-physical sabotage, including equipment repair and downtime compensation.
- Mitigate Risks from Supply Chain Attacks: As supply chains become increasingly interconnected, insurance should cover third-party risks, ensuring that companies are protected from vulnerabilities introduced by vendors.

By aligning insurance coverage with both attack vectors and end goals, industrial organizations can build a robust cybersecurity and risk management strategy that addresses the full spectrum of cyber threats they face.

Understanding the distinction between attack vectors and end goals is crucial for effective risk management in industrial environments. Cyber threats can come from multiple pathways—ranging from advanced persistent threats to insider risks—and their impacts can vary widely, from data theft to physical sabotage. By structuring insurance policies to account for both vectors and goals, organizations can ensure they are prepared for the full range of cybersecurity risks, minimizing the potential for operational, financial, and reputational damage. This layered approach provides clarity for both insurers and industrial clients, fostering a better understanding of cyber risk and enabling the development of comprehensive coverage solutions.

Table 8.1 – Example of how vectors can map to end goals

	APTs	**Phishing**	**Supply Chain Attacks**
Data Theft	Through long-term infiltration and exfiltration of sensitive information.	By gaining access to credentials that allow attackers to infiltrate sensitive databases.	
Ransomware		By tricking an employee into downloading malicious software.	
Surveillance and Espionage	Through ongoing monitoring of critical industrial processes.		If attackers use third-party software to gain unauthorized access to a company's networks.
Vandalism/Sabotage			By injecting malicious code into industrial control systems, leading to physical damage.

8.4 Policy, Regulatory and Insurance Interactions

Insurance plays a critical role in shaping the overall policy landscape, particularly in areas like cybersecurity where technological advancements outpace the regulatory process. In situations where legislators may be slow to act or lack the necessary expertise to fully understand the complexities of cybersecurity, insurance can fill the gap by driving industry standards and incentivizing best practices. Through underwriting and risk assessment, insurers are often in a position to influence corporate behavior by setting requirements for coverage that promote stronger cybersecurity measures. This indirect form of governance ensures that companies are held accountable for managing cyber risks, even in the absence of formal regulations.

In rapidly evolving fields like operation and engineering technologies, ICS and ICS cybersecurity, where vulnerabilities can have both digital and physical consequences, the insurance industry's ability to assess and price risk encourages organizations to prioritize security investments. By offering reduced premiums or enhanced coverage for companies that adhere to recognized cybersecurity frameworks or implement advanced threat detection systems, insurers create financial incentives that push businesses toward better risk management. This, in effect, becomes a form of policy-making, where insurers set the expectations for cybersecurity readiness and resilience, influencing how organizations allocate resources toward securing their critical infrastructure.

Moreover, in the absence of immediate legislative action, insurance serves as a stabilizing force by standardizing risk management practices across industries. Since insurers have a vested interest in minimizing claims, they often require clients to comply with industry best practices, such as regular security audits, vulnerability assessments, and adherence to cybersecurity standards like NIST or IEC 62443. This ensures that even without comprehensive legal mandates, companies are still motivated to maintain a strong cybersecurity posture. In this way, the insurance sector becomes a de facto regulator, driving consistent and responsible cybersecurity policies that protect not only individual organizations but also the broader ecosystem in which they operate.

8.5 Glossary

- Cybersecurity Risk: Potential for loss or harm related to technical infrastructure or use of technology within an organization.
- Operational Technology (OT, ET, and ICS): Hardware and software that detects or causes changes through direct monitoring or control of physical devices, processes, and events.
- Information Technology (IT): Use of computers to store, retrieve, transmit, and manipulate data or information.
- Environmental Technology (ET): Application of environmental science to conserve the natural environment and resources.
- Internet of Things (IoT): Network of physical objects embedded with sensors, software, and other technologies to connect and exchange data.
- Artificial Intelligence (AI): Simulation of human intelligence in machines programmed to think and learn.

- Safety Integrity Level (SIL): A relative level of risk-reduction provided by a safety function.
- Failure Mode and Effects Analysis (FMEA): Step-by-step approach for identifying all possible failures in a design, manufacturing, or assembly process.
- Supervisory Control and Data Acquisition (SCADA): Control system architecture comprising computers, networked data communications, and graphical user interfaces.

9 CYBER AND AI RISKS FOR CBRN RELATED FACILITIES: NAVIGATING SECURITY IN AN ERA OF DEMOCRATIZED KNOWLEDGE

9.1 Introduction: the Democratization of Knowledge and Capability

The landscape of Chemical, Biological, Radiological, and Nuclear (CBRN) facility security has undergone a fundamental transformation with the advent of artificial intelligence (AI) and advanced cyber technologies. This transformation extends far beyond mere technological advancement – we are witnessing an unprecedented democratization of knowledge that challenges traditional security paradigms and control mechanisms. The implications of this shift are profound, affecting everything from daily operations to international security protocols.

In the past, expertise in CBRN operations was confined to a select group of specialists with extensive training and restricted access to sensitive information. These experts underwent years of specialized education, accumulated practical experience in controlled environments, and operated within strict regulatory frameworks. Their knowledge was protected by both institutional barriers and the inherent complexity of CBRN operations. Today, this paradigm has been fundamentally disrupted by the emergence of sophisticated AI systems that can provide detailed technical knowledge about complex chemical processes, biological systems, and facility operations to anyone with internet access.

The democratization of CBRN knowledge through AI presents particularly acute challenges for chemical facilities, where AI can now assist in process optimization, chemical synthesis planning, and even the identification of novel compounds. What once required years of specialized education and laboratory experience can now potentially be accomplished through AI-guided processes. These systems can suggest detailed synthetic routes for complex chemicals, optimize reaction conditions, and predict the properties of new compounds - capabilities that were previously limited to highly trained specialists working in controlled environments.

The implications of this knowledge democratization extend across the full spectrum of CBRN facilities. A pharmaceutical manufacturing plant, for instance, must now consider how AI might be used to repurpose its legitimate processes for illicit purposes. A biological research laboratory needs to evaluate how AI could be employed to modify standard protocols in ways that bypass traditional safety controls. Nuclear facilities must assess how AI-enabled systems might be manipulated to affect critical safety parameters. This new reality demands a fundamental rethinking of security approaches across all CBRN sectors.

The challenges are compounded by the rapid pace of AI advancement and its increasing accessibility. Open-source AI tools, cloud computing resources, and vast amounts of publicly available technical data have created an environment where sophisticated analysis and process optimization capabilities are available to a wide range of actors. This democratization of capabilities raises serious concerns about the potential for misuse, whether through deliberate malicious action or inadvertent dangerous applications.

Moreover, the integration of AI into CBRN facilities has created new vulnerabilities in facility operations. Modern CBRN facilities rely heavily on automated systems for process control, safety monitoring, and security management. While these systems enhance efficiency and safety under normal conditions, they also create new attack vectors that could be exploited by adversaries with AI capabilities. The potential for AI-enabled attacks to manipulate these systems while evading detection represents a significant evolution in the threat landscape.

The international community has begun to recognize these challenges, but regulatory frameworks and security protocols have struggled to keep pace with technological advancement. Traditional approaches to CBRN security, based on controlling access to physical materials and technical knowledge, must be updated to address the realities of AI-enabled knowledge democratization. This requires new thinking about how we protect sensitive information, verify compliance with international agreements, and maintain effective control over CBRN materials and processes in an increasingly connected and AI-enabled world.

9.2 The Evolution of CBRN Facility Operations

The digital transformation of CBRN facilities has fundamentally altered how these installations operate and manage security. Traditional operational boundaries between physical and cyber domains have blurred, creating a complex web of interdependencies that demands new approaches to safety and security. This evolution represents not just a technological shift but a fundamental change in how we must think about facility operations and risk management.

Modern CBRN facilities increasingly rely on interconnected digital systems for critical operations. These systems range from basic process control mechanisms to sophisticated AI-driven analytics platforms that manage entire facility operations. The integration of these technologies has created unprecedented operational efficiencies but has also introduced new vulnerabilities that must be carefully managed. For instance, a modern chemical processing facility might use AI systems to optimize reaction conditions, monitor safety parameters, and manage supply chains simultaneously - creating multiple potential points of failure or manipulation.

The transformation is particularly evident in how facilities handle sensitive processes and materials. Traditional approaches relied heavily on physical security measures and human oversight. Today, AI systems actively participate in decision-making processes, often operating with significant autonomy. This shift has improved precision and efficiency but has also created new challenges in ensuring proper oversight and maintaining operational security. For example, an AI system optimizing a chemical production process might identify more efficient synthesis routes that could potentially be exploited for unauthorized purposes.

The integration of AI into facility operations has also transformed how knowledge is managed and applied within CBRN facilities. Previously, operational expertise resided primarily in the minds of experienced personnel who understood facility processes through years of hands-on experience. Now, much of this knowledge is captured and operationalized through AI systems that can analyze vast amounts of operational data, identify patterns, and make complex decisions in real-time. This shift has improved operational consistency but has also created new risks related to the protection of sensitive operational knowledge.

Supply chain management in CBRN facilities has undergone a similar transformation. AI systems now monitor and optimize the flow of materials, track inventory levels, and manage supplier relationships. These systems can detect supply chain anomalies and predict potential disruptions before they occur. However, this integration also creates new vulnerabilities, as these same systems could potentially be manipulated to hide unauthorized activities or facilitate the diversion of sensitive materials.

The evolution of facility operations has particularly affected how safety and security measures are implemented. Traditional safety systems relied on relatively simple automated controls backed by human oversight. Modern facilities employ sophisticated AI-driven safety systems that can monitor multiple parameters simultaneously, predict potential safety issues before they occur, and automatically initiate corrective actions. While these systems have generally improved safety outcomes, they have also created new challenges in ensuring system integrity and preventing potential manipulation.

Personnel roles within CBRN facilities have also evolved significantly. Operators must now understand not only the physical processes they oversee but also the AI systems that help control them. This has created new training requirements and changed how facilities manage human resources. The traditional distinction between operational and technical staff has blurred, requiring new approaches to personnel development and security clearance processes.

9.3 Emerging Risk Categories

The integration of AI into CBRN facilities has created a complex landscape of emerging risks that extends far beyond traditional security concerns. These new challenges combine technological vulnerabilities with human factors in ways that were virtually impossible to anticipate when many facilities were initially designed. The risk landscape has become particularly complex in chemical facilities, where AI systems can potentially influence both process control and material handling in subtle but dangerous ways.

Advanced persistent threats have evolved to exploit the increasing sophistication of facility control systems. Unlike traditional cyber attacks that might focus on data theft or system disruption, modern threats can manipulate facility operations while maintaining the appearance of normal function. For instance, an AI-enabled attack might gradually modify chemical process parameters over time, creating dangerous conditions while staying within apparent safety limits. These attacks can be particularly insidious because they exploit the very systems designed to enhance facility safety and efficiency.

The risk of process manipulation has become increasingly sophisticated with the advent of AI-enabled control systems. Modern CBRN facilities rely heavily on automated systems to maintain optimal operating conditions. While these systems have generally improved safety and efficiency, they have also created new vulnerabilities. An advanced attacker might use AI to learn normal operational patterns and then implement subtle changes that could compromise safety or facilitate unauthorized production while evading detection by traditional monitoring systems.

Knowledge exploitation represents another critical risk category. The digitalization of facility operations has created vast repositories of operational data and process knowledge. This information, when analyzed by sophisticated AI systems, could reveal sensitive details about facility operations, security measures, and potential vulnerabilities. The risk extends beyond direct cyber attacks - AI systems could potentially be used to piece together sensitive information from seemingly innocuous public data sources, creating new challenges for information security.

The convergence of physical and cyber systems has created new vulnerabilities at the intersection of these domains. Modern CBRN facilities often use integrated systems that control both physical access and digital operations. An attack that compromises these systems could have cascading effects across multiple facility systems. For example, an AI-enabled attack might simultaneously manipulate process controls while interfering with physical security systems, creating opportunities for unauthorized access or material diversion.

Supply chain integrity has emerged as a particularly complex risk area. Modern CBRN facilities rely on sophisticated supply chain management systems that use AI to optimize inventory levels and manage supplier relationships. These systems create new vulnerabilities that could be exploited to introduce contaminated materials, divert sensitive substances, or manipulate facility operations through supply chain disruptions. The global nature of modern supply chains amplifies these risks, as attacks could potentially originate from anywhere in the world.

The rise of synthetic biology and advanced chemical synthesis capabilities has created new risks related to the potential production of unauthorized materials. AI systems can now suggest novel synthesis routes, optimize reaction conditions, and predict the properties of new compounds. While these capabilities have legitimate applications in research and development, they could potentially be misused to develop new chemical or biological agents that bypass existing control measures. This risk is particularly acute in facilities that handle dual-use materials or conduct advanced research.

The human factor in security has become more complex with the integration of AI systems. Insider threats have evolved beyond traditional concerns about physical access and material theft. Modern insider threats might involve the manipulation of AI systems, the exploitation of automated processes, or the use of legitimate access to gather data that could be analyzed by AI systems to reveal sensitive operational details. The challenge of detecting and preventing these threats is compounded by the increasing complexity of facility operations and the growing number of personnel who have some level of access to critical systems.

9.4 Chemical Facility-Specific Considerations

The unique characteristics of chemical facilities create distinct challenges in the context of AI integration and cybersecurity. These facilities often handle large volumes of hazardous materials under precisely controlled conditions, making them particularly vulnerable to AI-enabled manipulation. The complexity of chemical processes, combined with the potential for cascading effects from even minor process disruptions, requires special consideration in the modern threat landscape.

Chemical processing facilities face unprecedented challenges in maintaining process integrity in an AI-enabled environment. Modern chemical plants rely on sophisticated control systems that manage complex reactions, maintain precise temperature and pressure conditions, and ensure proper mixing and separation of materials. The introduction of AI has enhanced these capabilities but has also created new vulnerabilities. For instance, an AI system compromised by malicious actors could subtly alter reaction conditions while presenting normal readings to human operators, potentially leading to dangerous situations or the production of unauthorized materials.

The storage and handling of hazardous materials presents another critical area of concern. Chemical facilities often maintain significant inventories of dangerous substances that require careful management. AI systems now play a crucial role in monitoring storage conditions, tracking inventory levels, and managing material movements. While these systems have generally improved safety and efficiency, they have also created new risks. A sophisticated attack could potentially manipulate inventory records to hide material diversion or alter storage conditions in ways that could lead to dangerous chemical reactions.

Process optimization capabilities, enhanced by AI, present both opportunities and risks for chemical facilities. Modern AI systems can analyze vast amounts of operational data to identify more efficient production methods and reduce waste. However, these same capabilities could potentially be exploited to optimize the production of prohibited substances or to identify novel synthesis routes that bypass existing control measures. The dual-use nature of many chemical processes makes this risk particularly acute, as legitimate process improvements could potentially be adapted for malicious purposes.

Transportation and logistics within chemical facilities have become increasingly automated and AI-dependent. Modern facilities use sophisticated systems to manage material movements, coordinate deliveries, and track shipments. These systems improve efficiency but also create new vulnerabilities in the supply chain. AI-enabled attacks could potentially manipulate shipping records, redirect hazardous materials, or create conditions that compromise safe transport protocols.

Emergency response systems in chemical facilities have evolved to incorporate AI capabilities for incident detection and response coordination. While these systems enhance safety under normal conditions, they also present new attack vectors. A sophisticated adversary could potentially use AI to interfere with emergency response systems, either by generating false alarms that disrupt operations or by masking genuine emergency conditions until it's too late for effective intervention.

The integration of research and development activities with production operations creates additional challenges. Many chemical facilities maintain research laboratories that use AI to accelerate the development of new products and processes. The connection between research systems and production networks, while beneficial for efficiency, creates potential pathways for the exploitation of sensitive information or the introduction of malicious code into production systems.

Quality control systems, now heavily reliant on AI for real-time analysis and adjustment, present another area of vulnerability. These systems monitor product quality and adjust process parameters to maintain specifications. An attack that compromises these systems could potentially allow the production of off-specification materials without detection, with implications for both product safety and regulatory compliance.

9.5 Protection Strategies and Integration

The complexity of modern CBRN facilities demands a sophisticated, multi-layered approach to protection that integrates traditional security measures with advanced AI-enabled defenses. This integration must account for both the unique characteristics of individual facilities and the broader context of evolving global threats. Protection strategies must be adaptive, responsive, and capable of addressing both current and emerging challenges.

System architecture in modern CBRN facilities must be designed with security as a fundamental consideration rather than an add-on feature. This begins with the implementation of rigorous segmentation between critical systems, creating multiple layers of protection that can contain potential breaches. For instance, process control networks should be physically and logically separated from administrative systems, with strictly controlled interfaces between different security zones. This segmentation must be dynamic, capable of adapting to new threats while maintaining operational efficiency.

The implementation of advanced monitoring capabilities represents a critical component of modern protection strategies. Modern CBRN facilities require sophisticated systems that can monitor both physical processes and digital operations simultaneously. These systems must be capable of detecting subtle anomalies that might indicate manipulation while avoiding false alarms that could disrupt legitimate operations. AI-enabled monitoring systems can analyze patterns across multiple parameters, identifying potential threats that might be invisible to traditional security measures.

Access control systems have evolved to incorporate sophisticated authentication mechanisms that go beyond traditional credentials. Modern facilities implement multi-factor authentication systems that combine physical tokens, biometric data, and behavioral analysis to ensure that only authorized personnel can access sensitive areas and systems. These systems must be intelligent enough to recognize legitimate variations in access patterns while identifying suspicious behavior that might indicate a security threat.

The protection of process control systems requires particular attention in chemical facilities. These systems must maintain precise control over chemical reactions and material handling while remaining resistant to manipulation. Modern protection strategies incorporate real-time verification of control system inputs and outputs, using AI-enabled analysis to detect unauthorized modifications to process parameters. This includes monitoring both the direct control signals and the secondary indicators that might reveal subtle manipulation attempts.

Emergency response capabilities must be integrated into the overall protection strategy while remaining secure against potential manipulation. Modern facilities implement sophisticated emergency management systems that can coordinate response actions across multiple domains. These systems must be protected against both direct attacks and indirect manipulation through sensor data or communication channels. Regular testing and validation of emergency response systems helps ensure their reliability while identifying potential vulnerabilities.

The human element remains crucial in facility protection, requiring comprehensive training programs that address both traditional security procedures and emerging threats. Personnel must understand how AI systems can be both tools for protection and potential vectors for attack. Training programs must be continuous and adaptive, evolving to address new threats as they emerge. This includes regular exercises that simulate various attack scenarios, helping personnel develop the skills needed to recognize and respond to sophisticated threats.

Supply chain security has become increasingly important as facilities rely more heavily on automated ordering and inventory management systems. Protection strategies must address both physical and digital aspects of supply chain security, ensuring the integrity of materials from source to point of use. This includes implementing sophisticated tracking systems that can detect tampering or diversion while maintaining efficient operations.

International cooperation plays an increasingly important role in facility protection, as threats often transcend national boundaries. Facilities must participate in information sharing networks that allow rapid dissemination of threat intelligence while protecting sensitive operational details. This cooperation extends to the development of common standards and protocols for facility protection, ensuring consistency in security measures across different jurisdictions.

9.6 Policy Development and International Framework

The rapidly evolving landscape of AI-enabled threats to CBRN facilities demands a comprehensive reconsideration of existing policy frameworks and international cooperation mechanisms. Traditional regulatory approaches, developed in an era of primarily physical threats, must be adapted to address the complex challenges presented by AI integration and knowledge democratization. This evolution requires careful balance between promoting beneficial technological advancement and maintaining effective control over sensitive operations and materials.

International verification regimes face particular challenges in adapting to AI-enabled facility operations. The traditional approach to verification, based largely on physical inspection and material accounting, must now incorporate mechanisms for evaluating the integrity of AI systems and digital controls. Inspectors must be equipped with new tools and methodologies for assessing whether AI-enabled systems are being used appropriately and securely. This includes developing new protocols for examining AI decision logs, verifying system integrity, and detecting potential manipulation of automated processes.

The development of new international standards for AI implementation in CBRN facilities has become increasingly urgent. These standards must address not only the technical aspects of AI system security but also the broader implications for facility operations and safety. For instance, standards must define acceptable levels of AI autonomy in critical decisions, establish requirements for human oversight, and specify minimum security measures for AI-enabled control systems. The challenge lies in creating standards that are both rigorous enough to ensure safety and flexible enough to accommodate rapid technological advancement.

Information sharing frameworks have become particularly critical in the context of AI-enabled threats. The global nature of these threats requires enhanced mechanisms for sharing threat intelligence, best practices, and incident response experiences. However, this sharing must be balanced against the need to protect sensitive facility information and maintain competitive advantages. New frameworks must be developed that allow facilities to benefit from collective security knowledge while maintaining appropriate confidentiality of proprietary information.

National regulatory frameworks must evolve to address the specific challenges posed by AI integration in CBRN facilities. This includes updating licensing requirements, inspection protocols, and compliance monitoring mechanisms. Regulators must develop new competencies in evaluating AI systems and their potential impact on facility safety and security.

This may require the establishment of specialized units within regulatory bodies focused on AI-related risks and controls.

The role of international organizations in coordinating response to AI-enabled threats has become increasingly important. Organizations such as the International Atomic Energy Agency (IAEA) and the Organisation for the Prohibition of Chemical Weapons (OPCW) must adapt their procedures and capabilities to address new challenges. This includes developing new guidance documents, training programs, and verification protocols that specifically address AI-related risks and controls.

Export control regimes face particular challenges in addressing AI technologies. The dual-use nature of many AI systems, combined with their often intangible nature, creates new complexities in controlling their proliferation. Traditional approaches to export control, focused primarily on physical items and specific technologies, must be adapted to address the unique characteristics of AI systems and knowledge. This may require new frameworks for evaluating and controlling the transfer of AI capabilities that could be misused in CBRN facilities.

9.7 Future Considerations

The future security landscape for CBRN facilities will be shaped by continuing technological advancement and the evolving nature of global threats. Understanding and preparing for these future challenges requires a forward-looking approach that considers both technological trends and their potential implications for facility security and operations. This preparation must account for both anticipated developments and the potential for unexpected technological breakthroughs that could fundamentally alter the threat landscape.

The convergence of AI with other emerging technologies presents particularly complex challenges for future facility security. Quantum computing, for instance, may soon enable AI systems to break current encryption methods, requiring fundamental changes in how facilities protect sensitive data and control systems. Similarly, advances in biotechnology and synthetic chemistry, enhanced by AI capabilities, may create new possibilities for the production of harmful materials that bypass current detection and control measures.

Remote operation capabilities are likely to expand significantly in the coming years, driven by both technological advancement and operational requirements. This trend will create new challenges for facility security, as the separation between physical operations and control systems continues to grow. Future security measures must address the vulnerabilities created by remote operations while maintaining operational efficiency. This may require new approaches to authentication, system monitoring, and incident response that can function effectively across distributed operations. The evolution of AI capabilities will likely lead to increasingly sophisticated autonomous systems in CBRN facilities. While these systems can enhance efficiency and safety, they also create new security challenges that must be addressed. Future security frameworks must consider how to maintain effective human oversight of autonomous systems while preventing their potential misuse. This includes developing new approaches to system validation, performance monitoring, and emergency intervention.

Workforce development presents another critical consideration for future facility operations. As AI systems become more sophisticated, the skills required for facility operation and security will continue to evolve. Future personnel will need to combine traditional technical knowledge with advanced understanding of AI systems and their potential vulnerabilities. This will require new approaches to training and certification that can keep pace with technological advancement.

9.8 Conclusions

The security of CBRN facilities has entered a new era where traditional threats combine with AI-enabled risks to create unprecedented challenges. Success in this environment requires a comprehensive approach that integrates physical security, cybersecurity, and human factors while remaining adaptable to emerging threats. The democratization of knowledge through AI has fundamentally altered the security landscape, requiring new approaches to facility protection and control.

International cooperation will become increasingly crucial as threats continue to evolve and transcend national boundaries. The development of effective security measures requires shared understanding of threats and coordinated response capabilities. This includes not only technical cooperation but also the development of common standards and protocols for facility security. The future security of CBRN facilities will depend on our ability to anticipate and address evolving challenges while maintaining effective control over critical operations. This requires ongoing commitment to technological advancement, personnel development, and international cooperation. Success in this endeavor will require continued investment in both technical capabilities and human expertise, combined with flexible and adaptive security frameworks that can evolve to meet new challenges as they emerge.

The strategies and approaches outlined in this chapter provide a foundation for addressing current and emerging threats to CBRN facilities. However, the dynamic nature of these threats requires constant vigilance and adaptation. Facility operators, regulators, and security professionals must remain committed to continuous improvement and innovation in security measures, ensuring that protective measures keep pace with evolving threats.

10 INDUSTRIAL RELIABILITY, CYBERSECURITY, AND RESILIENCE EDUCATION: CONCEPT

The modern industrial sector is undergoing a profound digital transformation, characterized by the convergence of advanced technologies, the integration of Information Technology (IT) with Operational Technology (OT), and the widespread adoption of the Internet of Things (IoT) and Industrial IoT (IIoT). While these advancements bring unprecedented operational efficiency and innovation, they also introduce complex cybersecurity risks and reliability challenges that threaten the safety, security, and continuity of industrial operations.

To address these multifaceted challenges, a comprehensive and tailored educational system is required. This chapter presents a concept for an integrated educational framework designed to develop the necessary competencies and skills in industrial reliability, cybersecurity, and resilience. This approach aims to bridge the gap between conventional IT security education and the unique requirements of industrial environments, emphasizing critical competencies, regulatory knowledge, practical skills, and continuous learning.

10.1 Background and Rationale for Integrated Education

The shift toward interconnected, digitalized industrial systems has significantly expanded the attack surface for cyber threats, making cybersecurity and reliability crucial elements of industrial operations. OT systems, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, traditionally isolated from network-based threats, are now increasingly connected to IT networks. This connectivity exposes these systems to new vulnerabilities that require specialized knowledge and skills to secure.

Traditional educational programs often lack a focus on the unique challenges posed by OT environments. Industrial settings involve specific operational constraints, including real-time processing requirements, legacy systems, and safety-critical operations, which make the application of conventional cybersecurity measures more complex. Furthermore, the proliferation of IoT and IIoT devices in industrial environments adds layers of complexity, as these devices need to be managed, secured, and monitored effectively.

This situation necessitates a multidisciplinary educational approach that encompasses knowledge of industrial processes, critical computing, IoT/IIoT security, human-machine interaction, and regulatory frameworks. The proposed educational concept aims to create a comprehensive framework to develop skilled professionals capable of addressing the diverse and evolving demands of industrial cybersecurity, reliability, and resilience.

10.2 The (Big) Safety and Security Model

The "(Big) Safety and Security Model" is a holistic framework for understanding and addressing the complex relationship between safety and security in industrial environments. In this model, safety and security are viewed as interdependent elements of operational reliability and resilience rather than separate domains.

10.2.1 Key Elements of the Model

1. Integration of Safety and Security: The model emphasizes that a breach in cybersecurity can directly impact physical safety. For instance, a cyber-attack on an industrial

control system could result in equipment malfunctions, posing risks to human life and environmental safety.

2. Multi-Layered Defense: The model advocates for a multi-layered defense approach, incorporating physical, procedural, and technological measures to protect industrial environments.
3. Risk Management: Risk assessment and management are central elements of the model, which calls for regular risk evaluations to identify vulnerabilities, implement countermeasures, and adapt to evolving threats.

10.2.2 Educational Application

The "(Big) Safety and Security Model" forms the foundation for building educational programs that cover both safety and cybersecurity. Curriculum topics include:

1. Safety-Cybersecurity Interdependence: Courses explore the relationship between cybersecurity measures and physical safety in industrial environments.
2. Defense-in-Depth Strategies: Practical training focuses on implementing multi-layered security measures, teaching students to build resilient industrial environments.
3. Dynamic Risk Management: Training on applying risk management methodologies that account for both cyber threats and physical safety hazards.

10.3 (Big) Safety and Security Spaces

The concept of "(Big) Safety and Security Spaces" refers to the various environments and contexts within industrial settings where safety and security measures must be applied. These spaces include physical locations, virtual environments, data processing zones, and human-machine interfaces.

10.3.1 Types of Safety and Security Spaces

1. Physical Spaces: Plant floors, control rooms, and equipment areas where physical security measures are critical.
2. Virtual Spaces: Networks, data storage, and cloud services requiring cybersecurity measures.
3. Data Processing Zones: Areas where data is collected, processed, and analyzed, necessitating measures like data encryption and access controls.
4. Human-Machine Interaction Spaces: Interfaces between operators and control systems that require a balance of usability and security.

10.3.2 Educational Integration

The curriculum integrates these safety and security spaces into a comprehensive learning experience:

1. Physical Security Modules: Training on the implementation of physical security measures and their integration with cybersecurity.
2. Data Processing and Analysis: Courses focus on securing data processing zones, emphasizing data integrity and secure information flow.

3. Human-Machine Interaction Security: Training on securing Human-Machine Interfaces (HMIs) by incorporating human factors and behavioral analytics.

10.4 Chain "Data-Information-Knowledge-Activity" and its Role in Security and Safety Management

The "Chain 'Data-Information-Knowledge-Activity'" (DIKA) represents the process of converting raw data into actionable knowledge and activities within industrial environments. Effective management of this chain is vital for both cybersecurity and operational reliability.

10.4.1 Elements of the DIKA Chain

1. Data: Raw, unprocessed information collected from sensors, devices, and control systems.
2. Information: Data that has been processed, structured, and interpreted to provide context and insights.
3. Knowledge: The application of information to gain understanding, predict outcomes, and inform decision-making.
4. Activity: The actions taken based on knowledge, such as implementing security measures or initiating incident response procedures.

10.4.2 Processing and Security & Safety Management

1. Data Collection and Security: Emphasizing secure data collection methods, including encrypted communication between sensors and control systems.
2. Information Analysis: Training students in using data analytics and AI to process information and identify cybersecurity incidents.
3. Knowledge-Based Decision Making: Teaching professionals to use processed information for informed decision-making that ensures safety and security.
4. Automating Activities: Exploring automated responses to detected anomalies or security threats.

10.4.3 Educational Application

The DIKA chain is integrated into the educational framework through:

1. Data Security Courses: Covering techniques for securing data at rest and in transit.
2. Data Analysis and AI for Security: Providing practical training in analyzing industrial data to detect anomalies and respond to cyber threats.
3. Operational Decision-Making: Using case studies to illustrate how knowledge derived from data analysis can optimize security measures.

10.5 Levels and Chains in Safety & Security Management Systems (S&S MS)

The "Levels and Chains S&S MS" concept refers to the multi-tiered structure of safety and security management systems in industrial environments.

10.5.1 Levels of Safety & Security Management

1. Strategic Level: Focuses on policy-making, regulatory compliance, and strategic planning.
2. Tactical Level: Encompasses the development of security plans, risk assessments, and the implementation of security measures.
3. Operational Level: Involves real-time monitoring, incident response, and daily operations.
4. Technical Level: Deals with the technical aspects of cybersecurity, such as configuring firewalls and managing access controls.

10.5.2 Chains of Activities in S&S MS

1. Risk Assessment Chain: A continuous process of identifying, analyzing, and mitigating risks at all levels.
2. Incident Response Chain: Steps taken to detect, respond to, and recover from cybersecurity incidents.
3. Compliance Chain: Ensuring compliance with industry standards, regulations, and internal policies.

10.5.3 Educational Integration

Educational programs teach students how to navigate and manage the different levels and chains of S&S MS:

1. Strategic Management Courses: For senior-level students, focusing on developing security policies and regulatory compliance strategies.
2. Tactical and Operational Training: Practical exercises in designing and implementing security plans and conducting risk assessments.
3. Technical Skills Development: Courses on configuring security technologies and conducting vulnerability assessments.

10.6 Core Competencies and 3 Key Qualifications in the Education System

To meet the unique needs of industrial cybersecurity and resilience, the educational system focuses on developing three key qualifications:

10.6.1 Shaping Reliability and Cybersecurity Policy in Industry

Designed for senior managers, policymakers, and strategists.

Competencies:

- In-depth knowledge of industrial processes and control systems
- Advanced skills in risk assessment and policy development
- Understanding of regulatory compliance in industrial settings

Learning Outcomes:

- Ability to craft comprehensive cybersecurity policies
- Skills in conducting thorough risk assessments
- Capability to manage security programs aligned with business objectives

10.6.2 Management of Reliability and Cybersecurity for Industrial Devices

Targets technical specialists, system architects, and OT security professionals.
Competencies:

- Expertise in ICS security and vulnerability assessments
- Skills in secure system design and IoT security
- Knowledge of industrial network protocols and security measures

Learning Outcomes:

- Ability to design and implement secure architectures for industrial control systems
- Skills in conducting comprehensive vulnerability assessments
- Capability to manage security measures in OT environments

10.6.3 Management of Reliability and Cybersecurity in Industry

Aimed at senior cybersecurity managers and operations executives.
Competencies:

- Strategic cybersecurity planning for industrial environments
- Understanding of operational resilience and business continuity
- Knowledge of emerging technologies and their security implications

Learning Outcomes:

- Ability to develop comprehensive cybersecurity strategies aligned with business goals
- Skills in integrating cybersecurity with broader operational resilience planning
- Capability to lead cross-functional teams in addressing complex cybersecurity challenges

10.7 Practical Training and Industry Collaboration

Practical training is a core component of the educational concept, ensuring students can apply theoretical knowledge in real-world settings. Key components include:

10.7.1 Simulation Exercises

- Use of simulated industrial control systems for hands-on experience
- Practice implementing security measures and conducting vulnerability assessments
- Incident response simulations based on real-world scenarios

10.7.2 Collaborative Projects

- Interdisciplinary projects bringing together IT, OT, and cybersecurity students
- Development of integrated security solutions for industrial environments
- Fostering cross-functional teamwork and communication skills

10.7.3 Industry Partnerships

- Internship programs with industrial organizations
- Guest lectures from industry experts

- Collaborative research projects addressing real-world industrial cybersecurity challenges

10.8 Multidisciplinary and Integrated Approach

A multidisciplinary approach is vital for addressing the complexities of industrial cybersecurity:

10.8.1 IT/OT Convergence

- Courses focusing on managing and securing integrated IT and OT environments
- Understanding the differences and interdependencies between IT and OT domains
- Strategies for secure IT/OT integration in industrial settings

10.8.2 Human Factors and Cybersecurity

- Incorporating aspects of industrial psychology into the curriculum
- Examining how human behavior impacts cybersecurity in industrial environments
- Designing systems and processes that promote secure practices among operators

10.8.3 Engineering and Cybersecurity Integration

- Integrating cybersecurity principles into engineering design processes
- Understanding the security implications of engineering decisions in industrial systems
- Developing secure-by-design approaches for industrial control systems

10.9 Standardization and Certification

Standardization and certification are crucial to ensure a consistent level of expertise among professionals:

10.9.1 Global Certification Programs

- Development of internationally recognized certification programs
- Establishing benchmarks for required competencies in industrial cybersecurity and reliability
- Regular updates to certification requirements to reflect evolving industry needs

10.9.2 Mutual Recognition Agreements

- Promoting agreements between nations and industry bodies
- Ensuring cross-border recognition of cybersecurity qualifications
- Enhancing workforce mobility in the global industrial cybersecurity sector

10.10 Alignment with Industry Standards

- Integrating key industry standards (e.g., IEC 62443, NIST Cybersecurity Framework) into the curriculum

- Teaching students how to implement and maintain compliance with these standards
- Preparing students for roles in standards development and implementation

10.11 Ethical Considerations and Secure-by-Design Principles

Ethics and security-by-design are integral to the curriculum:

10.11.1 Ethical Hacking and Penetration Testing

- Teaching ethical guidelines for vulnerability assessments
- Emphasizing the importance of responsible disclosure
- Balancing security testing with operational safety considerations

10.11.2 Secure-by-Design Approaches

- Incorporating security features into product design from the outset
- Focusing on encryption, secure communications, and lifecycle management
- Developing strategies for securing legacy systems in industrial environments

10.11.3 Privacy and Data Protection

- Understanding data protection regulations in industrial contexts
- Implementing privacy-preserving technologies in industrial data processing
- Balancing data utilization for operational efficiency with privacy concerns

10.12 Future Trends and Adaptation

The concept prepares students for future developments in industrial cybersecurity:

10.12.1 Emerging Technologies

- Understanding the impact of 5G networks on industrial operations and security
- Exploring the implications of quantum computing for industrial cryptography
- Investigating the security aspects of edge computing in industrial environments

10.12.2 Advanced Threat Detection

- Training in the use of AI and machine learning for threat detection and response
- Developing skills in behavioral analytics for monitoring operator actions
- Exploring predictive maintenance from a cybersecurity perspective

10.12.3 Resilience and Adaptive Security

- Teaching strategies for building resilient industrial systems
- Exploring adaptive security measures that evolve with changing threat landscapes
- Developing skills in continuous security monitoring and improvement

10.13 Conclusions

The proposed educational concept presents a comprehensive framework for building the competencies required to address the complex challenges of industrial cybersecurity and reliability. By integrating core elements such as the "(Big) Safety and Security Model," critical computing, IoT security, and the three key qualifications, the educational programs aim to produce professionals who can navigate the evolving landscape of industrial cybersecurity effectively.

This multidisciplinary, practical approach fills the existing skills gap, fosters a culture of security, and equips the workforce to drive secure and resilient industrial operations. As industries continue their digital transformation, the future of industrial cybersecurity will depend on the development and continuous evolution of these competencies, ensuring that industrial organizations can thrive in an increasingly interconnected world.

The success of this educational concept will rely on ongoing collaboration between academia, industry, and regulatory bodies to ensure that the curriculum remains relevant and responsive to emerging challenges. By cultivating a new generation of industrial cybersecurity professionals, this educational framework contributes to the overall security, reliability, and resilience of critical industrial infrastructure in the face of evolving cyber threats.

References

1. IEC TS 62443-1-1:2009 – Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models.
2. IEC 62443-2-1:2024 – Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners.
3. IEC TR 62443-2-3:2015 – Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment.
4. IEC 62443-2-4:2023 – Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers.
5. IEC TR 62443-3-1:2009 – Industrial communication networks – Network and system security - Part 3-1: Security technologies for industrial automation and control systems.
6. IEC TR 62443-3-2:2020 – Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design.
7. IEC 62443-3-3:2013 – Industrial communication networks – Network and system security - Part 3-3: System security requirements and security levels.
8. IEC 62443-4-1:2018 – Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.
9. IEC 62443-4-2:2019 – Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.
10. IEC TS 62443-6-1:2024 – Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4.
11. ISO/IEC 27000:2018 – Information technology — Security techniques — Information security management systems — Overview and vocabulary.
12. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
13. ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls.
14. ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
15. ISO/IEC 27032:2023 – Cybersecurity - Guidelines for Internet security
16. IEC 61508-1:2010 – Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements.
17. IEC 61508-2:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.
18. IEC TS 61508-3-1:2016(E) – Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3-1: Software requirements - Reuse of pre-existing software elements to implement all or part of a safety function.
19. IEC TS 61508-3-2:2024 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3-2: Requirements and guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation.

20. IEC 61508-4:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations.

21. IEC 61508-5:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels.

22. IEC 61508-6:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

23. IEC 61508-7:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures

24. IEC 61511 (all parts), Functional safety – Safety instrumented systems for the process industry sector.

25. IEC TR 63069:2019 – Industrial-process measurement, control and automation – Framework for functional safety and security.

26. IEC Guide 120:2018, Security aspects – Guidelines for their inclusion in publications.

27. NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations. – National Institute of Standards and Technology), 2020.

28. NIST SP 800-53A Rev. 5 – Assessing Security and Privacy Controls in Information Systems and Organizations. – National Institute of Standards and Technologies, 2022.

29. NIST SP 800-82 Rev. 2 – Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). – National Institute of Standards and Technologies, 2015.

30. NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security – National Institute of Standards and Technologies, 2023.

31. NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View. – National Institute of Standards and Technologies, 2011.

32. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 2018.

33. Health and Safety Executive, 2017. Cyber Security for Industrial Automation and Control Systems.

34. U.S. Department of Homeland Security, Chemical Facility Anti-Terrorism Standards (CFATS), 2019 Annual Report, Washington, DC, 2020.

35. Framework for Improving Critical Infrastructure Cybersecurity. – National Institute of Standards and Technologies Version 1.1, 2018.

36. DNV-RP-G108 Cyber security in the oil and gas industry based on IEC 62443 Recommended Practice, October 2021.

37. Computer Security for Nuclear Security, IAEA Nuclear Security Series, No. 42-G, Vienna, 2021.

38. ENISAS (2024): National Cybersecurity Strategies Guidelines & tools; Accessed October 2024 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

39. World Economic Forum. The Global Risks Report 2024, 19th Edition.

40. [1] World Health Organization, Laboratory Biosecurity Guidance, WHO/CDS/EPR/2006.6, Geneva, 2020.

41. NREL/TP-5T00-90302 Cyber-Informed Engineering Research and Development Guide. US Department of Energy. 2024. https://doi.org/10.2172/2448074

42. FY 2024 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap https://www.nitrd.gov/pubs/FY2024-Cybersecurity-RD-Roadmap.pdf

43. Whitepaper Industrial Security based on IEC 62443, TÜViT Nord Group, 2019.

44. Honeywell Industrial cyber security. Safely embrace the digital age with advanced solutions and services to reduce cyber risk BR-18-4 0-ENG | 09/18.

45. The IACS Cybersecurity Certification Framework. (ICCF). Lessons from the 2017 study of the state of the art, European Reference Network for Critical Infrastructure Protection (ERNCIP Project).

46. Lessons for Operators inIndustrial Cybersecurity eBook 2019, ISA, Siemens.

47. Breaking down cybersecurity and functional safety requirements for industrial control systems, Siemens and CSA Group, 2019.

48. Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications, Schneider Electric, 2018.

49. Effectively Maintaining the Security of Industrial Control Systems, Schneider Electric, 2018.

50. How to Effectively Implement ISA 99 / IEC 62443, Forescout, 2019.

51. Establishing zones and conduits industrial cybersecurity center In accordance with the ISA99/IEC 62443 standard, ICC. 2018.

52. Process Control Networks Secure Architecture Design, Honeywell, 2012

53. Industrial cyber security. Safely embrace the digital age with advanced solutions and services to reduce cyber risk. Honeywell, 2018.

54. Technical guide Cybersecurity for ABB drives, ABB, 2017.

55. Define your functional safety and cyber security requirements to optimise safety & security, ABB, 2019.

56. U.S. Department of Energy Cybersecurity strategy 2018-2020.

57. AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan. – American Gas Association, 2006. – 123 p.

58. Common Cybersecurity Vulnerabilities in Industrial Control Systems. – U.S. Department of Homeland Security, 2011. – 76 p.

59. National Cybersecurity and Communications Integration Center / Industrial Control Systems Cyber Emergency Response Team (NCCIC/ICS-CERT). 2015 Year in Review. – U.S. Department of Homeland Security, 2016. – 22 p.

60. Holland Michel, Arthur. 2020. 'The Black Box, Unlocked: Predictability and Understandability in Military AI.' Geneva, Switzerland: United Nations Institute for Disarmament Research. doi: 10.37559/SecTec/20/AI1

61. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security / Yastrebenetsky M., Kharchenko V. (Edits). – IGI Global. – 2014. – 470 p.

62. Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems /Yastrebenetsky M., Kharchenko V. (Edits). – IGI Global. – 2020. – 501 p. DOI: 10.4018/978-1-7998-3277-5

63. T. Nguyen, T. Levin, C. Irvine. High robustness requirements in a Common Criteria protection profile // Proceeding of 2006 IEEE 4th International Workshop on Information Assurance (IWIA). – P.78-87.

64. S. Srinivasan, R. Kumar, J. Vain. Integration of IEC 61850 and OPC UA for Smart Grid automation // 2013 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia). – P. 1-5.

65. Materials of the Tempus project SEREIN "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains" https://serein.eu.org/

66. Materials of the Erasmus+ project ALIOT "Internet of Things: Emerging Curriculum for Industry and Human Applications" https://aliot.eu.org/

67. Babeshko I., Illiashenko O., Di Giandomenico F. Towards Effective Safety and Cybersecurity Co-engineering in Critical Domains, 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2023, pp. 1-8, https://doi.org/10.1109/DESSERT61349.2023.10416431

68. Dotsenko S., Illiashenko O., Budnichenko I., Kharchenko V. (2021) Knowledge Management Model Based Approach to Profiling of Requirements: Case for Information Technologies Security Standards. In: T. Tagarev, K.T. Atanassov, V. Kharchenko, J. Kacprzyk (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies, Springer International Publishing, Volume 84 of the series Studies in Big Data, pp. 255-277 https://doi.org/10.1007/978-3-030-65722-2_16

69. Dotsenko S., Illiashenko O., Kamenskyi S., Kharchenko V. (2021) Embedding of Integrated Security Management System into Industry 4.0 Enterprise Management: Cybernetic Approach. In: T. Tagarev, K.T. Atanassov, V. Kharchenko, J. Kacprzyk (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies, Springer International Publishing, Volume 84 of the series Studies in Big Data, pp. 279-296 https://doi.org/10.1007/978-3-030-65722-2_17

70. Illiashenko O., Kharchenko V., Morozova O., Phillips, C. Internet of Things for Human and Industry Application: ALIOT Project and R&D Issues, PCI 2020: 24th Pan-Hellenic Conference on Informatics, November 20 - 22, 2020 Athens, Greece, Association for Computing Machinery New York, NY, United States, pp. 350-353 https://dl.acm.org/doi/10.1145/3437120.3437338

71. Potii O., Tsyplinskyi Y., Illiashenko O., Kharchenko V. (2020) Criticality Assessment of Critical Information Infrastructure Objects: A Category Based Methodology and Ukrainian Experience. In: Dziech A., Mees W., Czyżewski A. (eds) Multimedia Communications, Services and Security. MCSS 2020. Communications in Computer and Information Science, vol 1284, pp 78-97, Springer, Cham. https://doi.org/10.1007/978-3-030-59000-0_7

72. Dotsenko, S., Fesenko H., Illiashenko O., Kharchenko V., Moiseenko V., Yermolenko L. Integration of Security, Functional and Ecology Safety Management Systems: Concept and Industrial Case, 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, May 14-18, 2020, pp. 470-474, DOI: https://doi.org/10.1109/DESSERT50317.2020.9125010

73. Dotsenko S., Illiashenko O., Kamenskyi S., Kharchenko V. Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045, Information & Security vol. 43, no. 3 (2019): 305-317, https://doi.org/10.11610/isij.4323

74. Dotsenko S., Illiashenko O., Budnichenko I., Kharchenko V. (2021) Knowledge Management Model-Based Approach to Profiling of Requirements: Case for Information Technologies Security Standards. In: T. Tagarev, K.T. Atanassov, V. Kharchenko, J. Kacprzyk (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies, Springer International Publishing, Volume 84 of the series Studies in Big Data, pp. 255-277 https://doi.org/10.1007/978-3-030-65722-2_16

75. Illiashenko O., Kharchenko V., Kor A-L. Gap-analysis of Assurance Case-Based Cybersecurity Assessment: Technique and Case Study // Advanced Information Systems. – 2018. – №2(1). – P. 64–68. https://doi.org/10.20998/2522-9052.2018.1.12

76. Kharchenko V., Yastrebenetsky M. About Concept of Big Safety // Reliability Theory&Application. – 2021. - No 1 (61), Volume 16, March. - P.1-17. https://doi.org/10.24412/1932-2321-2021-161-13-29

77. Kharchenko V., Fesenko H., Illiashenko O. Quality Models for Artificial Intelligence Systems: Characteristic-Based Approach, Development and Application // Sensors. - 2022. - 22, 4865 – P. 1-29. https://doi.org/10.3390/s22134865

78. Lysenko S., Bobrovnikova K., Kharchenko V., Savenko O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency // Algorithms. – 2022. - 15(7): 239. - P.1 -27. https://doi.org/10.3390/a15070239

79. Kharchenko V., Ponochovnyi Y., Ivanchenko O., Fesenko H., Illiashenko O. Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems // Cryptography. – 2022. - 6, 44. – P.1-32. https://doi.org/10.3390/cryptography6030044

80. Dotsenko S., Illiashenko O., Kharchenko V., Morozova O. Integrated Information Model of an Enterprise and Cybersecurity Management System: From Data to Activity // Int. J. Cyber Warf. Terror. – 2022. - 12(2). – P. 1-21. https://doi.org/10.4018/IJCWT.305860

81. Veprytska O., Kharchenko V. AI powered attacks against AI powered protection: classification, scenarios and risk analysis. Proceedings of the 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece. - 2022. - P. 1-7. https://doi.org/10.1109/DESSERT58054.2022.10018770.

82. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., Di Giandomenico F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection // Entropy. - 2023. - Vol. 25, no. 8. - P. 1–35. https://doi.org/10.3390/e25081123

83. Fesenko H., Illiashenko O., Kharchenko V., Kliushnikov I., Morozova O., Sachenko A., Skorobohatko S. Flying Sensor and Edge Network-Based Advanced Air Mobility Systems: Reliability Analysis and Applications for Urban Monitoring // Drones. - 2023. - Vol. 7, no. 7 - P. 1–27. https://doi.org/10.3390/drones7070409

84. Fedorenko G., Fesenko H., Kharchenko V., Kliushnikov I., Tolkunov I. Robotic-biological systems for detection and identification of explosive ordnance: concept, general structure, and models. Radioelectronic and Computer Systems. 2023. No. 2(106). P. 143–159. https://doi.org/10.32620/reks.2023.2.12

85. Moskalenko V., Kharchenko V., Moskalenko A., Kuzikov B. Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods. Algorithms. 2023. Vol. 16, no. 3, article no.165. P. 1–44. https://doi.org/10.3390/a16030165

86. Abakumov A., Kharchenko V. Combining Experimental and Analytical Methods for Penetration Testing of AI-Powered Robotic Systems. CEUR Workshop Proceedings. - 2023. - Vol. 3403. - P. 526–538. https://ceur-ws.org/Vol-3403/paper40.pdf

87. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique // Radioelectronic and Computer Systems. - 2023. - No. 4(108). - P. 143–159. http://doi.org/10.32620/reks.2023.4.12

88. Kharchenko V., Ponochovnyi Y., Babeshko I. Multi-fragmental and multi-phase availability models of the safety-critical I&C systems with two-cascade redundancy // International Journal of Electronics and Telecommunications. - 2024. - Vol. 70, No. 1. – P. 211-218. https://doi.org/10.24425/ijet.2024.149533

89. Yastrebenetsky, M., & Kharchenko, V. (2024). Analysis of big safety attributes: from critical technical systems to individuals and communities // EUREKA: Physics and Engineering. -2024 - No6. – P. 129-141. https://doi.org/10.21303/2461-4262.2024.003565

Eugene Babeshko
Oleg Illiashenko
Vyacheslav Kharchenko
Olga Morozova
Adam Paturej
Krzysztof Paturej
Emil Peña
Oleksandr Potii
Zdzisław Rapacki

MANUAL
ON CYBERSECURITY, RELIABILITY AND RESILIENCE ASSURANCE IN THE CRITICAL INDUSTRIES

Monography

Edited by
Vyacheslav Kharchenko, Adam Paturej, Oleksandr Potii

Computer typesetting
Oleg Illiashenko, Olga Morozova

Design of cover
Paweł Ostrek

Print
International Centre for Chemical Safety and Security (ICCSS)
Leszno 8/1
01-192 Warsaw
Poland