University of Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation:	Spring semester, 2021
Industrial Asset Management	Open

Author: William Ragnar Gaustad

Supervisor: Professor Jayantha Prasanna Liyanage, PhD

Title of master's thesis:

Cyber Security applications in Cyber Physical Systems

Credits: 30 ECTS

Keywords:	
Cyber Physical Systems Cyber Security Industry 4.0 Standardization Systems Architecture	Number of pages: 99 + supplemental material/other: 0 Stavanger, 14-06-2021

Cyber Security Applications in Cyber Physical Systems

William Gaustad

Faculty of Science and Technology

University of Stavanger

June 2021

Supervisor: Jayantha Prasanna Liyanage

Abstract

The dynamic evolutions of Cyber Physical Systems in the Industry 4.0 context are considered, their inherent complexity and pertinent interfaces are examined contemplating the influence of the current security environments and their future trends. The increased number of spheres of influence affecting the Cyber Security of Cyber Physical Systems generate an escalation of the required interpretations for enabling a secure system, consequently organizations have encountered hindrance towards the required security targets.

It is intended with the present work to comprehend the convolutions surrounding the organizations interpretation of securing a Cyber Physical System, subjected on selected topics, aiming to elucidate influencing factors and their relationships.

The research conducts an introductory investigation of the perceptions of influencing factors for secured Cyber Physical Systems, namely the digitalization trend, reference architectures and their heterogeneity in Industry 4.0, application domain nuances, Cyber Security trends and its latest technological developments. Consequently, it surveys the Cyber Physical Systems and Cyber Security associations reviewing the present industrial landscape through references to organizations cultural and strategical facets and typical employed governance. Due to the unique features of a Cyber Physical System, the latter is further probed accounting for deployment review during the lifecycle. The objective is to assess omissions which influence the application of Cyber Security in Cyber Physical Systems, with particular incidence in the organizations, governance and, technology contexts, where improvements and recommendations in the organizations security culture and, governance interpretation and application of the IEC 62443 are derived and leaving further observations which can support the development of future researches.

Key Words: *Cyber Physical Systems, Cyber Security, Industry 4.0, Standardization, Systems Architecture.*

Preface

The elaboration of the present work culminates my attendance on the Master of Science degree in Industrial Asset Management offered by the faculty of Science and Technology at the University of Stavanger.

It was a great honor to have received the opportunity of accomplishing the studies on a topic of significant interest for both my personal and professional perspectives.

For its realization, I would like to express my gratitude to my supportive family, friends, colleagues, with a special endorsement to my thesis supervisor Professor Jayantha Prasanna Liyanage.

William Ragnar Gaustad

Stavanger, June 2021

"Science and technology multiply around us. To an increasing extent they dictate the languages in which we speak and think. Either we use those languages, or we remain mute."

J.G. Ballard

Contents

Abstract I
Preface II
Contents III
List of figures VI
List of tables IX
1 Introduction 1
1.1 Background 2
1.1.1. Motivation 3
1.2 Scope of Work 4
1.2.1. Objectives 5
1.3 Methodology 5
1.4 Limitations 6
1.5 Thesis structure 6
2 Digitalization 7
3 Cyber Physical Systems 9
3.1 Heterogeneity 9
3.2 Conceptual architectures 11
3.2.1 ANSI/ISA - 95 11
3.2.2 CPS 5C 12
3.2.3 CPS 8C 14
3.2.4 Summary 15
3.3 Application domains 16
3.3.1 Health 16
3.3.2 Energy 17
3.3.3 Transportation 18
3.3.4 Production systems 20
3.3.5 Robotics 21
3.3.6 Summary 22
4 Cyber security 23
4.1 Concepts 24
4.1.1 Security and privacy 24
4.1.2 Attacks and threats 25
4.1.3 Cyber Kill Chain 29

4.1.4 Threat agents and trends 30
4.2 Incidences 32
4.2.1 LockerGoga 32
4.2.2 NotPetya 33
4.2.3 Sunburst 34
4.2.4 Summary 35
4.3 Technological developments 36
4.3.1 Lightweight cryptography 36
4.3.2 Intrinsic security 37
4.3.3 Machine learning 39
4.3.4 Intrusion detection 41
4.3.5 Fuzzy logic 42
4.3.6 Microsegmentation 43
4.3.7 Summary 44
5 Current industrial landscape review within the Cyber Security and Cyber Physical Systems domains 45
5.1 Organizations 45
5.1.1 Culture 45
5.1.2 Strategy 46
5.1.3 Summary 46
5.2 Governance 46
5.2.1 International Organization for Standardization - ISO 48
5.2.2 International Electrotechnical Commission - IEC 50
5.2.3 Norwegian Oil and Gas Association - NOG 54
5.2.4 Summary 55
6 Cyber Security governance review in Cyber Physical Systems lifecycle 56
6.1 Concept 58
6.2 Development 60
6.3 Production 66
6.4 Utilization 68
6.5 Support 69
6.6 Retirement 71
6.7 Summary 71
7 Gap analysis 73
7.1 Organizations 75
7.1.1 Culture 75

7.1.2 Strategy 76
7.2 Governance 76
7.2.1 Security program maturity 77
7.2.2 Interpretation 78
7.2.3 Execution 80
7.3 Technology 81
7.4 Summary 82
8 Recommendations and expected effects 83
8.1 Recommendations 83
8.1.1 Cyber security culture: ”The knowledge driver” 83
8.1.2 Convergence of IEC 62443 publications reference topologies 84
8.1.3 Improved systems integrator entity engagement 84
8.2 Expected effects 85
8.2.1 Augmented awareness/cognitive levels 85
8.2.2 Reduced vulnerability surface 85
9 Discussions 86
9.1 Summary 86
9.2 Learning outcomes 86
9.3 Challenges 87
9.4 Recommendations for future works 87
10 Conclusion 88
References 89
Bibliography 89
Standards 94
Webography 97

List of figures

Chapter 1

Figure 1. 1: Trend in capability versus system complexity as a defense mechanism (A) Past, (B) Present and (C) Future, (Sonalker, Griffor, 2017). 3

Chapter 2

Figure 2. 1: Overview of the six core elements of enterprise architecture (Bossert et al., 2021). 8
Figure 2. 2: Shifting applications to perpetual evolution architecture (Bossert et al., 2021). 8

Chapter 3

Figure 3. 1: Cyber Physical Systems conceptual layout (Ali, Balushi et al., 2018). 9
Figure 3. 2: ISA-95 Architecture for Industrial Automation Systems (Dai et al, 2019). 11
Figure 3. 3: Service-Oriented Architecture Enabled Industrial Cloud and Edge Computing Systems (Dai et al., 2019). 12
Figure 3. 4: The CPS 5C architecture (Lee et al., 2015). 12
Figure 3. 5: Applications and techniques associated with each level of the 5C architecture (Lee et al., 2015). 13
Figure 3. 6: The proposed CPS 8C architecture (Jiang, 2018). 14
Figure 3. 7: A conceptual overview of medical cyber-physical systems (Lee et al., 2017). 16
Figure 3. 8: CPS electric energy system with its embedded DyMonDS (Ilic, 2017). 17
Figure 3. 9: Three TCPS communications: V2V, V2I, and D2D (Han et al., 2017). 18
Figure 3. 10: Function layers of transportation cyber-physical systems (Wu et al., 2017). 19
Figure 3. 11: Cyber-physical production system (CPPS) architecture framework (Lee, 2018). 20
Figure 3. 12: ICMS system architecture (Wang, 2018). 21
Figure 3. 13: Comparison of conventional, web-based and cloud-based robotic cells (Wang, 2018). 21

Chapter 4

Figure 4. 1: Running total of ransomware leak site publications in 2020 (PwC, 2021). 23
Figure 4. 2: Mapping of cyber security principles to the physical security controls they enable (Fink et al., 2018). 24
Figure 4. 3: Mapping example security mechanisms (rows) to information security principles and physical security controls they enable (columns) (Fink et al., 2018). 25
Figure 4. 4: Tree diagram of attacks and threats on Cyber Physical Systems Technologies (Maleh et al., 2019). 25
Figure 4. 5: Man-In-The-Middle - MITM Attack (Ponnusamy et al., 2020). 27
Figure 4. 6: Network Access Security Model (Stallings, 2017). 27
Figure 4. 7: Periodic Table of Cybersecurity Threats (Pogrebna et al., 2019). 28
Figure 4. 8: Adapted Lockheed Martin Cyber Kill Chain steps (Bahrami et al., 2019) 29
Figure 4. 9: CKC based taxonomy of APT features (Bahrami et al., 2019). 30
Figure 4. 10: Involvement of threat agents in the top cyberthreats (Sfakianis et al.,2019). 31
Figure 4. 11: The LockerGoga ransom note (Panda Security, 2019). 32

Figure 4. 12: Cyber attack on Hydro's worldwide organization High-level timeline of events (Hydro, 2019). 32
Figure 4. 13: Top 20 countries depend on number of infected organizations (Fayi, 2018). 33
Figure 4. 14: Creating SolarWinds Orion Software (Nides, 2021). 34
Figure 4. 15: Sunburst Attack Chain (Nides, 2021). 35
Figure 4. 16: Trade-offs between security, cost, and performance (Tawalbeh et al., 2018). 36
Figure 4. 17: Building Blocks for Intrinsic Security (Rooyakkers et al. 2016). 37
Figure 4. 18: An OSA™Cyber Architecture with an Intrinsic Hardware Root of Trust (Rooyakkers et al. 2016). 38
Figure 4. 19: Generic model of applicability of machine learning to IoT network for threat detection (Sharma et al., 2020). 39
Figure 4. 20: SIEM Pattern as UML component diagram (Vielberth et al., 2018). 40
Figure 4. 21: Classification of anomaly based intrusion detection techniques (Möller, 2021). 41
Figure 4. 22: Block diagram of a generic rule based intrusion detection system (Möller, 2021). 42
Figure 4. 23: Left - 3D Surface for Model-1, Right - 3D Surface for Model-2 (Jana et al, 2018). 42
Figure 4. 24: Distributed segmentation with network overlay isolation (Chowdary et al., 2018). 43

Chapter 5

Figure 5. 1: Example of a Security Planning Process (Stallings, 2018). 47
Figure 5. 2: Cybersecurity Standards Adoption (Schreider, 2020). 47
Figure 5. 3: ISO Information Technology Security Standards (Schreider, 2020). 48
Figure 5. 4: Parts of the IEC 62443 Series and their status (ISA, 2021). 51

Chapter 6

Figure 6. 1: Life cycle model with some of the possible regressions (ISO/IEC/IEEE 27748-1, 2018). 57
Figure 6. 2: Model Relationships (IEC 62443-1-1, 2009). 59
Figure 6. 3: Reference architecture alignment with an example segmented architecture (IEC 62443 2-1, 2010). 61
Figure 6. 4: Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk (IEC 62443-3-2, 2020). 62
Figure 6. 5: Detailed cyber security risk assessment workflow per zone or conduit (IEC 62443-3-2, 2020). 63
Figure 6. 6: Security level lifecycle model: Assess phase (IEC 62443 2-1, 2010). 64
Figure 6. 7: Security level lifecycle model: Develop and implement phases (IEC 62443 2-1, 2010). 65
Figure 6. 8: Security level lifecycle model: Maintain phase (IEC 62443 2-1, 2010). 70
Figure 6. 9: Presented governance during Cyber Physical System lifecycle. 71
Figure 6. 10: Scope of service provider capabilities. (IEC 62443 2-4, 2015). 72

Chapter 7

Figure 7. 1: Reflections originated from concepts cross analysis. 74
Figure 7. 2: Cybersecurity level over time (IEC 62443-1-1,2019). 77
Figure 7. 3: Integration resources to develop the CSMS (IEC 62443-1-1,2019). 77
Figure 7. 4: Conduit example (IEC 62443-1-1, 2009). 79
Figure 7. 5: High-level manufacturing example showing zones and conduits (IEC 62443-3-3, 2013). 79
Figure 7. 6: IACS Automation Solution Security Lifecycle (adopted from ISA, 2020). 80

Chapter 8

Figure 8. 1: Supporting Cybersecurity (Alvarez-Dionisi et al., 2019). 83
Figure 8. 2: IACS Automation Solution Security Lifecycle (adopted from ISA, 2020). 84

List of tables

Chapter 1

Table 1. 1: Thesis Objectives. 5

Chapter 3

Table 3. 1: The comparisons of the 5C architecture and the 8C architecture (Jiang, 2018). 15

Chapter 5

Table 5. 1: Overview of ISO standard and content (ISO, 2021). 48
Table 5. 2: IEC 62443 Standard publications and content (IEC, 2021). 51
Table 5. 3: Applicable NOG Guidelines and their content (Norsk Olje & Gas, 2021). 54
Table 5. 4: Example of standard application in system component acquisition activity. 66

Chapter 6

Table 6. 1: The traditional Systems Development Lifecycle - SDLC (Elliot, 2004). 56
Table 6. 2: Example of activities for each stage (ISO/IEC/IEE 27748-1, 2018). 57
Table 6. 3: Example of standard application in asset Concept phase. 58
Table 6. 4: Example of standard application in asset Development phase. 60
Table 6. 5: Example of standard application in asset Production phase. 67
Table 6. 6: Example of standard application in asset Inspection and Test activity. 67
Table 6. 7: Example of standard application in asset Utilization phase. 68
Table 6. 8: Example of standard application in asset Support phase. 69
Table 6. 9: Example of standard application in asset Retirement phase. 71

Chapter 7

Table 7. 1: Gap analysis summary. 82

1 Introduction

The advent of the Industry 4.0 concept, announced by the German government during the Hannover Fair in 2011, introduced new industrial concepts assimilating the advances in fields such as information technology, services, and manufacturing comprehending increments in mechanization and automation, digitalization, networking, and miniaturization. Further, it anticipated the integration of dynamic value creation networks through the integration of physical and virtual systems across different branches, economic sectors, industries, and its types. Founded in eight main technological advances, namely, adaptative robotics, data analytics and artificial intelligence, simulation, embedded systems, communication and networking, cloud systems, additive manufacturing, and virtualization technologies (*Salkin et al., 2018*) it assumed, in the german case, the proposition to ensure an industry fit for future manufacturing, primarily securing and continuously developing the leading position in industrial manufacturing, promoting an digital structural change and a framework to achieve it (*Klitou et al., 2017*).

Application of the concept to Cyber Physical Systems, term introduced in the United States in 2006 and prompted by the increase in technical systems interacting between physical world and computing systems (*Törngrenet al., 2017*), has potentiated todays industries, enabling new domains of application, and refining existing, in both, adding new opportunities and challenges. Thus, the exploitation of this potential is broadly researched, with a transformation trend translating into new generations of Cyber Physical Systems which potentiate economic values across all chains, create new market niches, and represent a sustained and seamless change of the paradigm.

The nature of these new generations of Cyber Physical Systems, denoted by a continuous increase of interchanged data between unbounded participating elements poses new classes of Cyber Security threats, underperformances, and position losses. Characterized from micro to macro, and undetected in many instances, these demand a nurture of the same substance of development for countermeasures as for the one deployed in their targets and where the correct praxis is paramount.

In Norway, the research project CPS Plant, sponsored by a consortium of three norwegian industrial partners, Norsk Hydro, Benteler Automotive, Hycast and the academic partners SINTEF Digital and NTNU (Trondheim and Gjøvik) intends to develop and implement Cyber-Physical Systems technologies and methods integrating the virtual and physical worlds enabling improved production performance both in the manufacturing and production industries aiming to apply these innovations towards a CPS framework supporting the Norwegian ambition of integrating the concept of Industry 4.0 on the national industry (*Rødseth et al., 2020*).

1.1 Background

Digitalization is becoming the basis of social and economic developments, people, devices, and machines are more and more often networked and emergent technologies are quickly integrated. Cyber security represents skills, techniques, processes, and run-throughs built for ensuring the network protection, computes and programs against malware, attacks, damage, and unauthorized accesses. Such developments occur naturally in the Cyber Physical Systems extensive domains, examples reach from, for example, smart grids using duplex communications through Information Technology to distribute electric power from renewable energy sources into the power grids supporting sustainable values, have in some degree added additional types of vulnerabilities, essentially due to the nature of the communication technology (*Prasad et al., 2020*).

In the advanced digital manufacturing domain, *Wegner et al. (2017)* posts that the security requirements for Cyber Physical Systems are divergent from the traditional IT systems, where layered defense mechanisms around core components in detriment of peripheral components is enhanced while the former requisites a balanced approach, seeking to protect both the core and peripheral elements.

Within cloud systems , *Zhang et al. (2017)*, describes Decentralized Cyber Physical Systems, through a cloud abstraction conceptualizing a model for smart factories, and where a type of agent is introduced to connect devices and people, the agent function is primarily to connect elements withing the factory to the cloud eliminating the problem of the Information Island, which is no more than the information resources breakdown in blocks and isolated through the organizations divisions and subdivisions. Clearly the concept yields the advantages of the integration of new technological advances, and again in this case, the centralization on a cloud abstraction, requires prominence of the Cyber Security performances since these are directly associated with organizational economic metrics.

Infrastructural Cyber Physical Systems, which provide critical services such as power and water, have in some cases, added the cyber component for convenience on top of the Industrial Control System, which in its turn emphases naturally on the physical aspects of the system, allowing access and control of equipment, *Fink et al. (2018)* observed that in some instances the connection points between Industrial Control System components and external networks are undocumented and not understood as these remote accesses have evolved during long periods of time.

The development of Complex Cyber Security Systems comprised of different stages, namely, requirement collection, architecture design, implementation, test, deployment, and operation, represent a multidisciplinary exchange of technical and sensitive data between stakeholders, to improve engineering efficiency and quality, data logistics solution seamless integrated in engineering workflows are utilized. This data logistics is an attractive target for cyber threats, especially considering that is deployed as a repository providing central access. In this type of project, distributed globally

throughout different expertise groups that the cyber threats are more prominent (*Biffl et al, 2019*).

The observations mentioned in this section correlate to an increasing trend in Cyber Physical System complexity, *Sonalker et al. (2017)* depict a relation between the trend and the threat capability, accounting not only for the mentioned technological developments in section 1, but as well with, the association to legacy codes and suboptimal software engineering practices.

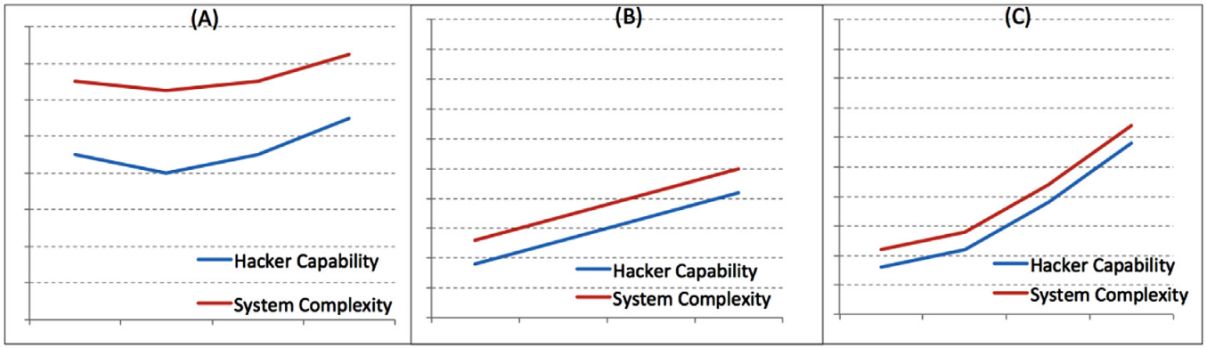


Figure 1. 1: Trend in capability versus system complexity as a defense mechanism (A) Past, (B) Present and (C) Future, (Sonalker, Griffor, 2017).

1.1.1.Motivation

Cyber Physical Systems are characterized by an increased tendency for data exchange supporting a competitive business advantage and absorption of technological developments, and simultaneously an inevitable demand for secure data exchange is required. The future trends, presented by *Sonalker et al. (2017)*, in figure 1.1 - (C), characterizes the context of interest, together with the intentions surrounding the soar patterns for complexity, namely the surveillance of technological emergences and its motivations, and reflections concerning the circumstances of the escalation of parallel jeopardizing capacities towards the Cyber Physical System and its tactics.
Securing the Cyber Physical System in this context is therefore compulsory and so are the incidences in applicability of informative and normative directives, contemplated with industry best practices.

1.2 Scope of Work

The selection of the topic is founded by the observation of an increased interest by organizations towards Cyber Security in an era which the digitalization paves the way to new technological migrations of Cyber Physical Systems and where instances of inadequate understandings are perceived, originated by the environment complexity.
Concretely, different methods and approaches are utilized for securing a Cyber Physical System with particular attributes during its lifecycle, and where substantial number of dependencies must be accounted, elevating the complexity of such deployments, requiring to the deployers an complete understanding of these domains.
The theme protrudes from the traditional technological fields driven by the technological advances conjugated with the organization's competitive advantages expectations, introducing new application areas which are bound to be intrinsic in the Industrial Asset Management domain.

The scope of the present thesis aims initially on the exploration of selected argumentative factors driving increased complexity patterns, more explicitly on the organizations need for digitalization, the influence of the characteristics of Cyber Physical Systems, namely architecture and application domain, in its security and, Cyber Security trends and technological developments providing an overview of the context.
It is pertinent, as a part of the research, to review the organization's approach towards Cyber Security, on cultural and strategical levels to grasp the harmonization degrees to the surrounding environments. It is of the outmost importance to capture the available and applicable Cyber Security governance traditionally applied towards Cyber Physical Systems, for this particular exercise the publications from the *International Organization for Standardization – ISO*, *International Electrotechnical Commission – IEC* and, *Norwegian Oil and Gas Association – NOG* are selected and further illustration of typical deployments during the lifecycle are realized, enabling the comprehension of the compliance degree on the characterized context.
It is intended with the elaborations previously described to capture gaps across the presented concepts and designate improvement areas which will culminate in three appointed recommendations, one in terms of the organizational approach towards Cyber Security and two in terms of the application of the IEC 62443 standard and consequently evaluate the hypothetic expected effects through the propositions conjectural execution.

1.2.1. Objectives

The translation of the scope of work defined in previous section to objectives of the present study are profiled in table 1.1.

Table 1. 1: Thesis Objectives.

Item	Focus Area	Specification
1	Cyber Physical Systems	a) Current technological developments, identification of dependencies which might impact cyber security performances. b) Evaluation of new designs and their impact on system resilience bound in system recovery after security breach.
2	Cyber Security	a) State of the art, feasibilities, and deployments in new Cyber Physical Systems. b) Current practices, normative and informative regulations. c) Identification of eventual constrains, inadequate approaches/implementations and gaps.
4	Organizations	a) Capability degree of cyber security cultural programs and strategical objectives on high paced technological environments.
3	Improvement areas	a) Presentation of recommendations based on the observed conclusions. b) Hypothetical expected effects from the recommendation's conjectural execution.

1.3 Methodology

The development of the present work derives primarily from the collection of information through a careful and selective literature review focusing on the reasons for current digitalization trends, originating factors for systems heterogeneity, Cyber Physical Systems reference architectures and application domains, Cyber Security threat trends and technological developments and, governance approach, from established from scientific articles and books, relevant standards, and opinion papers. Although a comprehensive quantity of relevant sources is available, in some instances they are not representative of the case of interest concept, but specific observations can be considered due to technological similarities.

Complementing the primary source, reflections obtained from professional practitioners from *Det Norske Veritas Germanischer Lloyd – DNV GL* are appraised and contemplated in the work, and insights from project executions, mainly from the Oil and Gas sector, are included contributing for an enlightenment of thematic.

Interpretative and appreciative processes are applied on the information sources, to obtain qualitative appreciations which are used in present executions.

The methodology is valued with the collaboration of the thesis supervisor, which conducted an assertive counselling, contributing for a concise compilation of information for the pursue of the desired outcomes.

1.4 Limitations

The development of the present work focuses on qualitative appreciations bounded by the presented body of concepts of interest which the results are not supported by any quantitative data analysis.
The selection of the concepts for scrutiny is formed from an interpretation of the most influencing and relevant factors towards the thematic.
The research does not present a formal introduction of any framework, method, approach, or guideline, it rather introduces a set of recommendations which can be considered by the readers discretion.

1.5 Thesis structure

The composition of the thesis include:

Chapter 1, Introduction: Familiarization with the theme, context and selected precursory concepts dealt on the work and development techniques.

Chapter 2, Digitalization: Motivation, background, and trends on current technological migrations of organizations.

Chapter 3, Cyber Physical Systems: Key attributes of Cyber Physical Systems and their contravention towards Cyber Security.

Chapter 4, Cyber security: Informative concepts about Cyber Security. Illustration of significant incidents and the latest trends concerning information security technological developments.

Chapter 5, Current industrial landscape review within the Cyber Security and Cyber Physical Systems domains: Cultural and strategical practices exercised by organizations. Overview on selected governance commonly applied by organizations.

Chapter 6, Cyber Security governance review in Cyber Physical Systems lifecycle: Illustration of typical governance utilization of selected standards and guidelines during the Cyber Physical System lifecycle with normative and informative application examples.

Chapter 7, Gap analysis: Selected findings, challenges and inadequate practices based in the evaluation of the presented concepts and focusing on the organizations, governance, and technology domains.

Chapter 8, Recommendations and expected effects: Selected improvement proposals based on the gap analysis outcomes. Interpretation of the hypothetical expected effects with the conjectural execution of the recommended improvement proposals.

Chapter 9: Discussions: Execution summary, learning outcomes, challenges and recommendations for future works.

Chapter 10: Conclusion: Final remarks and observations.

2 Digitalization

Digitalization constitutes a key factor, improving the competitiveness of the industry in a increasing globalized and uncertain market according with *Echeberria (2021)*, and further characterizes the transformation through the vertical networking of smart production systems and horizontal integration through new global value chain networks, through-engineering across value chains and impact of exponential technologies. The context faced by the global industries comprise in substantial economic challenges, originated by paced societal and technological development, decrease in the natural resources availability, increase in the energy prices, employee age and market globalization. The industry requires agility and responsive capabilities of managing the whole value-chain by way of virtual and physical structures cooperating and adapting along the whole lifecycle from innovation to production and distribution. The main driving technologies are internet based and internet of services, together with the new developments in computational power, leading to cloud computing and services, originating new service-based industrial systems where functionalities reside on-device and in-cloud. 10 strategic trends with potential for this evolution are presented by *Echeberria (2021)*, namely, the *Artificial Intelligence Foundation*, *Intelligent Apps and Analytics*, *Intelligent Things*, *Digital Twins*, *Conversational Platforms*, *Immersive Experience*, *Blockchain*, *Event Driven*, *Continuous Adaptive* Risk and Trust and finally *Cloud to the Edge*, detailing the last trend, it describes repositoriums, processing capabilities and connectivity links closer to the information node, diminishing the impact of latency challenges, bandwidth bottlenecks and providing greater embedded functionality at the edge, translating in increasing distributed models. It is worth noticing that this approach doesn`t undermine the cloud conception, the trend is merely to allocate the computational resources close to the information node, and the technology services and service-oriented models in the cloud.

The continuous adoption of new technological and emergent developments on an enterprise architecture is explored by *Bossert et al. (2021)*, and the *Perpetual Evolution* is presented. The concept introduces an approach towards the organizations agility of adopting technologies in a prompt manner, allowing the maintenance of its market capabilities against the competition or even to compete against “digital native” companies.

The concept captures the pretended transformation of the six core elements, represented in figure 2.1, comprehending the complex architecture of a large organization, *Business Operations*, *Business Capabilities*, *Business Applications*, *IT Integration Platform*, *Infrastructure Services*, *Information and Communication Technology*.

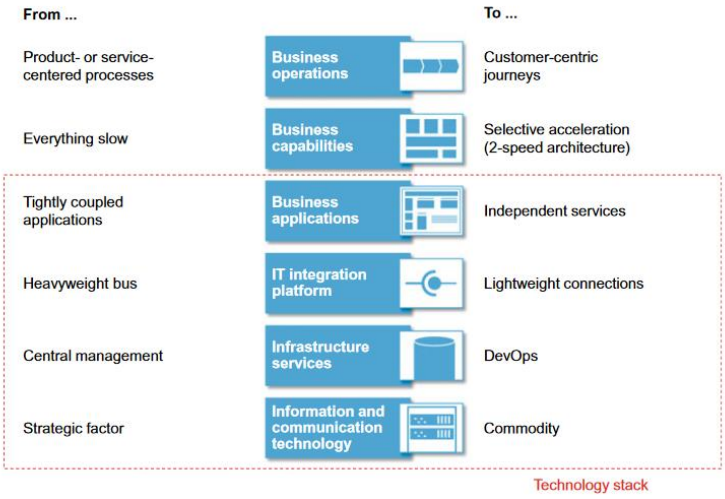


Figure 2. 1: Overview of the six core elements of enterprise architecture (Bossert et al., 2021).

Considering the evolution pretended with this concept, and taking the *Business Applications* layer as reference, *Bossert et al. (2021)*, propose the modifications of core applications such as ERP, CRM and HRM modules without modifying to complete versions of the applications, achieved by the platform and services in one release container, *Service-Oriented-Architecture - SOA* or microservices for the functional elements and true modularity of the underlying platform.

Figure 2. 2: Shifting applications to perpetual evolution architecture (Bossert et al., 2021).

The *Perpetual Evolution* characterizing the *Business Capabilities* layer hence demands more frequent connectivities, integration needs and consequently more security policies.

Both examples adhere to the assumption that digitalization on the present and future poses increasingly higher demands for connectivities and disperse residences of applications, reinforcing the idea that digitalization increases the architectural heterogeneity of organizations.

3 Cyber Physical Systems

The interpretation of a Cyber Physical System lays in the composition of three main elements, the physical, the cyber and the interconnectivity, it is in the latter that the vulnerabilities reside in the present context, *Pichler et al. (2020)*, further describe the juncture as being directly associated by the frequent composition of networks comprising different suppliers platform systems distinguished by own standards and protocols, and where one of the key factors is the own Cyber Physical System heterogeneity, dependent on its topology, vertical and horizontal scalabilities, interoperability, application area, and its seamless integration of data.

3.1 Heterogeneity

The heterogeneity is directly associated to the scalability characteristics of a Cyber Physical System, continuous introduction of emergent technologies and parallel management of associated risks is according with *Ali et al*. *(2018)*, a relatively new development in the critical and complex data protection area targeting the confidentiality, integrity, availability, authenticity, eavesdropping, comprised key attack, man-in-the-middle and, denial of service attack as core features of a Cyber Physical System security. This new area is further influenced by current practices of adopting existing solutions in other technological fields, which might not be the most appropriated implementation(s), since the vulnerability types may be different. It is worth highlighting that in general Cyber Physical Systems are not designed for security, but for its core functionality, and where the cyber security component is not of the aspects taken in consideration while developing such systems.

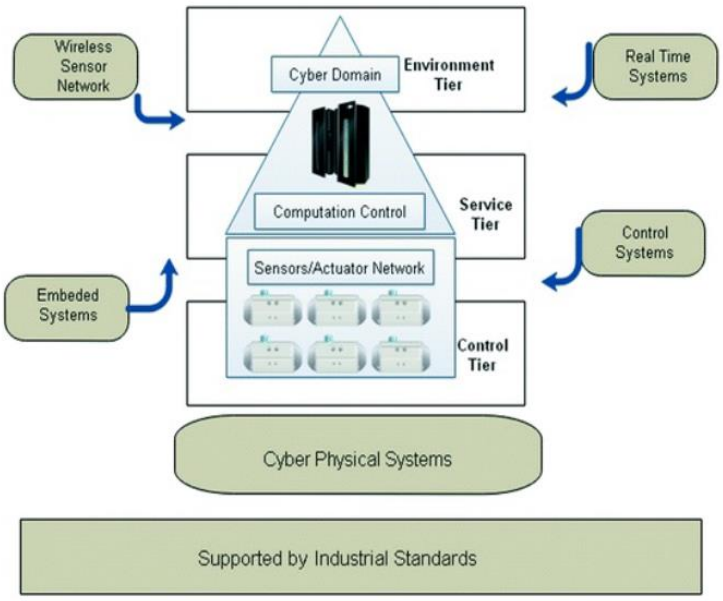


Figure 3. 1: Cyber Physical Systems conceptual layout (Ali, Balushi et al., 2018).

The heterogeneity of a Cyber Physical System is exacerbated by the introduction of emergent technologies, supporting a new and revolutionary novel of it. *Salkin et al. (2018),* narrate these as *Adaptative Robotics* as a development which enables artificial intelligence to compute with more autonomy fashioning smart manufacturing environments. *Embedded Systems* that provide two main functions, first the real time processing data from the physical infrastructure and feedback from the digital one, and secondly the intelligent data processing, decision making and computational sets supporting the physical infrastructure. *Additive Manufacturing* which enables the production of three-dimensional objects from digital models. *Cloud Technologies*, including cloud computing and cloud manufacturing, facilitate the coordination and linked production of available on demand manufacturing, and centralized computation and data treatment of dispersed data sources. *Virtualization Technologies* integrate computer supported reflections of real-world environments with additional and relevant information. *Simulation* as a tool supporting the visualization of outcomes due to parameter changes aiding the decision making, relevant especially in smart manufacturing environments for evaluations of autonomous planning rules. *Data Analytics and Artificial Intelligence* contribute on the facilitation of significant amounts of real-time data from different sources and its computation and analysis allowing corrective measures, new configurations, and optimal productions frequencies. *Communication and Networking* provide greater interaction between machines, systems, people, locations focusing on embedded intelligent sensors in real world environments and processes.

All these technologies provide new narratives on the constitution of a Cyber Physical System, since all contribute to a major extent on the opening of new connectivities, geographic dispersion of its elements, conceptualization of new hybrid systems, integration of diversified constituent system components indulging in a boundless to communication paths topology contrasting with the traditional Cyber Physical System concepts.

3.2 Conceptual architectures

3.2.1 ANSI/ISA - 95

Traditionally the information and communication structures of an Industrial Automation System are convergent to the ANSI/ISA-95 standard, through it 5 layers are defined from top to bottom, depicted in figure 3.2, and include the *Enterprise Resource Planning - ERP*, *Manufacturing Execution Systems - MES*, *Supervisory Control and Data Acquisition - SCADA*, *Programmable Logic Controller - PLC* and the field level consisting of actuators and sensors. Information can only flow through two adjacent layers in this setup, limiting the efficiency of data exchange when the demanded frequency is high (*Dai et al., 2019*).

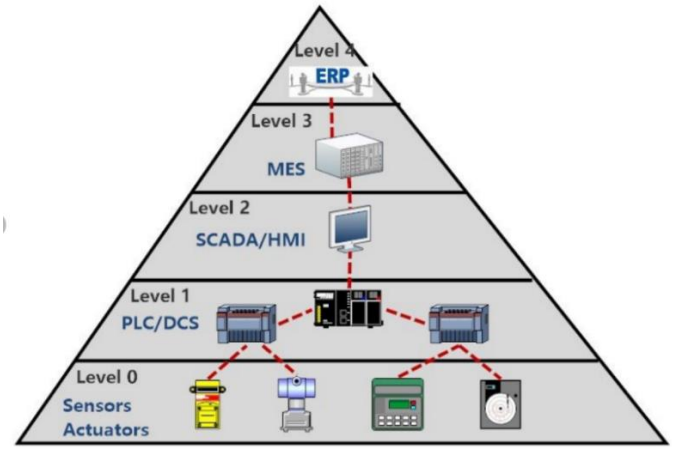


Figure 3. 2: ISA-95 Architecture for Industrial Automation Systems (Dai et al, 2019).

On the Industrial Cyber Physical Systems, *Dai et al. (2019)*, proposes that the efficiency bottleneck is minimized with the division of the 5 layers in two distinct groups. The ERP and MES layers are aggregated and allocated to industrial clouds due to low real-time requirements and the remaining layers remain as industrial edges handling the real-time constrains, this service-oriented architecture serves the data exchange through flexible interfaces.

From figure 3.3 it is relevant to denote the increased connectivity when compared with the traditional ISA-95 architecture for Industrial Automation Systems.

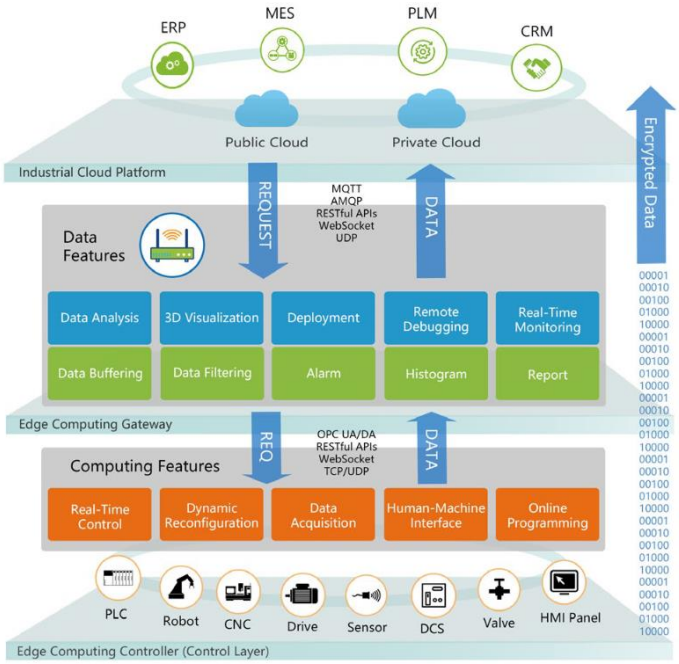


Figure 3. 3: Service-Oriented Architecture Enabled Industrial Cloud and Edge Computing Systems (Dai et al., 2019).

3.2.2 CPS 5C

Lee et al. (2015), realized the level of abstraction and specification of the two main components of a Cyber Physical System, namely the advanced connectivity ensuring the real-time data acquisition and the intelligent data management, analytics and computational capabilities constructing the cyber space, and for that a preposition of a *5 level Cyber Physical System structure - CPS 5C* was introduced.

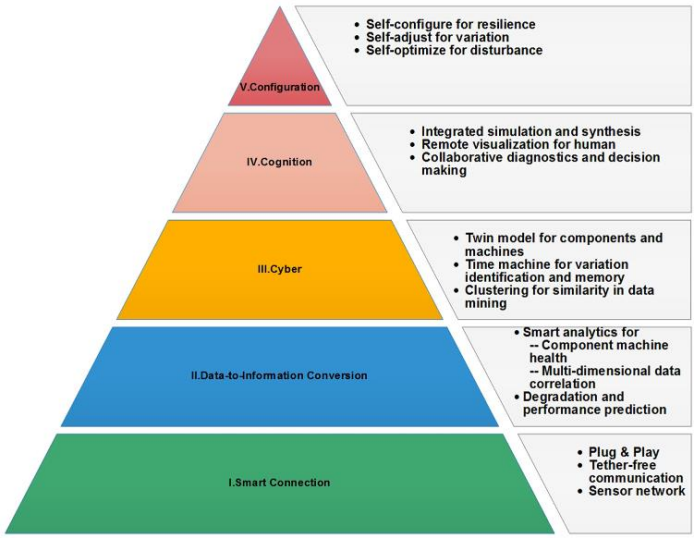


Figure 3. 4: The CPS 5C architecture (Lee et al., 2015).

Lee et al. (2015), further detail that the *Smart Connection* layer consists in the transduction of physical world values in information data, two aspects should be considered, the various data types allowing a seamless data management and sensorial characteristics, these aspects will also dictate the degree of scalability at this level. *Data-to-information Conversion*, provides information inference from data and typical applications in this layer are prognostics and health management, adding self-awareness to machines. The connectivity to the *Smart Connection* layer can be remote or local. *Cyber* layer represents an information hub where specific analytic applications determine machine fleet performances, but in addition due to the possibility of evaluating singular fleet element against its counterparts, providing self-comparison capabilities to machines. In the *Cognition* layer, complete fleet data structures are converged, enabling decisions on the task priorities, optimizing the processes. *The* Configuration layer applies decisions taken in the *Cognition* level back to the physical space, acting as a Resilience Control System.

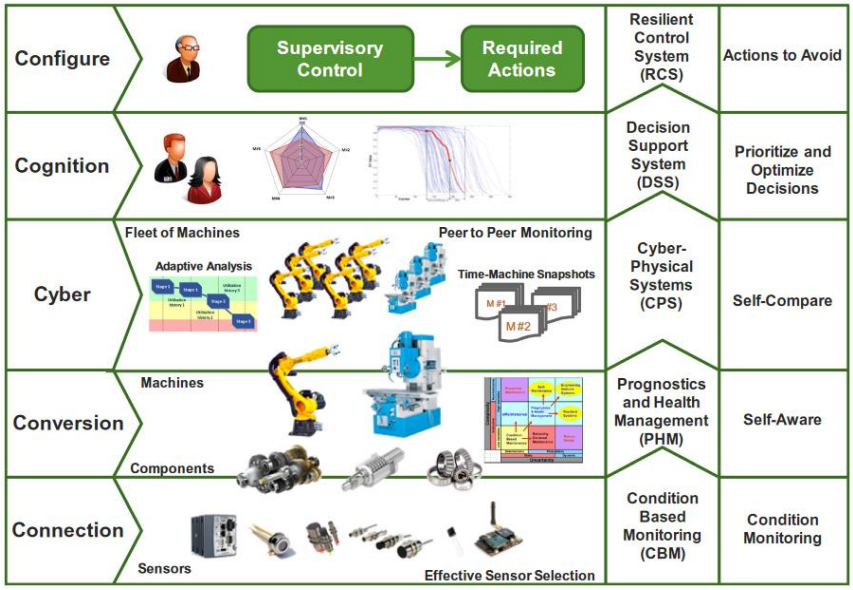


Figure 3. 5: Applications and techniques associated with each level of the 5C architecture (Lee et al., 2015).

3.2.3 CPS 8C

Jiang (2018) further improves the concepts proposed by *Lee et al. (2015)* and *ANSI*/ISA-95, by introducing 3C facets, *Coalition*, *Customer* and, *Content*, due to the observation that the previous concepts concentrate on the vertical integration.

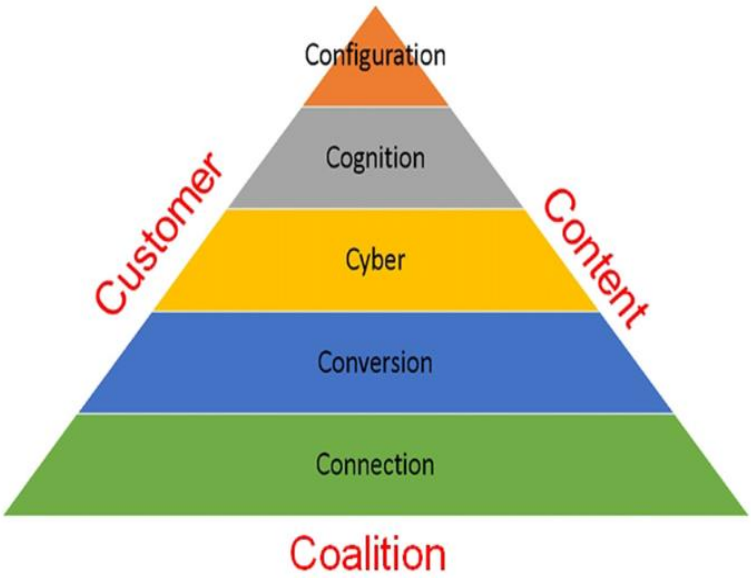


Figure 3. 6: The proposed CPS 8C architecture (Jiang, 2018).

Jiang (2018) elaborates the *Coalition* facet as the process focusing on the value chain and production chain integrations of different parties, the *Costumer* facet focusing on the integration of customers in the production process and finally the *Content* facet on the extraction and storage of design, manufacturing, product traceability contents.

The CPS 8C architectural concept introduces additional interfaces, such as the interactions with customers, storage of data though system owner or third parties and, information share upon the value chain joint ventures from distinct parties which culminate in a higher connectivity degree for a particular Cyber Physical System.

3.2.4 Summary

The three architectural concepts were presented in chapter 3, and in all the cases it is notorious a convergence to a soaring demand in systems connectivity to applications and entities residing in gross extent in cyber areas.

The improvements made in both the ISA-95 through *Dai et al. (2019)* with the allocation of industrial clouds, and *Jiang (2018)* with the CPS 8C architectures come to encounter the exigency of current digitalization and integration of emergent technological developments brought by the Industry 4.0.

In the *Jiang (2018)* preposition, the table 3.1 details the improvement brought by his concept, and it illustrates the need of joint ventures to acquire/maintain competitive advantages of a Cyber Physical System.

Table 3. 1: The comparisons of the 5C architecture and the 8C architecture (Jiang, 2018).

Architectures	Comparisons			
	Levels and facets	Vertical vs horizontal integration	Production type	Product whole lifecycle service
5C	5C levels: Connection Conversion Cyber Cognition Configuration	Focus more on vertical integration and less on horizontal integration	Mass production	Not emphasized
8C	5C levels: Connection Conversion Cyber Cognition Configuration 3C facets: Coalition Costumer Content	Focus on both vertical and horizontal integration	Mass production and mass customization	Emphasized

3.3 Application domains

3.3.1 Health

Increasingly used in health organizations, Medical Cyber Physical Systems provide high-quality continuous care for patients in complex clinical scenarios. For these systems it is indispensable the quality assurance in system software, interoperability, context aware decision support, autonomy, security and privacy, and certification (*Lee et al., 2017*).

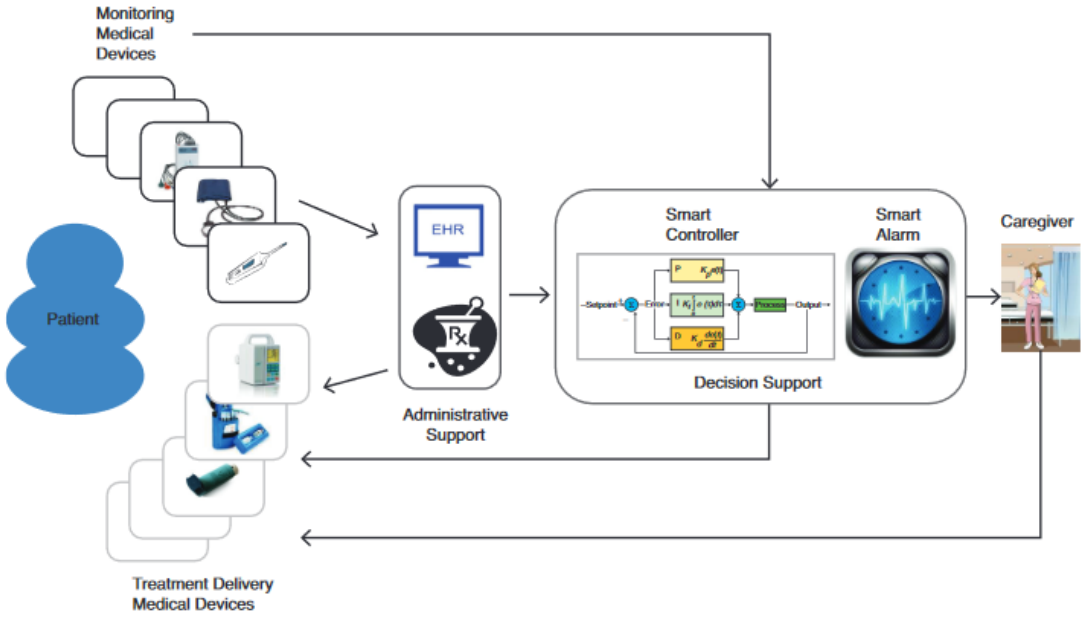


Figure 3. 7: A conceptual overview of medical cyber-physical systems (Lee et al., 2017).

Increased connectivity is inherent in these systems, due to the introduction of new devices, interfaces, accesses, and repositories where data confidentiality, authenticity and reliability are crucial.

3.3.2 Energy

Within the energy sector, *Ilic (2017)* refers to the *Dynamic Monitoring and Decision Systems – DyMonDS* as the foundation of the Cyber Physical System development, considering the necessity that operators and planners must make decisions based on information exchange with system users.

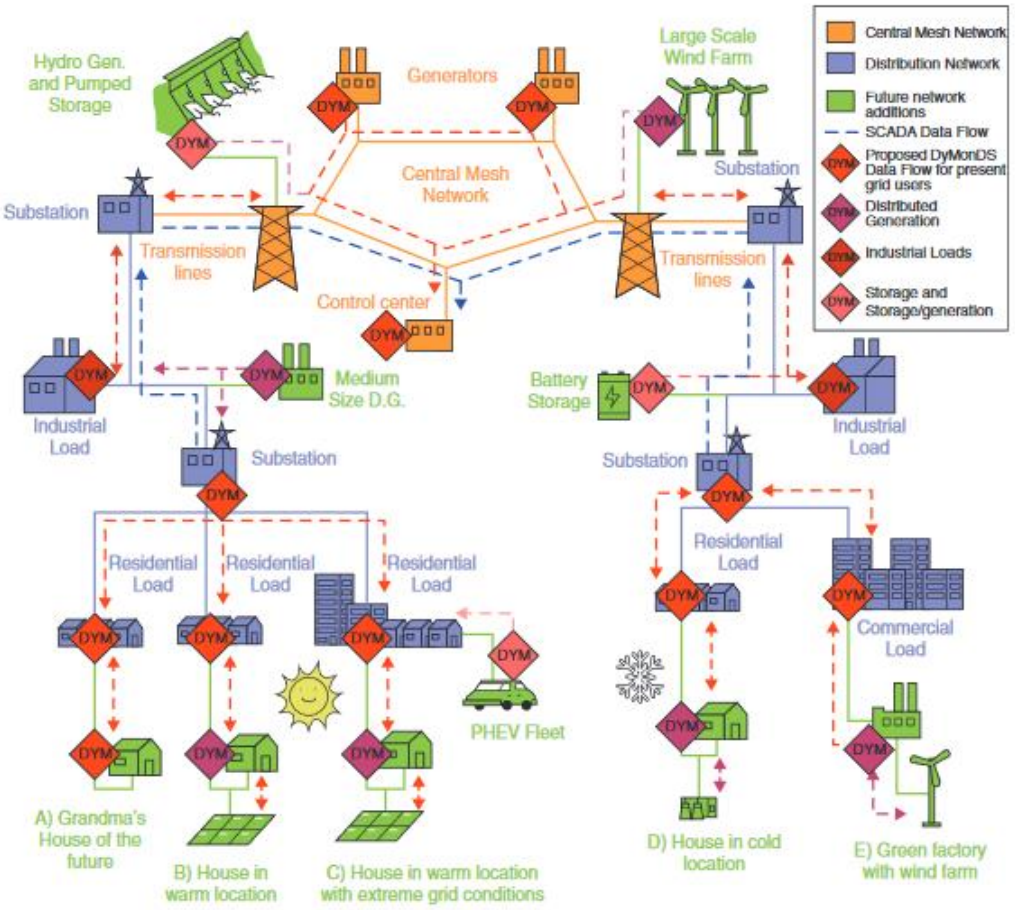


Figure 3. 8: CPS electric energy system with its embedded DyMonDS (Ilic, 2017).

In such Cyber Physical System, characterized by geographical dispersion across borders and legislative domains, the infrastructure is deficient in coordination and standardization of protocols, further aggravated by required expansion provisions typical in such systems.

3.3.3 Transportation

Transportation Cyber Physical Systems provide monitoring, control, and coordination for the major kinds of transportation, and are constituted by applications, cyberspace and physical space relaying on an infrastructure based in video surveillance, microwave detectors, radar detectors and magnetic detectors deployed in the immobile components and further aided by the mobile component through an array of sensors *(Han et al., 2017).*

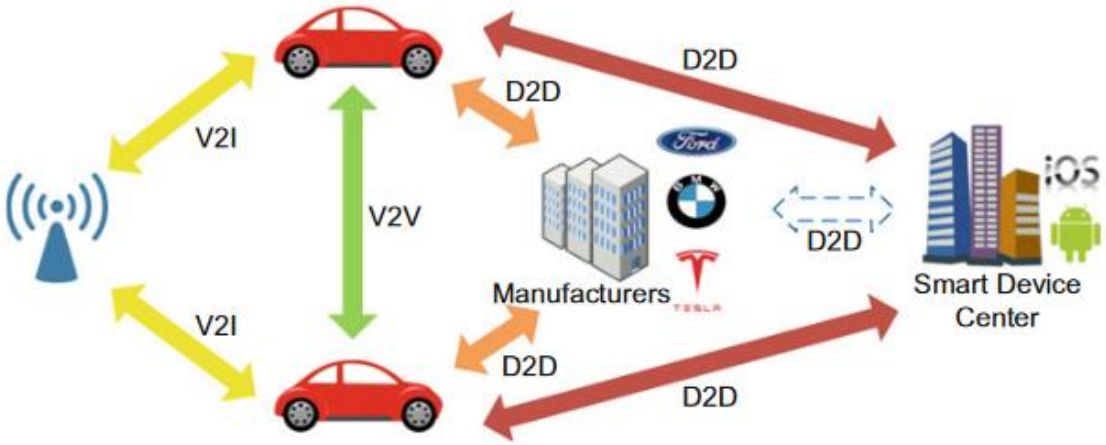


Figure 3. 9: Three TCPS communications: V2V, V2I, and D2D (Han et al., 2017).

Figure 3.9 represents three common communications in the highway transportation case, further described by *Han et al. (2017)*, the *Vehicle to Infrastructure – V2I* provides a short distance communication from the infrastructure, captured by infrared cameras or video surveillance to provide the vehicle information about weather, traffic conditions, work zones, potholes, etc. *Vehicle-to-Vehicle – V2V* allows nearby communication of position data between vehicles, and *Device-to-Device – D2D* that despite is emergence, provide vehicle health status back to the manufacturer through a direct connection.

The typical layers for a Transportation Cyber Physical System are detailed by *Wu et al. (2017)*, namely the perceptual composing of an extensive and undetermined number of sensor nodes and sink nodes, the communication layer composed of communication base stations and network nodes, the computing layer that due to the high capacity and computational demands cannot rely in traditional centralized architectures, being the cloud computing, network storage, distributed computing and virtualization the primary choices. The control layer augments the control capacities of physical transportation and the service layer providing real time data to the user terminal.

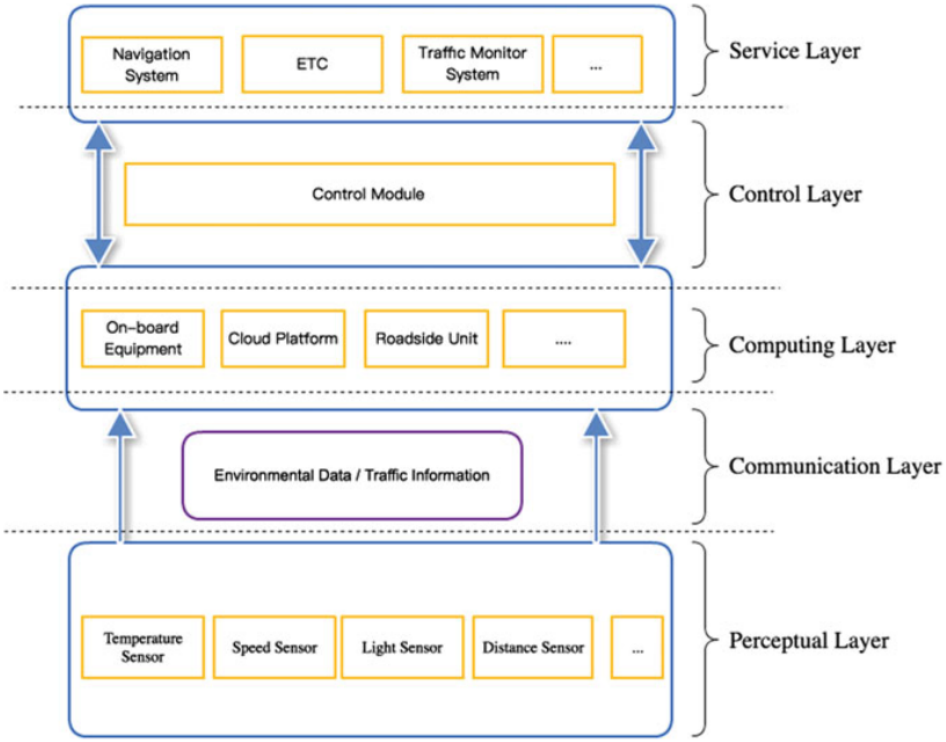


Figure 3. 10: Function layers of transportation cyber-physical systems (Wu et al., 2017).

Wu et al (2017) appoints the dynamic topological structures, large scale networks and non-uniform distribution of nodes as the main challenges for this particular Cyber Physical System and drastically different of other types of systems.

These asymmetries in conjunction with the indeterministic sensor nodes and short connection cycles comprehend security pitfalls.

3.3.4 Production systems

Current migration of *Cyber Physical Production Systems – CPPS* from technologies supporting mass production to production of customized batches with low manufacturing lead times demand a centralization in *Internet of Things – IoT*, big data and *Artificial Intelligence -AI* technologies, in addition to the innovating supporting technologies such as *Enterprise Resource Planning – ERP*, *Manufacturing Execution Systems – MES*, and programmable logic controller automated factories which are deemed as not sufficient for the current demands. *Lee (2018)* explores the migratory need, through the evaluation of a particular industrial case for the quality prediction and manufacturing control of metal casting exemplifying with the architecture framework of figure 3.11.

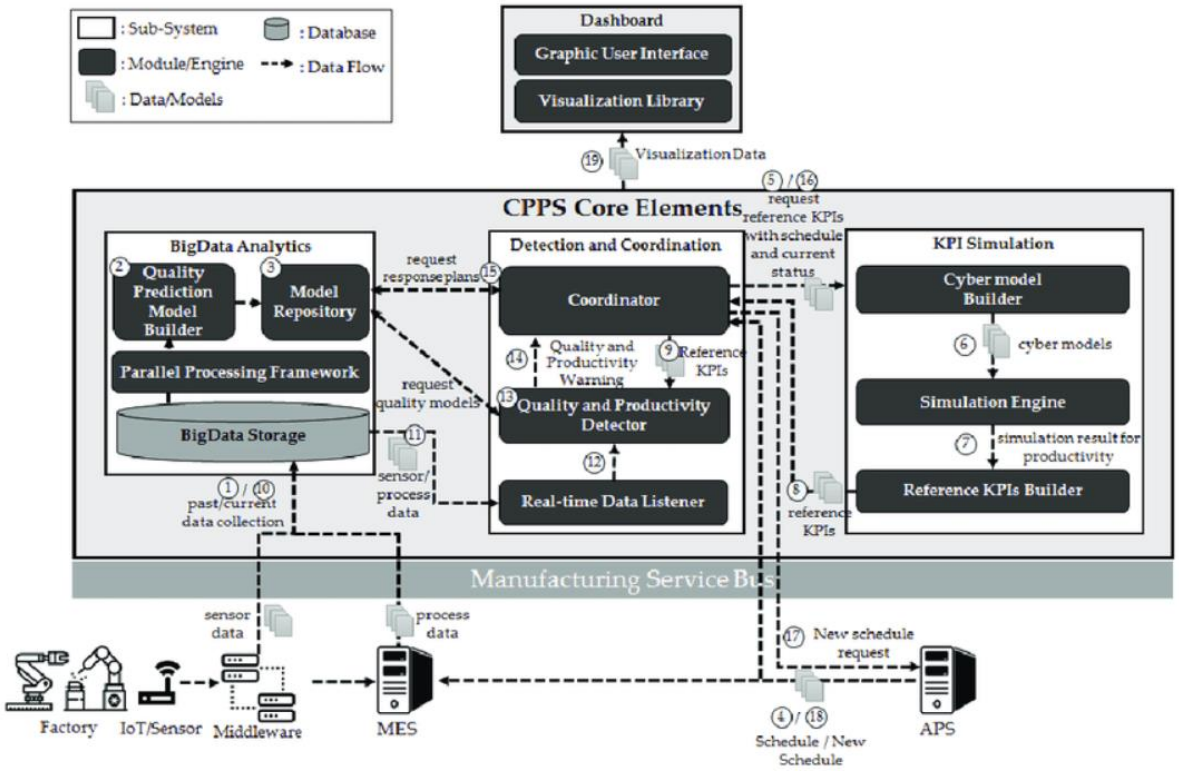


Figure 3. 11: Cyber-physical production system (CPPS) architecture framework (Lee, 2018).

The data flows are denoted with circled numbers in a chronological order fashion. The core sub-systems, big data analytics, detection, and coordination and KPI simulation systems envisage the key aspects additionally introduced in this case enabled by the IoT.

The introduction of new connectivities, residency of the core subsystems and exigency of real-time data poses new security challenges, in addition the transformation of a traditional manufacturing environment to an intelligent manufacturing floor and the compatibility and consistency aspects are in some cases overlooked, due to the fit to purpose approach mainly due to economic aspects.

3.3.5 Robotics

With the popularization of the cloud concept, providing a model for convenient, on-demand network access to a shared pool of computing resources, the manufacturing stakeholders adopted the concept as well in the manufacturing industry aiming to boost performances. The advantageous use of this concept in robotics is narrated by *Wang (2018)*, with the so-called Cloud Robotics, more precisely with the *Interoperable Cloud Manufacturing System – ICMS*, conceptualized through the figure 3.12.

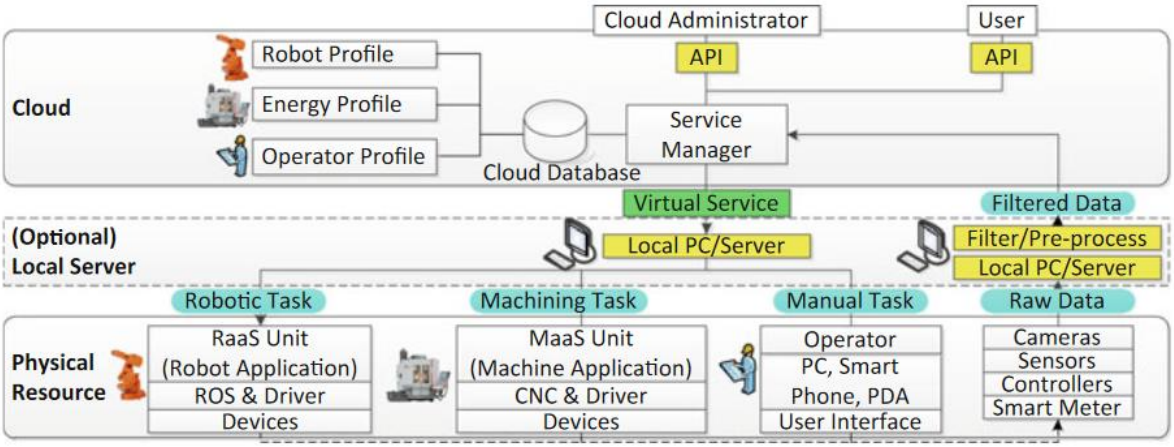


Figure 3. 12: ICMS system architecture (Wang, 2018).

Wang (2018) further describes the concept, with the cloud layer working as service coordinator and supervisor of the whole production system with the physical layer control units of production devices, example *Robot-as-a-Service – RaaS* and *Machine-as-a-Service – MaaS*, obtaining manufacturing tasks from the cloud.

It is worth noticing that the Cloud Robotics surge as a natural development due to network congestions of real time data transfer, figure 3.13 extracts these developments from conventional and web-based to cloud-based robotic cells and it is noticeable the relocation of the Robot Operation System from the cloud to the local environment, avoiding synchronization and stability risks. In addition, this approach enables a better secured system.

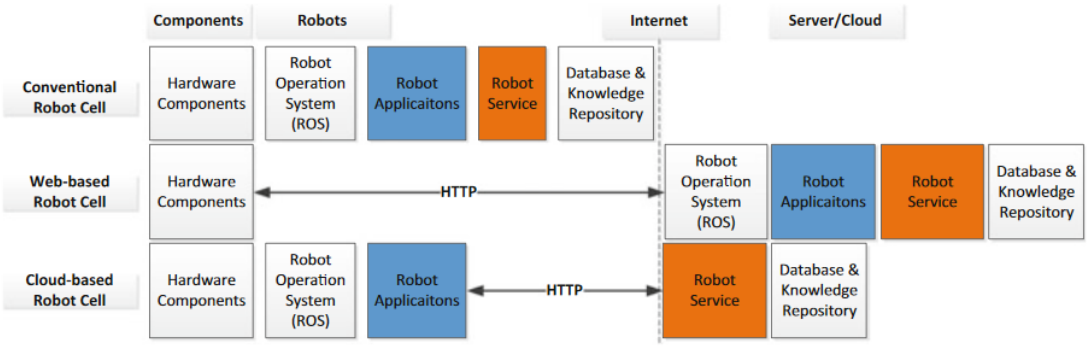


Figure 3. 13: Comparison of conventional, web-based and cloud-based robotic cells (Wang, 2018).

The concept here presented correlates in some degree with the concept presented in section 3.3.4, with the common denominator being the allocation of conventional subsystems to the cloud where implicitly the same risks and challenges are applicable.

3.3.6 Summary

Five application domains were presented, and their relationship with the integration of emergent technological developments and consequent challenges. It is notorious that these developments demand new interfaces and connectivities, with sectional systems residing in cyber spaces or in a conventional fashion but dispersed geographically. Integrating these require a top-down approach in terms of security analysis, interface compatibility, and real time performances which in many instances an ad hoc process is made, proportional to the integration of new system components in the Cyber Physical System opening new criticality levels in terms of system security and its performance.

4 Cyber security

On the 24th Annual Global CEO Survey conducted by *PwC (2021)*, cyber threats are the main concerns of CEO`s on the north America and western Europe regions, which coincides with the rapid acceleration of organizations digital transformation during the present pandemic.

These concerns are as well highlighted in the 2020 Cyber Threatscape Report produced by *Accenture CTI (2020)*, further detailing that the pandemic has opened the door to opportunistic threats, creating social engineering opportunities such as new phishing campaigns as well adding unprecedented pressure on organizations as they struggle with business continuity, travel restrictions and remote working. Further, as data continues to have high intrinsic value, sought after commodity, the strategy should encompass through an adaptative security, comprised by four elements, a secure mindset, secure network access, secure work environment and secure collaboration.

The main cyberthreats in 2020, were in accordance with the report, Cyber Threats 2020: A Year in Retrospect, produced by PwC (2021), composed by a clear shift towards the ransomware, independent of type of industry or location. The shift of tactics resulted in mass data exfiltration performed prior encryption of victim's systems, resulting in a prominence of data leakage to the public domain and adding pressure to meet the ransom demands. Figure 4.1 represents the ransomware leakages evolution throughout the year of 2020 and which the PwC`s Incident Response Team have responded.

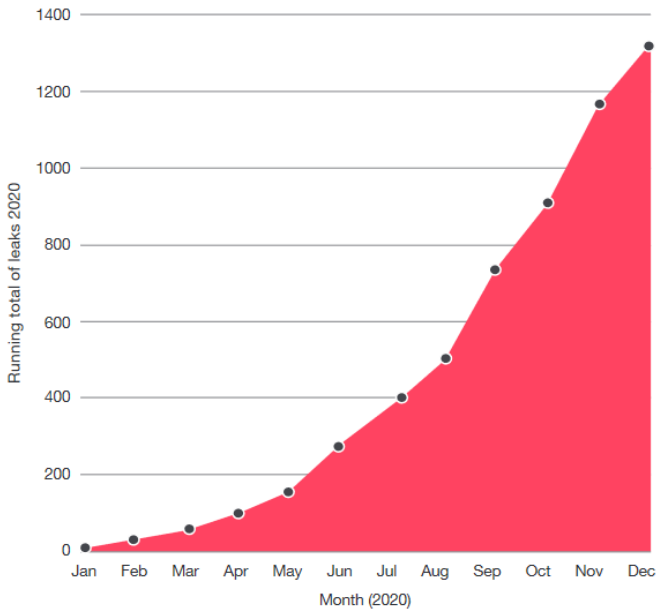


Figure 4. 1: Running total of ransomware leak site publications in 2020 (PwC, 2021).

4.1 Concepts

4.1.1 Security and privacy

Security and privacy are defined in two dissimilar contexts, the information and physical. *Fink et al. (2018)*, characterize by core principles.

Information security and privacy:

- *Confidentiality*: Computer related assets only accessible by authorized parties.
- *Integrity*: Modification of assets can only be performed by authorized parties or in authorized ways.
- *Availability*: Assets are made accessible to authorized parties at determined times.
- *Authentication*: Identification verification, mainly as a requisite for access.
- *Non-repudiation*: Preservation against an individual false denial of performing an action.

Physical security and privacy:

- *Deterrence:* Prevents actions through a credible threat of unacceptable counteraction.
- *Detection*: Positive assessment of the determined object caused the alarm, and the annunciation of it.
- *Delay*: Physical features, technical devices, security measures or protective forces that obstruct one adversary of accessing the protected asset or completing a hostile action.
- *Response*: Physical replication with the necessary force to stop de advancement of the adversary.
- *Neutralize*: Render enemy entities or material incapable of interfering with a particular operation.

The core principles in the two domains overlap but are not the same, figure 4.2 illustrates the translation of information principles to the physical domain and which controls they would enable.

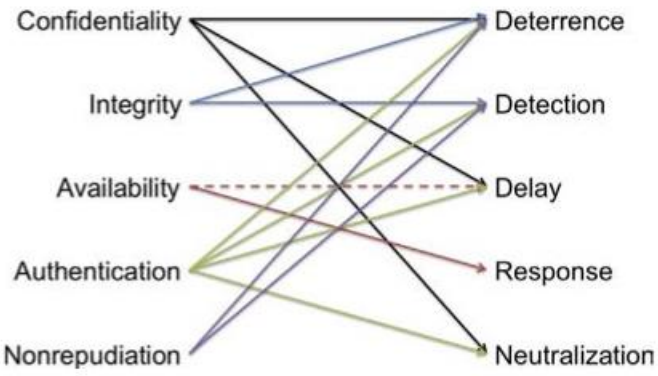


Figure 4. 2: Mapping of cyber security principles to the physical security controls they enable (Fink et al., 2018).

Some of the security mechanisms which would enable the principles in both contexts are illustrated in figure 4.3.

Security principles: / Implementation examples:	Confidentiality	Integrity	Availability	Authenticity	Nonrepudiation	Deterrence	Detection	Delay	Response	Neutralization
Barriers	+	+	-			++		+		+
Logs	-			+	++	+	+			
Alarms						+	++		+	
Encryption	++	+	-	+	+	+		+		+
Signatures		++		+	++		+			
Redundancy	-		++					-		
Identifiers	+			++	+	+	+	+		

Figure 4. 3: Mapping example security mechanisms (rows) to information security principles and physical security controls they enable (columns) (Fink et al., 2018).

The matrix is populated through "+" indicating that the mechanism enables the principle or control, "++" the mechanism is a primary mean of obtaining the principle or control and "-" indicating that the mechanism is in fact harmful for the principle or control.

4.1.2 Attacks and threats

According with ISO/IEC 27001:2013, threats can be deliberated, accidental or even environmental, *Maleh et al. (2019)* depict through figure 4.4 a tree diagram and its different branches containing type of attacks and threats to Cyber Physical Systems.

Figure 4. 4: Tree diagram of attacks and threats on Cyber Physical Systems Technologies (Maleh et al., 2019).

The tree branches illustrate attacks on sensor devices, actuators, computing components, communications and on feedbacks. Where the main attack types which have significant impact in a Cyber Physical System are *Eavesdropping* as an attack which the adversary intercepts information of the system, it is seen as a passive attack since there is no interference with the operation only observation. Cyber Physical Systems are vulnerable to this type of attack through traffic analysis through the monitoring of fata transferred in the sensor networks. In this attack the user privacy is breached. *Comprised-key attack* where the attack is executed when the attacker obtains an encryption key leading to the access of secured communication without the knowledge of the sender and receiver nodes, additionally the attacker can modify data and compute additional keys enabling the access to other secured communications or resources. The *Denial-of-Service – DoS Attack*, where attack is characterized by the prevention of legitim traffic or request for networks being processed by the System. It consists on the transmittal of huge data volumes to the network occupying the system resources and consequently disrupting the normal operations

A variant of DoS attack is the *Permanent Denial-of-Service – PDoS* which *Ponnusamy et al. (2020)* describes as the hardware sabotage by the DoS, and commonly referred as *Phlashing*. It is conducted through the bricking of an IoT device or destruction of its firmware via remote or physical administration on the hardware interfaces. It differentiates from the *Distributed Denial-of-Service – DDoS* which floods the targeted system with information and connection requests until the it slows down or crash while the PDoS damages the device until is useless and requiring repair. One example of PDoS in Linux IoT based targets running *BusyBo*x tollkit is the *BrickerBot* malware, it uses the toolkit open *Telnet* ports and conducts attacks on these through known default credentials, and after gaining access it deploys a set of Linux commands design to corrupt storage, disrupt internet connectivities and delete all device files.

Ponnusamy et al. (2020) further describe the *Man-In-The-Middle – MITM* attack, consisting on the interception of a third party or an outside entity in a 2-way communication between the victims. Several types of MITM attacks are frequent, one is the e-mail hijacking, tactic used to target accounts of large organization. Other is the Wi-Fi *Eavesdropping* where the attacker used public networks enabling the connection to a target device through a plausible and artificial network name. Other attack method is using the *Secure Socket Layer - SSL* or *Transport Layer Security – TLS* to create secure channels over an insecure network, it is conducted through the use of SSL over HTTP, or HTTPS were the hacker intercepts the traffic between the client and web server. Upon the discovery of the HTTPS URL, the SSL strip is replaced with an HTTP link and changes made are mapped and maintained. The attacking machine supplies certificates to the server and impersonates the client, the traffic is received back from the secure website and back to the client.

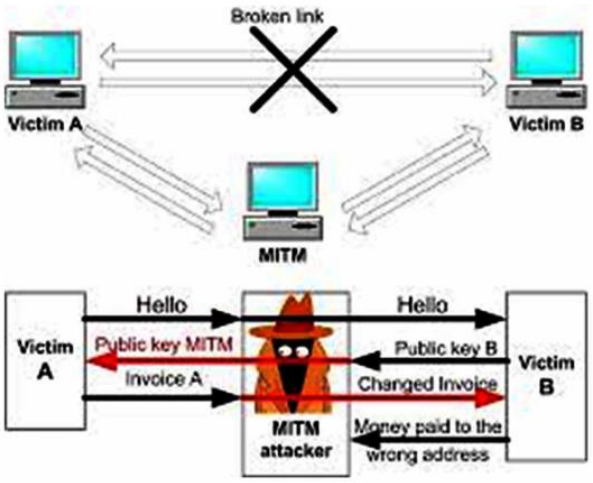


Figure 4. 5: Man-In-The-Middle - MITM Attack (Ponnusamy et al., 2020).

Stallings (2017) in his network security model complements the threats with viruses and worms as software attacks introduced by physical or virtual means, which are dealt by two main security mechanisms, the first designated by *gatekeeper* which comprehends password-based login procedures and screening logic designed to detect and reject these software payloads. The second line of defense would consist of internal controls to monitor activity and analyze stored information aiming on the detection of unwanted threads.

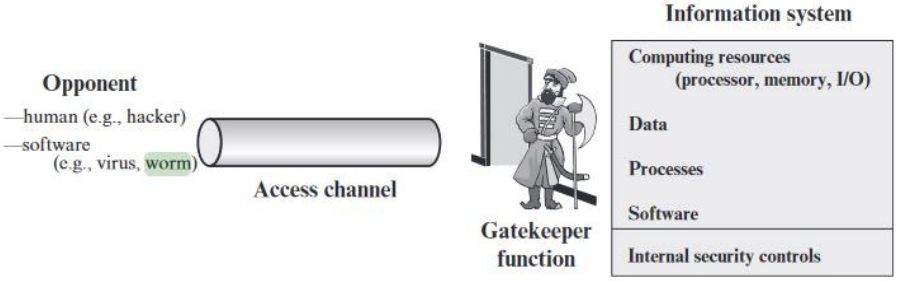


Figure 4. 6: Network Access Security Model (Stallings, 2017).

A Periodic Table of Cybersecurity Threats is elaborated by *Pogrebna et al. (2019)*, and illustrated through figure 4.7, comprehending the full spectrum of monomers, polymers and composite cyberthreats. It captures the escalation of the diversity, complexity and frequency of the threats projecting an increased demand of the organization's attention and demand for appropriate countermeasures.

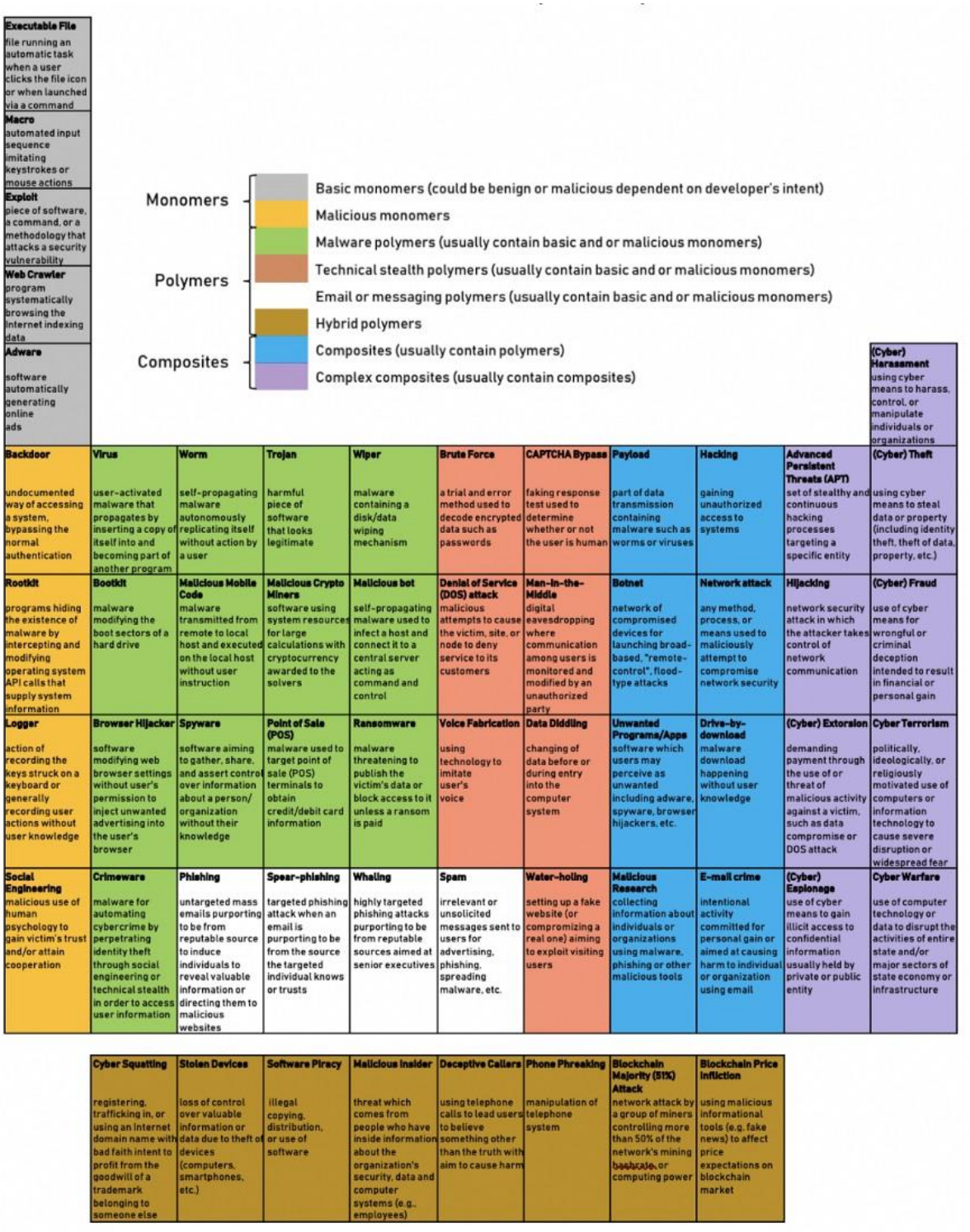


Figure 4. 7: Periodic Table of Cybersecurity Threats (Pogrebna et al., 2019).

4.1.3 Cyber Kill Chain

The Cyber Kill Chain model developed by Lockheed Martin provide information regarding the intrusive actions that attackers generally follow, consisting of seven steps described by *Bahrami et al. (2019)*:

- *Reconnaissance*: Consists on the identification, selection and profiling of potential targets.
- *Weaponization*: Comprises on malware design, including *Remote Access Trojan – RAT* integrated with an exploit code, in a deliverable payload. Efforts are made to reduce the risk of detection and evaluation by security analysts or solutions.
- *Delivery*: Involves the attempts to transfer the payload to the target`s environment and, in some cases, through another third party in order to exploit a trusted relationship between the third party and the target.
- *Exploitation*: Upon successful delivery of the payload, leveraging various techniques to trigger the malicious code will commence.
- *Installation*: Attempt to install access points, such as backdoors or other payloads, to gain persistent access to the target`s system or network.
- *Command and Control – C2*: Establishment of communication with the compromised host(s) realizing data control actions.
- *Actions on Objectives – AOO*: Realization of objectives, such as, data destruction, ransomware, further malware spread, etc.

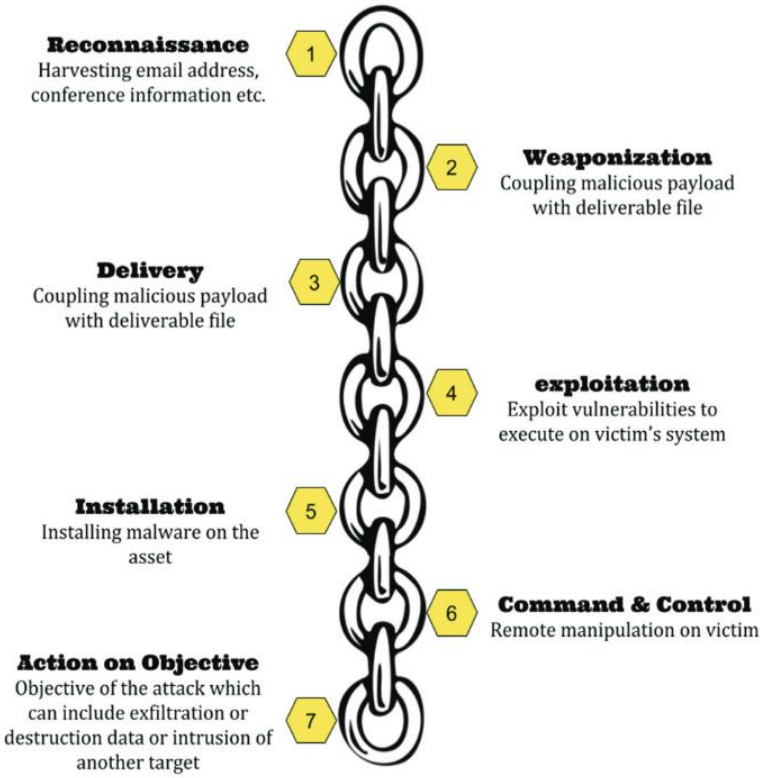


Figure 4. 8: Adapted Lockheed Martin Cyber Kill Chain steps (Bahrami et al., 2019)

A taxonomy mapping the CKC to *Advanced Persistent Threats - APT* features was produced by *Bahrami et al. (2019)*, contributing on key challenges that organizations have in protecting their assets against cyber threats, comprehended in between others by, real-time and predictive analysis, instant detection, and identification of potential attacks on target systems.

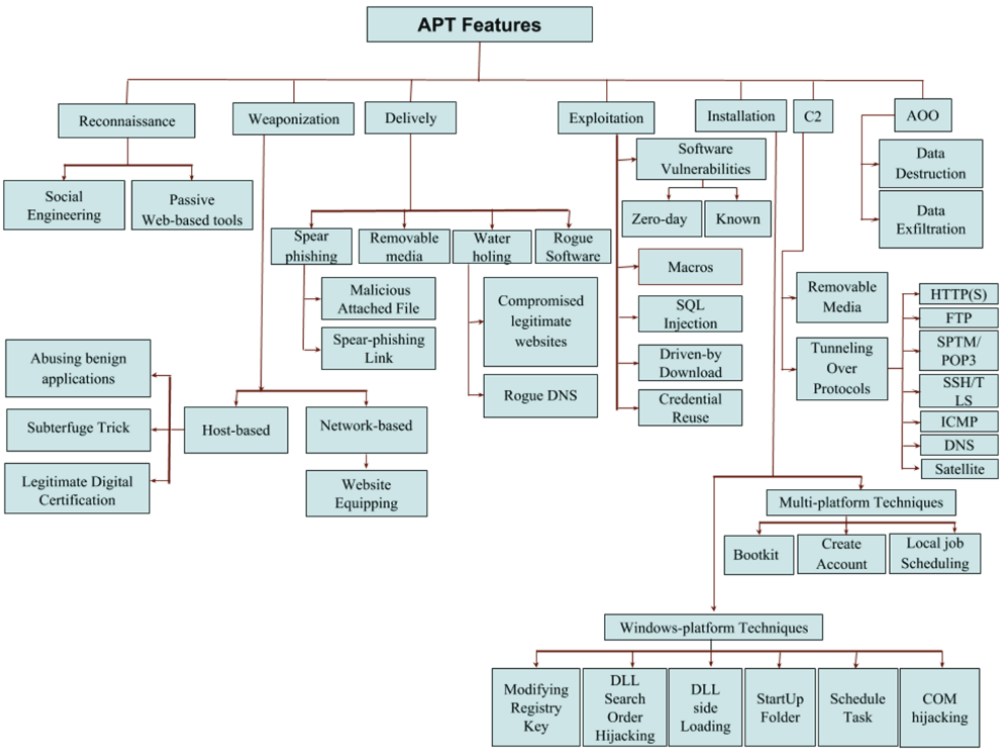


Figure 4. 9: CKC based taxonomy of APT features (Bahrami et al., 2019).

4.1.4 Threat agents and trends

Reflections surrounding the actors behind cyberthreats were compiled by *Sfakianis et al. (2019)*, producing a threat landscape of the year 2018.

Defenders perspective:

- Increased efforts to penetrate the infrastructure of threat agents, through intelligence, some actors created trustful relations to enter the hacker sphere and successful unveiling of state sponsored agents have been achieved,
- Identification of recursive behaviors and operation methods lead to recognition of type and origin of threat agents.
- Increased efforts to simulate threat agent tactics enhancing awareness and preparedness have been conducted by cyber security companies contributing towards a lower rate of success of the threat agent activities.
- Cyberthreats intelligence experts have underlined inefficiencies of defense strategies based in the CKC, with emphasis in activities triggered in later stages of the CKC, after the infiltration of the target is performed. The conclusion is

that the defense is often based in the last stages of the CKC while defenses in the earlier stages are neglected.

Threat agent perspective:

- Assumption that traditional state sponsored threat agents are repositioning themselves in changing the geopolitical space, new campaigns stemmed from known to new actors is occurring, with the change of tactics and targets, but still using similar tools, malicious sites and vulnerabilities.
- Vulnerabilities continue increasing, mainly sourced by vendor software patching.
- New methods for evading attribution and detection of attacks have emerged, file-less and memory resident threats as well the use of common attacks have been efficient in achieving objectives.
- Threat actors are making progress in using the supply chain to achieve they objectives.

As a complement to the mentioned trends, a correlation between the threat agent groups and the cyberthreats was produced for the year 2018.

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

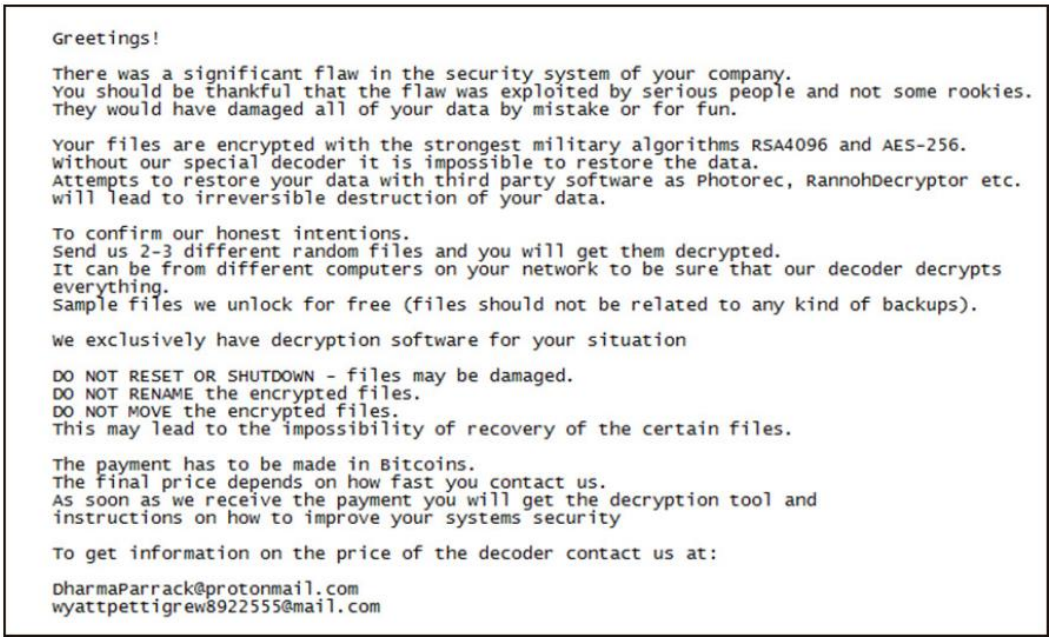
Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Figure 4. 10: Involvement of threat agents in the top cyberthreats (Sfakianis et al.,2019).

4.2 Incidences

4.2.1 LockerGoga

On the 19 of March 2019, Hydro was a target of an extensive cyber-attack. Production lines stopped in some of its 170 plants, some facilities switched from automated to manual operations. It affected 35000 employees across 40 countries and the financial impact approached the $71 million. The attack executed by the *LockerGoga* ransomware encrypted files on desktops, laptops, servers and posted a ransom note on the screens of the corrupted computers (*Briggs, 2019)*.



```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

Figure 4. 11: The LockerGoga ransom note (Panda Security, 2019).

Briggs, (2019), reports that a team of internal and external forensic investigators determined that in December 2018, the hackers had weaponized one e-mail attachment sent by a trusted costumer. A timeline is presented in figure 4.11.

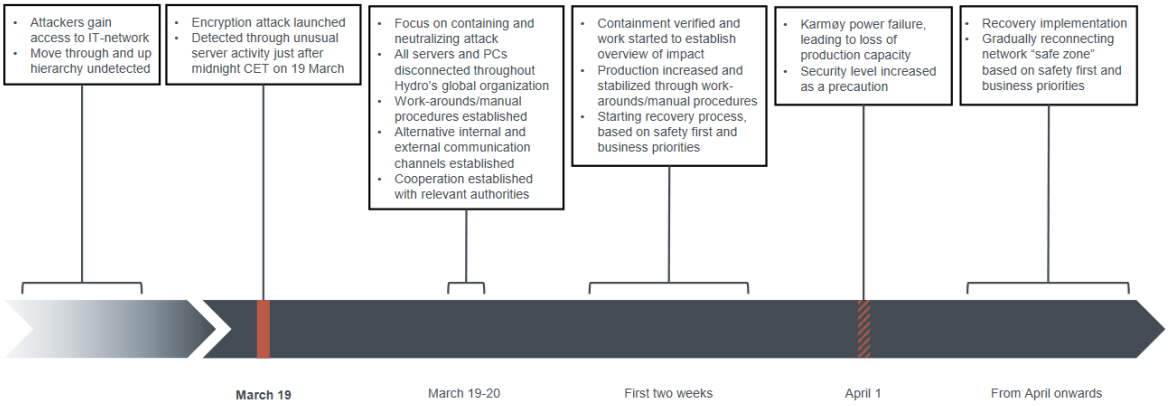


Figure 4. 12: Cyber attack on Hydro's worldwide organization High-level timeline of events (Hydro, 2019).

From the event description it is possible to identify, that the infection of the worm in the organizations IT systems occurred in December 2018, being the attack executed on March 2019, this shows that the attack was not instant, it was timely planned and the dormant time is crucial for the spreading of the malware throughout the infrastructure, further it was later identified that the one of the relevant aspects which undermined the security aspects was the use of a common *Windows Active Directory* for both corporate and plant networks managing the user access and common elements management.
In addition, the public announcement of the attack from Hydro side, have alerted other organizations for the type of attack, enabling a prompt response if necessary.

4.2.2 NotPetya

NotPetya has been the second information security concern in the world, *Fayi (2018),* further reflects that this ransomware not only encrypts files, but the system itself through the *Master File Table – MFT* after rebooting the infected system therefore the *Master Boot Record* becomes impracticable. It uses not only the *EternalBlue* vulnerability but others from Windows, such as *PsExec*, *Windows Management Instrumentation – WMI* and *EternalRomance* to propagate through the network.
The threat appeared as a ransomware but since the decryption was not possible it was considered as a *wiperware*.
The attack originated in Ukraine, through a distributed accounting software *MeDo*, which companies need to work with the government and was detected in other 64 countries.

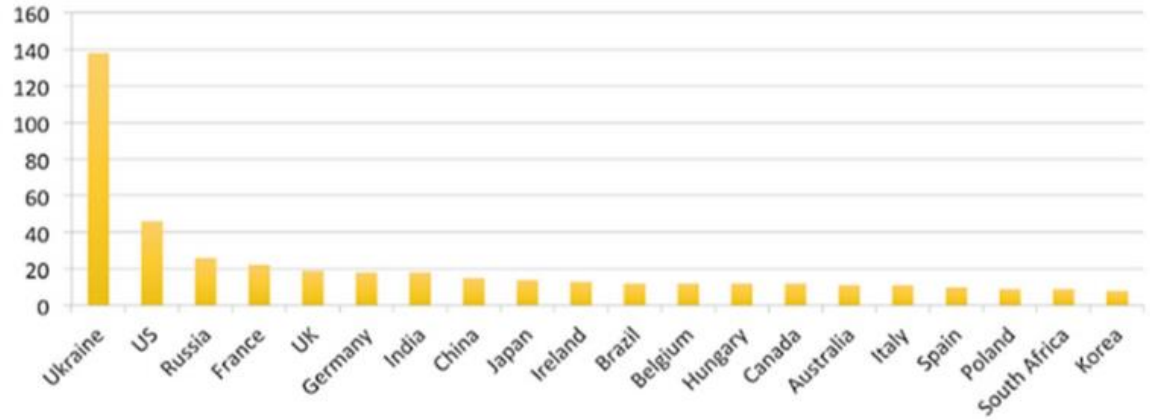


Figure 4. 13: Top 20 countries depend on number of infected organizations (Fayi, 2018).

Griffin et al. (2019) reported for Bloomberg that more than 30000 computers and 7500 servers were destroyed with the attack, long years investigation work was also lost at Merck & Co.`s, the pharmaceutical manufacturer. Production halted, and the forecasted demand of Gardasil 9 vaccine could not be met. Merck alone suffered losses of $1.3 billion.

4.2.3 Sunburst

The SolarWinds hacking campaign exposed fundamental cybersecurity vulnerabilities within the U.S. government agencies and the private sector, at least 100 private companies and 9 federal agencies had their data stolen *(Knake, 2021)*. The ongoing investigations will unveil the correct extension of the attack, but it is expected a much larger number of victims as this was one of the first successful supply chain attacks.

Nides (2021) details the sequence of the attack, the first step consisted on the deployment of a malware *Sunspot* in the SolarWinds Orion Platform during the software build process, watching for a new build to take place, upon build time the *Sunspot* would insert a backdoor, referred as *Sunburst* contained in a temporary source file used by the compiler, during the conclusion, Sunspot would remove the temporary source code file avoiding detection. Hence the codebase remained clear, while the compiled code signed with valid SolarWinds software certificate was shipped with the *Sunburst* backdoor.

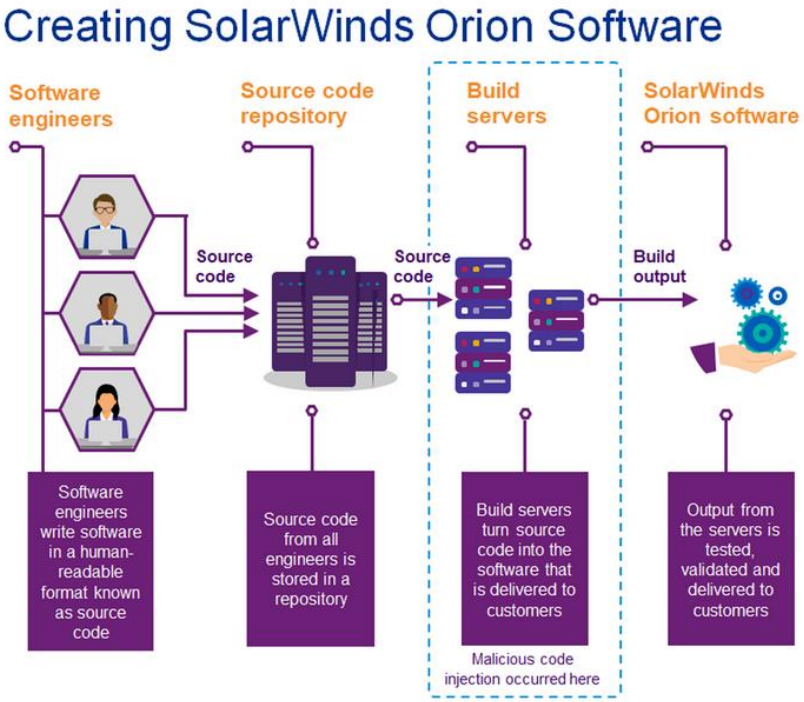


Figure 4. 14: Creating SolarWinds Orion Software (Nides, 2021).

Sunburst was designed to establish connection with the attackers, providing them with extensive capabilities, from creating and deleting files to execution and manipulation.

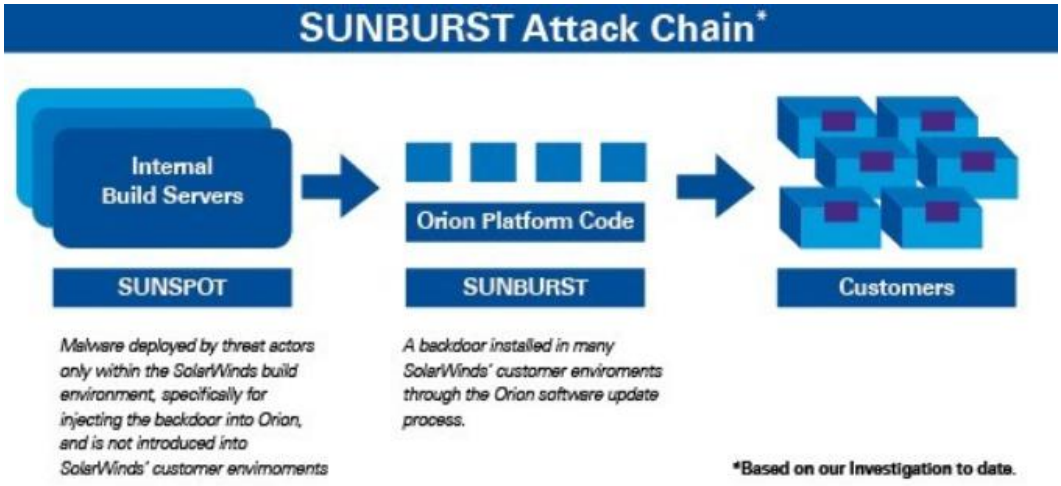


Figure 4. 15: Sunburst Attack Chain (Nides, 2021).

The method of deployment on the Sunspot on the SolarWinds internal servers is not yet disclosed, some sources suggest that it was an insider, others revealed weaknesses in the access credentials of one of the FTP servers.
SolarWinds is a leading technological company providing network management solutions, the conduction of the investigation has revealed some relaxation towards the cyber security aspects, namely employee awareness/commitment and overlooking regarding credential strengths practices.

4.2.4 Summary

The sophistication levels of cyber-attacks are continuously increasing, enhanced by illicit funding's and meticulously planned, and while some of the attacks subside in the obsolesce of the infrastructures, others prime on the inadequate cyber security strategies adopted by the organizations and mediocre implementation of cyber secure designs which further undermine protection capabilities against the current trends.
The examples presented, shown that the attack vectors are variated, originated in many cases in unknow sources, with variated end purposes. Additionally, information about vulnerabilities and attack methods are disseminated through the web, making it accessible to individuals or groups with unethical intentions. This ambiguous threat environment demands a clear, evolutionary, and continuous strategical, technological, and cultural process on cyber security fields from organizations enabling a reduction of prospects of successful attacks. The significance of these events urges new and additional focus areas from an Industrial Asset Management perspective.

4.3 Technological developments

4.3.1 Lightweight cryptography

Traditionally, cryptography intends to provide high level of service or objective security without considerations to the physical and virtual limitations of the systems. The origin of lightweight cryptography is the necessity of providing security services on constrained devices, which have limitations such as power source, connectivity, hardware, software, and processing potential, which are characteristic in the Cyber Physical Systems context. *Tawalbeh et al. (2018)* further describe that these trending algorithms when executed provide adequate security consuming less processing power and where the concept lays in two distinct contexts: hardware and software. In the hardware implementation two key parameters are determinant, the chip size and energy consumption while in the software context the code and RAM sizes are the key aspects and where both the two contexts can be concurrent. This entails a compromise between security, performance, and cost, which the development must be tailored for the pretended design.

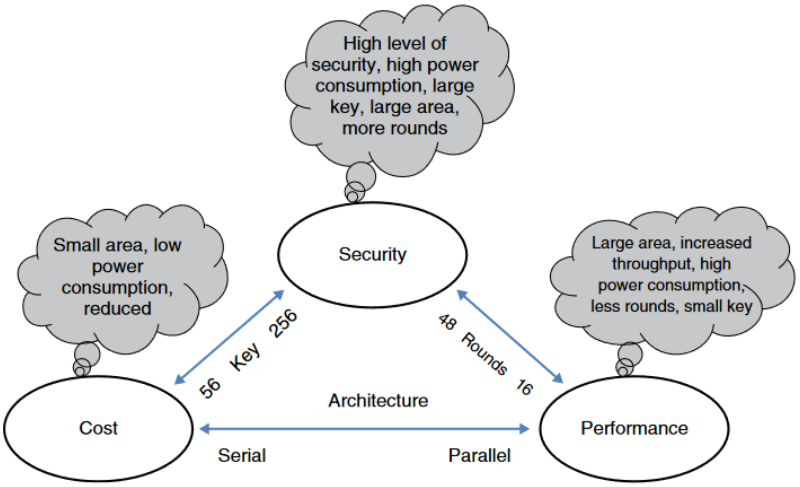


Figure 4. 16: Trade-offs between security, cost, and performance (Tawalbeh et al., 2018).

Tawalbeh et al. (2018) refers the four advantages of the lightweight cryptography, namely the *Gate Count*, which refers to the number of gates saved when compared to traditional implementation, *Power*, referring to the power consumption drawn the light algorithms, *Latency*, providing a quick throughput in applications where quick response time is required and *Memory*, being the advantage the RAM/ROM savings in this type of implementations. On the other side, the disadvantages are the significant amount of parameters that affect the power consumption which introduce uncertainties on modeling the performance scenarios, in addition to aspects such as hardware architecture and semiconductor behavior Further, there is no standard for these lightweight cryptographic algorithms, the *National Institute of Standards and Technology – NIST* have recently examined the possibility of releasing a specific standard, by involving subject experts, the question resides if there are enough proven

implementations for the standardization, the fact is further aggravated by the continuous market developments which continuously introduce new technological aspects which impact the algorithm compatibilities.

4.3.2 Intrinsic security

Bedrock Automation propose a new platform – *Open Secure Automation – OSA*, designed to meet improvements in performance, reliability, and security at lower lifecycle cost. One of the key aspects in this new platform is the Intrinsic Cyber Security.

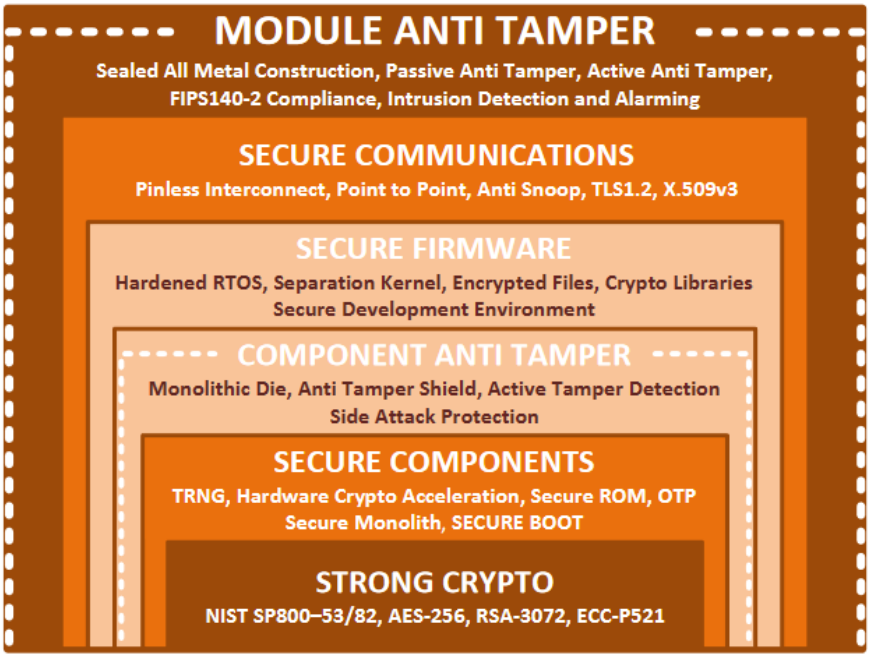


Figure 4. 17: Building Blocks for Intrinsic Security (Rooyakkers et al. 2016).

Rooyalkers et al. (2016), sustain that the design is a clear move forward for the traditional automation systems that are not natively cyber secure, and further argument through the evolutions of the building blocks presented in figure 4.17. The concept include the utilization of metal module housing present clear advantages over the traditional plastic housings, environmental hardening, structural integrity, thermal integrity, extended operational time and where *Electromagnetic Interference - EMI* and *Electromagnetic pulses - EMP* hardening, and cyber integrity – anti tamper, critical on a cyber security context are few of the advantages. Unnecessary ports are eliminated, reducing the compromise accesses to the system resources, and encryption and authentication are required to all devices that communicate on the remaining ports. Backplanes and module pins are susceptible to surface cyber-attacks, the design aims on pinless I/O backplanes and seal metal construction of all system modules. Counterfeit components are rejected by the system, the elimination of this cyber-attack vector is achieved through the design of intrinsic hardware and firmware authentication with strong encryption. The design makes use of encryption of strong encryption –

Suite B, which is published an TOP SECRET protection by the *National Security Agency – NSA*; reducing the encryption method degradation over time since one of the characteristics of an automation system is the expected life time of decades and the sophistication and capabilities of the cyber-attacks follow the technological developments. The secure boot is achieved, in case of cold start or hot reset, through an initial load from on-chip masked *Read Only Memory – ROM*, monolithically part of the microprocessor silicon, and the keys that authenticate, decrypt are stored in this internal secured memory. High quality *True Random Numbers* for cryptography processes are generated in the semiconductor hardware, rather than on mathematical generations on software making it less vulnerable to discovery.
Secure supply chain and *Key Management System – KMS* are paramount to eliminate an array of possible cyber-attack vectors, the KMS controls the creation and distribution of certificate and keys, it is mandatory at the suppliers factory that the equip and lock of every system components at the silicon level is performed on the creation process. All these developments translate in a *Hardware Root of Trust* embedded in the control system, which enable *Public Key Infrastructure – PKI* application on the system, contrarily to the traditional concepts of automation systems, rendering in the so-called architecture for intrinsic security.

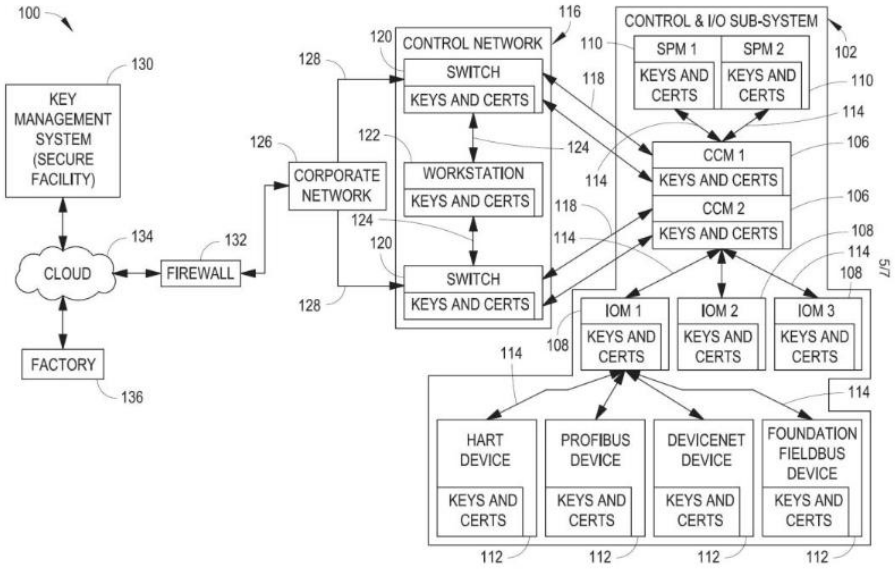


Figure 4. 18: An OSA™Cyber Architecture with an Intrinsic Hardware Root of Trust (Rooyakkers et al. 2016).

The concept has been adopted by several manufactures, for example, Bently Nevada is currently migrating their flag series 3500 series for Machinery Protection and Condition Monitoring System to a new range of products the Orbit 60 where the Intrinsic Cyber Security is one of the key characteristics.

4.3.3 Machine learning

Machine learning has contributed to the enhancement of security as well on threat detection in various networks, for example *Vehicular ad hoc Networks – VANETs*, *Mobile ad hoc Networks – MANETs*, cloud computing, between others. *Sharma et al. (2020)* further describe that due to the inherent characteristics of the IoT, traditional methods are insufficient, and aspects such as constrained resources, heterogeneity, dynamic changes of the network, substantial amount of devices and scalability can be modelled through machine learning and deep learning solutions. These models have advantages over traditional techniques, like the zero-day attacks capability.

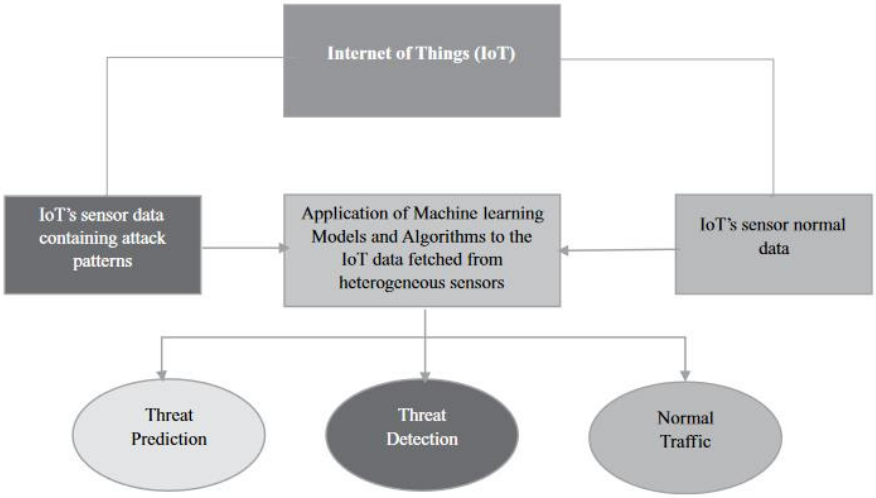


Figure 4. 19: Generic model of applicability of machine learning to IoT network for threat detection (Sharma et al., 2020).

Several Machine Learning based security solution for IoT are developed, the *Convolutional Neural Network – CNN* represents a technique which is suitable for learning from significant amounts of data, characteristic of the IoT, and where extraction and classification are two crucial phase enabling the enumeration and prediction of security risks in the IoT networks. The limitations in this technique are the time consumption of data collections as well as expensive computational algorithms.
In anomaly-based *Intrusion Detection System – IDS*, *K-Nearest Neighbor – KNN* is a technique providing attack detection capabilities, being the accuracy estimated in 84,82% detection rate and 5,56% false alarm rate. The *Support Vector Machines – SVM*, are powerful techniques which with high performance can detect malware, through the data collected for example on the resources monitoring of one system component, it as an accuracy estimated in 99.99% detection rate and 0.004% false alarm rate in one conducted study (*Sharma et al., 2020*).

Sharma et al. (2020) further mentions the present challenges in using these Machine Learning techniques:

- *Pre-Processing of Data*: Due to the characteristic of the IoT, data gathered from a variety of sensors is often constrained, discrete in nature and suffer from intermittent loss of connectivity. These irregularities and uncertainties lead to

complex processing tasks, it is necessary that the IoT ensures proper pre-processing computations before delivering the data to the Machine Learning techniques.

- *Redundancy Reduction and Compression of Data*: Some data collected by the IoT sensors isn't useful, there is a probability that the data is redundant or similar, a typical example would be the placement of close deployed sensors. This redundant information causes a waste of computational energy and issues when extracting useful features important in the optimal and efficient decision-making. It is required to have efficient redundant data elimination techniques, deployed preferably in the IoT network.
- *Subject to Adversarial and Other Attacks*: Machine Learning algorithms are prone to adversarial attacks, two easy attacks which can be performed are the causative attack in which the attacker tampers the training or test data to influence the model and other is the exploratory attack in which the attacker reverse engineers the machine learning based security model to determine the mechanisms behind it, making it possible to avoid detection.
- *Protection against the Eavesdropping and Confidentiality Violation Attackers*: Eavesdropping attacks are difficult to detect, especially in cases where the attacker is operating in the passive mode. There are cryptographic applications that can be used, but still the attacker can extract information by spoofing the identities of some communication devices.

One typical application of the Machine Learning algorithms reside in the *Security Information and Event Management – SIEM* systems, which *Vielberth et al. (2018)* describe has providers of centralized management, collection, preservation of historic log data, generation of reports for compliance purposes and which cover the threat management, provide real-time monitoring of security accidents and trigger proper reaction in case of accident.

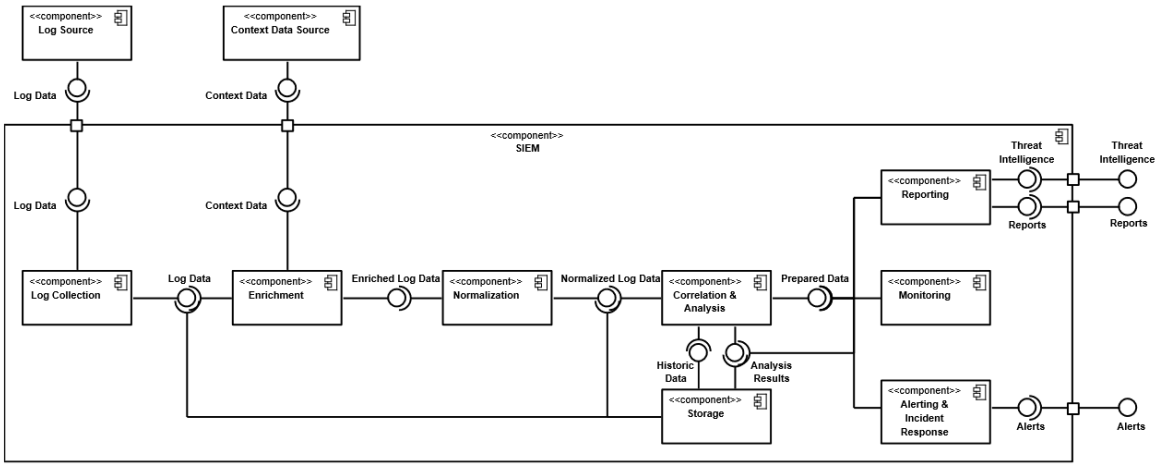


Figure 4. 20: SIEM Pattern as UML component diagram (Vielberth et al., 2018).

4.3.4 Intrusion detection

The Proliferation of heterogeneous computer systems and increased connectivity of networks in both public and private domain have challenged the *Intrusion Detection Systems - IDS*, *Möller (2021)* further conceptualizes as purpose the protection of computer systems and networks by detection of hostile cyberthreat attacks or exploitations in computer systems and networks by monitoring the data flows or packets flowing in the system and analyzing them for signs of suspicious activity and reporting possible security incidents. In addition, these systems also initiate actions in such occurrences, for example blocking the data flow or packet traffic from a particular suspicious IP address. The classical approaches are the *Host-based Intrusion Detection System – HIDS*, *Network-based Intrusion Detection System – NIDS* and *Specification-based Intrusion Detection System – SIDS* to which, in addition, two approaches are also deployed*,* the *Anomaly Intrusion Detection – AID*, that protects the computer system or network against malicious incidents and the *Misuse Intrusion Detection – MID* or *Signature Intrusion Detection - SID*, aiming to protect the computer system or network based on patterns against suspicious collection of sequences of activities or operations that are harmful.
AIDs are developed through Statistical or Cognitive Models or even Cognitive based Detection Techniques – CDT, being one of the disadvantages the number of false positives due to the difficulty in establishing a regular profile usage.

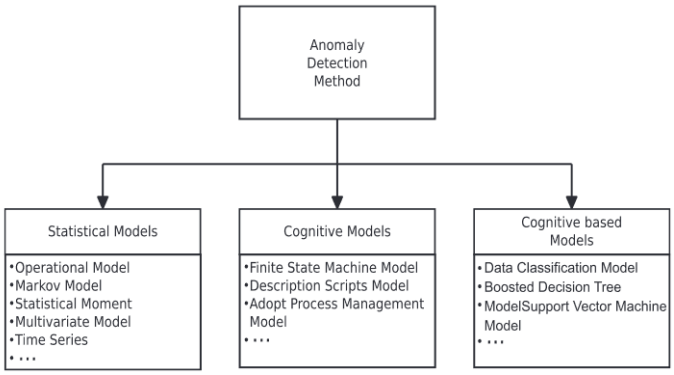


Figure 4. 21: Classification of anomaly based intrusion detection techniques (Möller, 2021).

MIDs are developed based on the recognition of known attacks signatures based through rules, these comprehended by *Blacklist-based Methods* or *Whitelist-based Methods* in addition to other techniques such as *Expert Systems – ES*, *Model-based Reasoning System – MRS*, *State Transition Analysis – STA* or *Key Stroke Monitoring – KSM*.

Limitations of the MIDs are the limited ability of detecting unknown cyber-attacks or insufficient detection accuracy by behavior-based methods, which are currently being alternated by developments in machine learning.

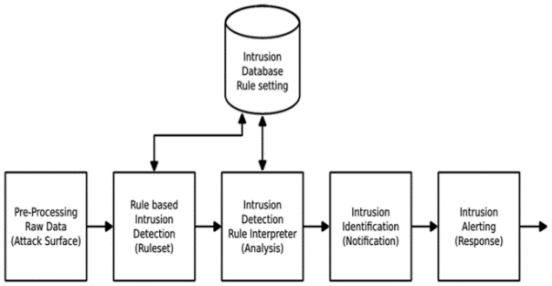


Figure 4. 22: Block diagram of a generic rule based intrusion detection system (Möller, 2021).

4.3.5 Fuzzy logic

Risk assessment models are crucial in supporting organizations on the selection of adequate techniques to protect their data assets. Due to cybercrime progression, the recognition and measuring security risks is vital to access data from innovative technologies but also to realize how technologies can be neglected, the cybercrime dynamics demand risk assessment models which can evolute by identifying and assessing security risks. *Alali et al. (2018)* purpose a *Fuzzy Inference Model – FIS* using the *Mamdani Fuzzy* model, based in four risk factors, vulnerability, threat, likelihood and impact to alternate to the common statistical approaches as the quantitative techniques, Monte Carlo simulation and Failure Mode and effect analysis and qualitative techniques which rely on the judgment of an event rather than on the statistical data such as scenario analysis. A semi-quantitative method provides the advantage of the two referred approaches, where the FIS is included, the methods imply that the analysis is subjective to the loss and is related to vague information.
The application of *Fuzzy Logic* in risk assessment models reduces the uncertainty when compared with the traditional methods, further, it is adaptable to dynamic environments through the adaptation of the logic models reducing the imperfections brought by them, *Jana et al. (2018)* demonstrate it, through the comparison of the Novel Interval Type 2 Fuzzy Logic improvement over the Novel Interval Type 1 controller.

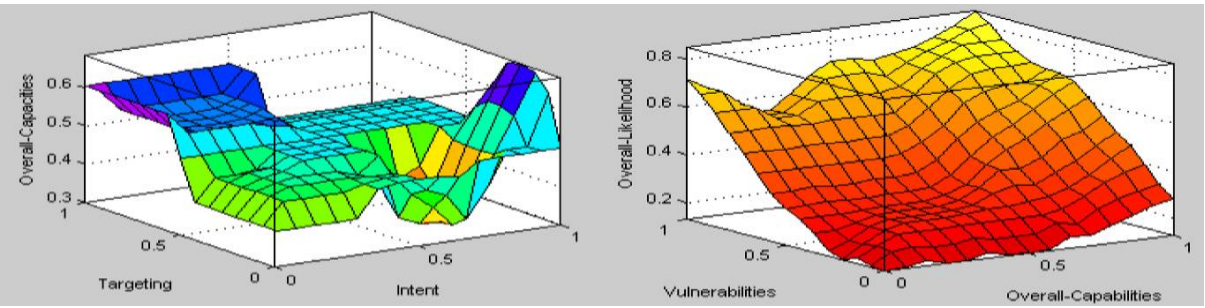


Figure 4. 23: Left - 3D Surface for Model-1, Right - 3D Surface for Model-2 (Jana et al, 2018).

4.3.6 Microsegmentation

Microsegmentation represents a natural evolution from the typical application of firewalls in a determined topology. *Chowdary et al. (2018)* reflect on the topic through the conceptual interpretation of a firewall serving as an isolation between two or more network segments according to some secure policy, working as an isolator from the internal secure network(s) and external non-secure network(s) it doesn`t provide the means to filter the traffic inside the secure network, it assumes that all the internal hosts on the internal segment are trustful. The traditional deployment model of the firewalls works sufficiently well on a restricted topology, but with the expansion of network connectivities, such as extranets, high speed lines, multiple entry points and telecommuting the model is insufficient. Firewalls are unable to protect the networks from internal attacks, the only method secure enough would be to introduce one firewall for each of the smaller networks representing one core asset inside the secure zone, which would translate in a significant and complex increase in the network administration. Another threat to the firewall is the end-to-end encryption, performed by third parties, which leads to a lack of deciphering the encrypted package since the firewall doesn`t have the key to look into it, by this, it is possible to bypass the destination restriction and hide the traffic. Further firewalls are a single-entry point, constituting both a traffic bottleneck due to increased network speeds but as well an important point of failure, if the firewall fails, all the internal networks remains isolated. Network segmentation is obtained through the creation of rules for communication paths, configuration of firewalls and VLANs, Microsegmentation brings the concept one step further by exploiting virtualization and software-defined networking technologies and make use their programmable interfaces for dynamic policy-based security assignment to the network at a granular level. It reduces the attack surface due to the distributed stateful firewalling, it provides topology agnosticism segmentation, centralized ubiquitous policy control of distributed services, granular unit-level controls implemented by high-level policy objects, network based isolation and policy-driven unit-level service insertion and traffic steering.
Figure 4.24 depicts the VMware NSX platform solution.

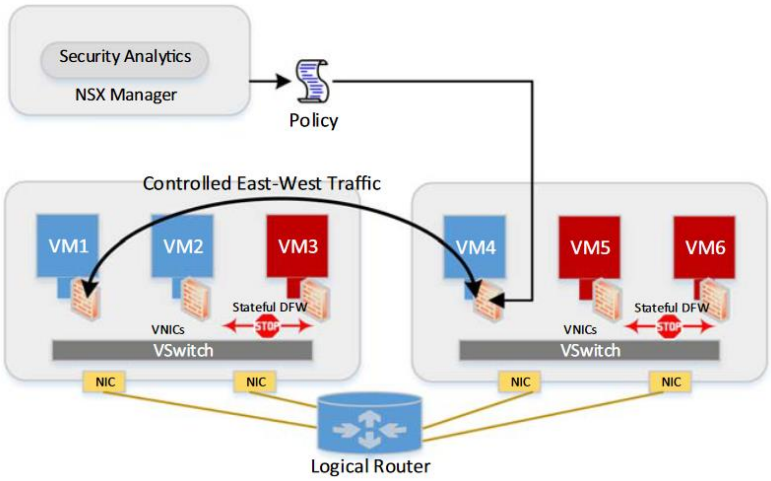


Figure 4. 24: Distributed segmentation with network overlay isolation (Chowdary et al., 2018).

4.3.7 Summary

The technological developments presented in this section are some of the solutions currently being developed offering new approaches and methods to achieve a stronger and more robust network/system security, the example brought in section 4.3.5 demonstrates that is not only the technical solutions that are a subject of interest on the topic but as well the achievement of an accurate risk assessment is an key aspect enabling organizations to choose the suitable security approach to their assets. There are developments in all areas related to the cybersecurity context, these have in many of the cases not reached the product testing phases, and will not be available in the market in short term, in addition some solutions might bring compatibility and interoperability challenges to the organizations already existing platforms.
These new developments demand new *CapEx/OpEx's* to the organizations in case they reveal themselves as interesting and technically compatible solutions, but this is part of the change of paradigm that organizations must undertake to accommodate the Digitalization competitiveness dealt in Chapter 2.

5 Current industrial landscape review within the Cyber Security and Cyber Physical Systems domains

With the technological development increase and integration of the emergent technologies the complexity of securing the organizations infrastructure also increase in a paced rhythm. The surrounding dynamics around the organizations inevitably influence the strategic propositions, core values and beyond affect the structures, their boundaries and competence areas, and value chains. These new perspectives constitute a transition to new paradigms shaping new challenges but opening simultaneously new opportunities.

5.1 Organizations

5.1.1 Culture

The *Cybersecurity Culture – CSC* is distinct from each organization and based in particular attributes of an identity in terms of technological adoptions, processes and intrinsic values, *Corradini (2020)* considers that an effective CSC is has to be considered an integral part of the *Organizations Culture – OC*, reinforcing the cohesion within the organization and creating an awareness that security is not a particular department problem, for example the IT department, it requires the involvement of all the elements that constitute the organization. To achieve a CSC it is necessary a clear strategy, resources, methods and tools and an cooperative approach is superior to a imposition of procedures which constituents in many cases do not understand.
It is necessary the evaluation of the current security culture, avoiding the adoption of security programs which are insufficient for the organizations demands, a CSC is dependent on commitment and execution from its constituents, generally it is observed that organizations with a string safe work environment are more successful in enforcing a more secure behavior regarding cyber aspects. Two types of behavior are found from an effective CSC, actions related to the specific role in the organization and other actions such as cooperative behaviors and suggestions to improve the cybersecurity approach.
The change process requires a clear mindset from organizational perspective, it requires a plan regarding investments in cybersecurity education for its constituents and the expected outcomes, it is not appropriate to consider that one time education would solve the security concerns, of course it offers a concept of importance of the human behavior in security, but this is a continuous process, in line with the technological developments.

5.1.2 Strategy

Security strategies established by organizations create the security culture that optimizes the security resilience, these contribute to the integrity, reliability, image, and reputation of the organization. *Sullivant (2016)* categorizes the strategies in two components, the general security strategies, and the special security strategies. The former ensures public safety and confidence, encourages partnering internally and externally, facilitates meaningful information share and security authority, responsibility, and accountability. The latter fosters the establishment of a security risk management program, user-friendly security assessment model, profile estimation threats, maintenance of security competencies, emergency preparedness between others.
This continuous process demands the unification of the organization, a clear purpose and a common understanding of roles and responsibilities, accountabilities, and determination.

5.1.3 Summary

The cultural and strategic approaches fostered by organizations play an absolute crucial permissive for the success of adopted cybersecurity programs, the literatures presented in the section contextualize the observation and comprehend an active role of the organization's leadership and management reflecting towards all the structures the necessary propositions. In the fast-paced technological environment which organizations are involved, this should not be a low frequency exercise subject to exposure to not only relaxation on the organizations practices but as well to the risk of leaving unattended emergent risks. Organizations need to consider on the financial component not only the technological and technical aspects, but as well the cultural and strategic ones.

5.2 Governance

Cyber Physical Systems cybersecurity compliance with normative and informative regulations is conditional to substantial amount of factors ranging from organizations attributes as holdings, type, location, dispersion to more technological factors such as level of technology penetration on the organizations infrastructure, digitalization, automatization, etc.
The broad range of applicable regulations introduces complexity on the organizations process of mapping the necessary criteria for the selection of security solutions which protect the intended domain(s). Therefore, it is necessary for organizations the adoption of selection and compilation processes to ensure the capture and update of the applicable norms which are further transmitted in the organizations value chain, transpiring vertically and horizontally the adherence of values and requirements.

Stallings (2018) illustrates a security plan derived from the *National Institute of Standards and Technology – NIST*, *Special Edition* 800-18, *Guide for Developing*

Security Plans for Federal Information Systems providing an overview of the security requirements of the system and describing the controls in place or planned to meet the requirements.

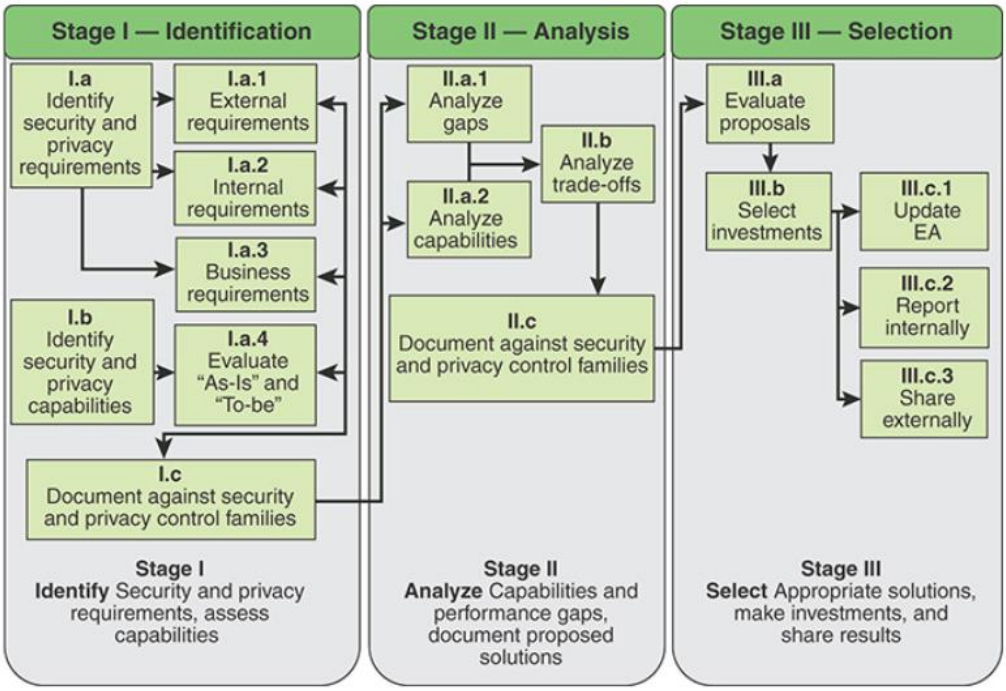


Figure 5. 1: Example of a Security Planning Process (Stallings, 2018).

Similarly, *Landoll (2016)*, substantiates the process formulated in the NIST SP 800-18 through a *Policies, Standards, and Procedure (PSPs)* development process, suggesting a convergence in interactions and interfaces of the proceeding.

The composition of the most adapted cybersecurity standards bodies in 2018 and 2019 was compiled by *Schreider (2020)*, constituted by *International Organization for Standardization – ISO*, *National Institute of Standards and Technology – NIST*, *Center for Internet Security`s – CIS*, *Payment Card Industry Data Security Standard – PCI DSS* and where industry specific standard families are excluded. Further it was noticed that most organizations use at least two standards in their cybersecurity programs.

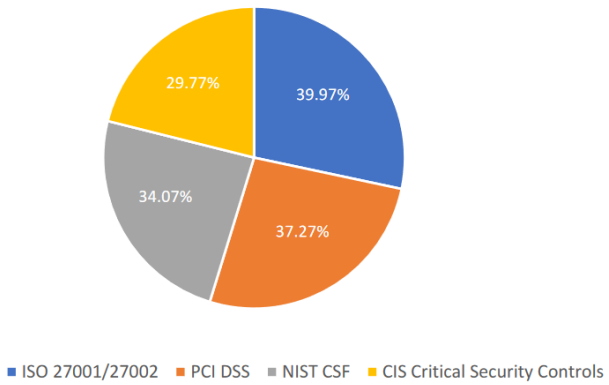


Figure 5. 2: Cybersecurity Standards Adoption (Schreider, 2020).

5.2.1 International Organization for Standardization - ISO

ISO offers publications for cybersecurity topics which are review every 5 years. The most used ISO information technology security standards are illustrated in the figure 5.3.

Figure 5. 3: ISO Information Technology Security Standards (Schreider, 2020).

Table 5.1 summarizes the respective contents of the standards published by ISO.

Table 5. 1: Overview of ISO standard and content (ISO, 2021).

Standard	Content
ISO/IEC 27001:2013 *Information Security Management Systems – Requirements (ISMS)*	Requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
ISO/IEC 27002:2013 *Code of Practice for Information Security Controls.*	Guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).
ISO/IEC 27003:2017 *Information Security Management System Implementation (ISMS) Guidance.*	Provides explanation and guidance on ISO/IEC 27001:2013
ISO/IEC 27004:2016 *Information Technology – Security Techniques - Information Security Management – Monitoring, Measurement, Analysis and Evaluation.*	Guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: a) the monitoring and measurement of information security performance. b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls.

	c) the analysis and evaluation of the results of monitoring and measurement. ISO/IEC 27004:2016 is applicable to all types and sizes of organizations.
ISO/IEC 27014:2013 *Information Technology – Security Techniques - Governance of Information Security.*	Guidance on concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security related activities within the organization.
ISO/IEC TR 27016:2014 *Information Technology – Security Techniques - Information Security Management – Organizational Economics.*	Guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. Applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions.
ISO/IEC 27017:2015 *Information Technology – Security Techniques -Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services.*	Guidelines for information security controls applicable to the provision and use of cloud services by providing: - additional implementation guidance for relevant controls specified in ISO/IEC 27002. - additional controls with implementation guidance that specifically relate to cloud services. Provides controls and implementation guidance for both cloud service providers and cloud service customers.
ISO/IEC 27018:2019 *Information Technology – Security Techniques -Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*	Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. Specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services. Applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations. The guidelines in this document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.
ISO/IEC 27032:2012 *Information Technology – Security Techniques – Guidelines for Cybersecurity.*	Guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides: an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

ISO/IEC 27033-1:2015 *Information Technology – Security Techniques – Network Security – Part 1: Overview and Concepts.*	Provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links.)
ISO/IEC 27034-1:2011 *Information Technology – Security Techniques – Application Security – Part 1: Overview and Concepts.*	Provides guidance to assist organizations in integrating security into the processes used for managing their applications. Presents an overview of application security. It introduces definitions, concepts, principles, and processes involved in application security.
ISO/IEC 27035-1:2016 *Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of Incident Management.*	Presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt. The principles given in ISO/IEC 27035-1:2016 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in ISO/IEC 27035-1:2016 according to their type, size, and nature of business in relation to the information security risk situation. It is also applicable to external organizations providing information security incident management services.
ISO/IEC 27036-1:2014 *Information Technology – Security Techniques – Information Security for Supplier Relationships – Part 1: Overview and Concepts.*	Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. ISO/IEC 27036-1:2014 addresses perspectives of both acquirers and suppliers.
ISO/IEC 27037:2012 *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.*	provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition, and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

5.2.2 International Electrotechnical Commission - IEC

Industry specific standards were developed by the IEC Technical Committee 65 in collaboration with the *International Instrumentation Users Association*, referred to as the from its original and now obsolete Dutch name, and *Instrumentation, Systems and Automation Society - ISA 99* committee members *(IEC 62443 2-4, 2017)*.

The IEC 62443 is divided in several parts, the overview is represented through figure 5.4.

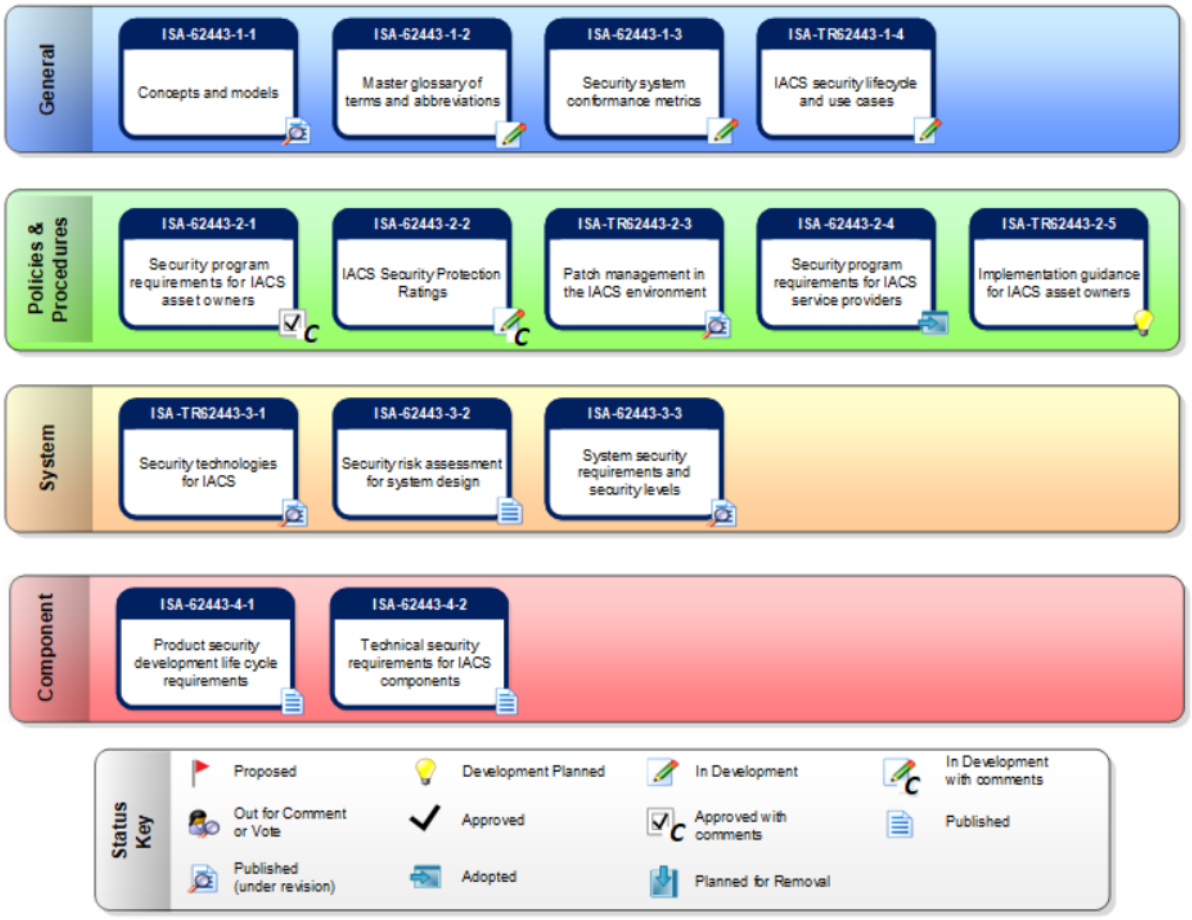


Figure 5. 4: Parts of the IEC 62443 Series and their status (ISA, 2021).

Table 5.2 summarizes the respective contents of the IEC 62443 published series.

Table 5. 2: IEC 62443 Standard publications and content (IEC, 2021).

Standard	Content
IEC 62443-1-1:2009 *Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models*	Defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.
IEC 62443-1-2:xxxx *Industrial Communication Networks – Network and System Security – Part 1-2: Master Glossary of Terms and Abbreviations.*	Currently under development.

IEC 62443-1-3:xxxx *Industrial Communication Networks – Network and System Security – Part 1-3: System Security Compliance Metrics.*	Development is planned.
IEC 62443-1-4:xxxx *Industrial Communication Networks – Network and System Security – Part 1-4: IACS Security Lifecycle and Use-Case.*	Currently under development.
IEC 62443-2-1:2010 *Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program.*	Defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.
IEC 62443-2-2:2020 *Industrial Communication Networks – Network and System Security – Part 2-3: IACS Security Program Ratings.*	Draft sent out for comments.
IEC 62443-2-3:2015 *Industrial Communication Networks – Network and System Security – Part 2-3: Patch Management in the IACS Environment.*	Describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. This Technical Report recommends a defined format for the distribution of information about security patches from asset owners to IACS product suppliers, a definition of some of the activities associated with the development of the patch information by IACS product suppliers and deployment and installation of the patches by asset owners. The exchange format and activities are defined for use in security related patches; however, it may also be applicable for non-security related patches or updates.
IEC 62443-2-4:2015 *Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers.*	Specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.
IEC 62443-2-5:xxxx *Industrial Communication Networks – Network and System Security – Part 2-5: Implementation Guidance for IACS Asset Owners.*	Development is planned.
IEC 62443-3-1:2009 *Industrial Communication Networks – Network and System Security – Part 3-1: Security Technologies for Industrial Automation and Control Systems.*	Provides a current assessment of various cybersecurity tools, mitigation countermeasures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cybersecurity technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary

	recommendations and guidance for using these cybersecurity technology products and/or countermeasures.
IEC 62443-3-2:2020 *Industrial Communication Networks – Network and System Security – Part 3-2: Security Risk Assessment for System Design.*	Establishes requirements for: defining a system under consideration (SUC) for an industrial automation and control system (IACS); partitioning the SUC into zones and conduits; assessing risk for each zone and conduit; establishing the target security level (SL-T) for each zone and conduit; and documenting the security requirements.
IEC 62443-3-3:2013 *Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels.*	Provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.
IEC 62443-4-1:2018 *Industrial Communication Networks – Network and System Security – Part 4-1: Secure Product Development Lifecycle Requirements.*	Specifies the process requirements for the secure development of products used in industrial automation and control systems. This specification is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). IEC 62443-4 defines secure development life cycle (SDL) requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element. The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining, and retiring hardware, software or firmware. These requirements only apply to the developer and maintainer of the product and are not applicable to the integrator or the user of the product.
IEC 62443-4-2:2019 *Industrial Communication Networks – Network and System Security – Part 4-2: Technical Security Requirements for IACS Components.*	Provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component). As defined in IEC 62443-1-1 there are a total of seven foundational requirements (FRs): a) identification and authentication control (IAC), b) use control (UC), c) system integrity (SI), d) data confidentiality (DC), e) restricted data flow (RDF), f) timely response to events (TRE), and g) resource availability (RA). These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.

5.2.3 Norwegian Oil and Gas Association - NOG

The Norwegian Oil and Gas Association – NOG has published several guidelines which support directly or indirectly the security of a Cyber Physical System, in this case oriented to Cyber Physical Production Systems. It is of informative interest that an overview is realized to some of its publications.

Table 5.3 summarizes provides an overview of the relevant guidelines and their purpose.

Table 5. 3: Applicable NOG Guidelines and their content (Norsk Olje & Gas, 2021).

Guideline	Content
NOG 104: 2016 *Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems.*	Guidance on how to implement the Norwegian Oil and Gas information security baseline requirements (ISBRs) in process control, safety and support (PCSS) ICT systems. The implementation guidance in the document is considered "good practice" for information security, but the organization should adapt the proposed solutions in accordance with their own information security policy and regulations and aligned with their national legislation. Implementing the information security controls and measures exactly as described in this guidance is not mandatory. Other methods and techniques may be used as long as the objectives of the ISBRs are achieved.
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases.*	Focuses on the activities which need to be performed during the different phases of engineering, procurement and commissioning, with respect to the different ISBR requirements in the Norwegian Oil and Gas Guideline no. 104.
NOG 123: 2009 *Recommended guidelines for classification of process control, safety and support ICT systems based on criticality.*	The document "Information Security Baseline Requirements for Process Control, Safety and support ICT Systems" (ISBR) was issued as Norwegian Oil and Gas Guideline no. 104. The guideline consists of 16 requirements to operators and suppliers within the oil and gas industry on the Norwegian Continental Shelf. The IBSR #2 requires that "Risk assessment shall be performed for process control, safety and support ICT systems and networks". To help focus the risk assessment on essential systems, a classification of the ICT systems in the process control environment may be needed. The document is a guideline on how to perform classification of Process Control, Safety and support ICT Systems based on the systems criticality.

Legend:

- ISBR – Information Baseline Security Requirements.

5.2.4 Summary

The section contains a group of bodies with normative and informative publications which are applicable in Cyber Physical Systems lifecycle. There are other bodies which are not mentioned, since the intended essence is the capture of international, industry specific, and national publications. From the examples introduced, it is possible to verify the complexity and amount of available regulations, further the translation of these into an organizational framework for information security require exhaustive and continuous processes leading to a demand of dedicated and skilled resources inside the organization.

6 Cyber Security governance review in Cyber Physical Systems lifecycle

The section exposes the application, but not limited, to selected standards, and seeks to illustrate common practices, and solutions brought by normative and informative references.
The layered composition of a Cyber Physical System structured by the physical, cyber-physical and network layers foster an aggregated approach comprised by different lifecycle frameworks characterized by their temporal spans.
In particular, these approaches can be derived and customized attending to the intrinsic complex characteristics of a determined Cyber Physical System constituted by concurring frameworks. One key originator is the *Systems Development Lifecyle - SDLC*, founded on the 1960`s to develop large scale functional business systems in an age of large industrial business conglomerates as detailed by *Elliot (2004)*. The stages of the traditional SDLC with the typical activities are described in table 6.1.

Table 6. 1: The traditional Systems Development Lifecycle - SDLC (Elliot, 2004).

Stages	Activities
Stage 1: *Systems Analysis*	• System definition. • Feasibility study. • Requirements specification
Stage 2: *Systems Design*	• Logical design. • Physical design.
Stage 3: *Systems Implementation*	• Programming. • Installation. • Conversion. • Documentation. • Training.
Stage 4: *Systems Evaluation*	• Testing. • Organization. • Maintenance.

The formal systems life cycle concept which the present work is founded is based on the ISO/IEC/IEEE 27748-1, comprising of the *Concept*, *Development*, *Production*, *Utilization*, *Support* and *Retirement* stages.

The figure 6.1 illustrates the lifecycle model with the interactions and some possible regressions between the different stages.

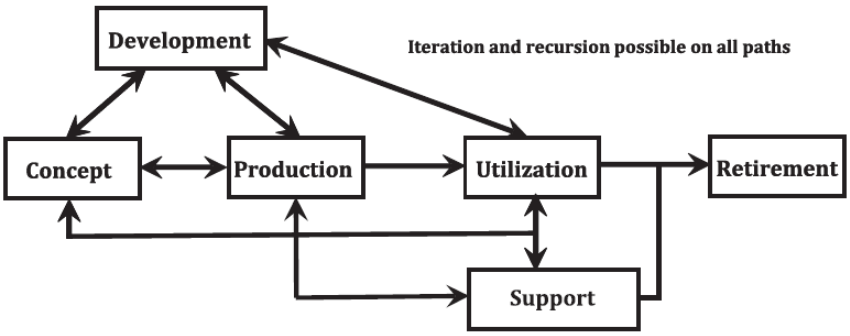


Figure 6. 1: Life cycle model with some of the possible regressions (ISO/IEC/IEEE 27748-1, 2018).

The ISO/IEC/IEEE 27748-1, exemplifies some key activities through the lifecycle model stages, underlining that these are not normative and are dependent on the organization approach.

Table 6. 2: Example of activities for each stage (ISO/IEC/IEE 27748-1, 2018).

Stages	Activities
Stage 1: *Concept*	• Identification of stakeholder`s needs. • Exploration of concepts. • Proposition of viable solutions.
Stage 2: *Development*	• Definition of system requirements. • Creation of solution description. • System build. • System verification and validation.
Stage 3: *Production*	• System production. • Inspection and testing.
Stage 4: *Utilization*	• Operation of system in accordance with user's needs.
Stage 4: *Support*	• Provision of sustained system capability.

Stage 4: *Retirement*	• Storage, archive, or disposal of system(s).

The processes further exemplified in this chapter are in a higher degree of incidence to Cyber Physical Production Systems but still very dependent on the organizational culture, asset type, project execution length, resources, and their skills. Further, the reference to NOG guidelines, which conceptually are referenced in the Oil & Gas Industry, are hereby discriminated with the solely purpose of illustration of applicability towards a particular Cyber Physical Production Systems which the function is inserted in this industrial domain.

6.1 Concept

Upon the initiation of the *Concept* campaign of a new project or on the retrofitting of an existing asset, either through the upgrade of the existing system or adding new modules or features for example, one of the first technical steps is the definition of the applicable standards and specifications, for that purpose a similar process as the one represented in figure 5.1 is conducted by the organization.

Traditionally, and apart of internal organization guidelines, the ISO, IEC and NOG standards/guidelines are followed for reference purposes. Few examples of typical application of the standards in this stage is presented in the table 6.3:

Table 6. 3: Example of standard application in asset Concept phase.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the conceptual phase for the Functional Design Specification: ISBR#1: An Information Security Policy for process control, safety and support ICT systems environments shall be documented. ISBR#2: Risk assessments shall be performed for process control, safety and support ICT systems and networks.
IEC 62443-1-1:2009 *Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models*	The standard includes two steps to be taken during the concept phase: Identification: - Recognize need for protection of property, assets, services, or personnel - Start developing the security program. Concept: • Development of the security program. • Document assets, services, and personnel needing some level of protection. • Document potential internal and external threats to the enterprise. • Establishment of the security mission, visions, and values.

	• Development of security policies for industrial automation and control systems and equipment, information systems and personnel.
ISO/IEC 27002:2013 *Code of Practice for Information Security Controls*	Section 6.1.5 states that the Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that: - information security objectives are included in project objectives. - an information security risk assessment is conducted at an early stage of the project to identify necessary controls. • information security is part of all phases of the applied project methodology.

Legend:

- ISBR – Information Baseline Security Requirements.

The IEC 62443-1-1 depicts the model relationships between all the series parts, where the definition of policies, procedures and guidelines based on the selection of the applicable regulations are one of the key aspects in the process.

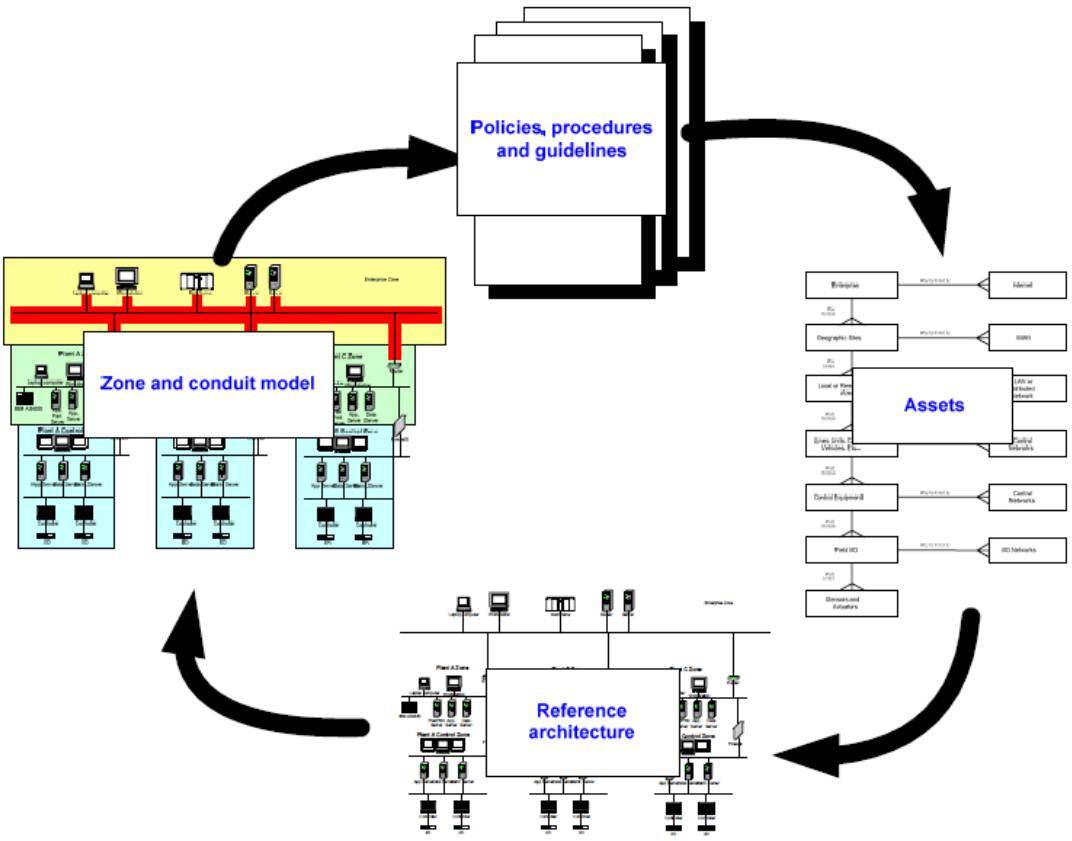


Figure 6. 2: Model Relationships (IEC 62443-1-1, 2009).

6.2 Development

The *Design* phase comprises the definition of information security detailed solutions adequate to the project in question. These are selected based in several requirements brought by the regulation definition realized in the *Concept* stage but as it is necessary to take in consideration the maturity of the selected application systems which are required to secure.

Table 6. 4: Example of standard application in asset Development phase.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the Development phase for the Functional Design Specification: ISBR#4: Infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled. ISBR#16: Procedures for reporting of security events and incidents shall be documented and implemented in the organization. For the Organization for Operations the following requirement applies: ISBR#7: Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.
IEC 62443-1-1:2009 *Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models*	The standard includes several steps to be taken during the Development phase, one of them is presented: Functional design: - Development of the security program is completed in this phase. - Definition of the 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. - Definition of the functional security organization and structure. - Definition of the functions required in the implementation plan. - Definition and publication of the security zones, borders, and access control portals. - Completion and issue of security policies, and procedures.
ISO/IEC 27001:2013 *Information Security Management Systems – Requirements (ISMS)*	Normative Annex A.14, sub-clause A.14.1 refers to the objective of assurance that information security is an integral part of information systems across the entire lifecycle. Including the requirements for information systems which provide services over public networks. In A.14.1.1 – Information Security Requirements Analysis and Specification, the information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

Legend:

- ISBR – Information Baseline Security Requirements.

The segmentation in conduits is achieved by the interpretation of the Process Control Safety Systems Information Communication Technologies – PCSS ICT architecture, and it relays in the principles depicted by for example in the IEC 62443 2-1 which represents a reference architecture.

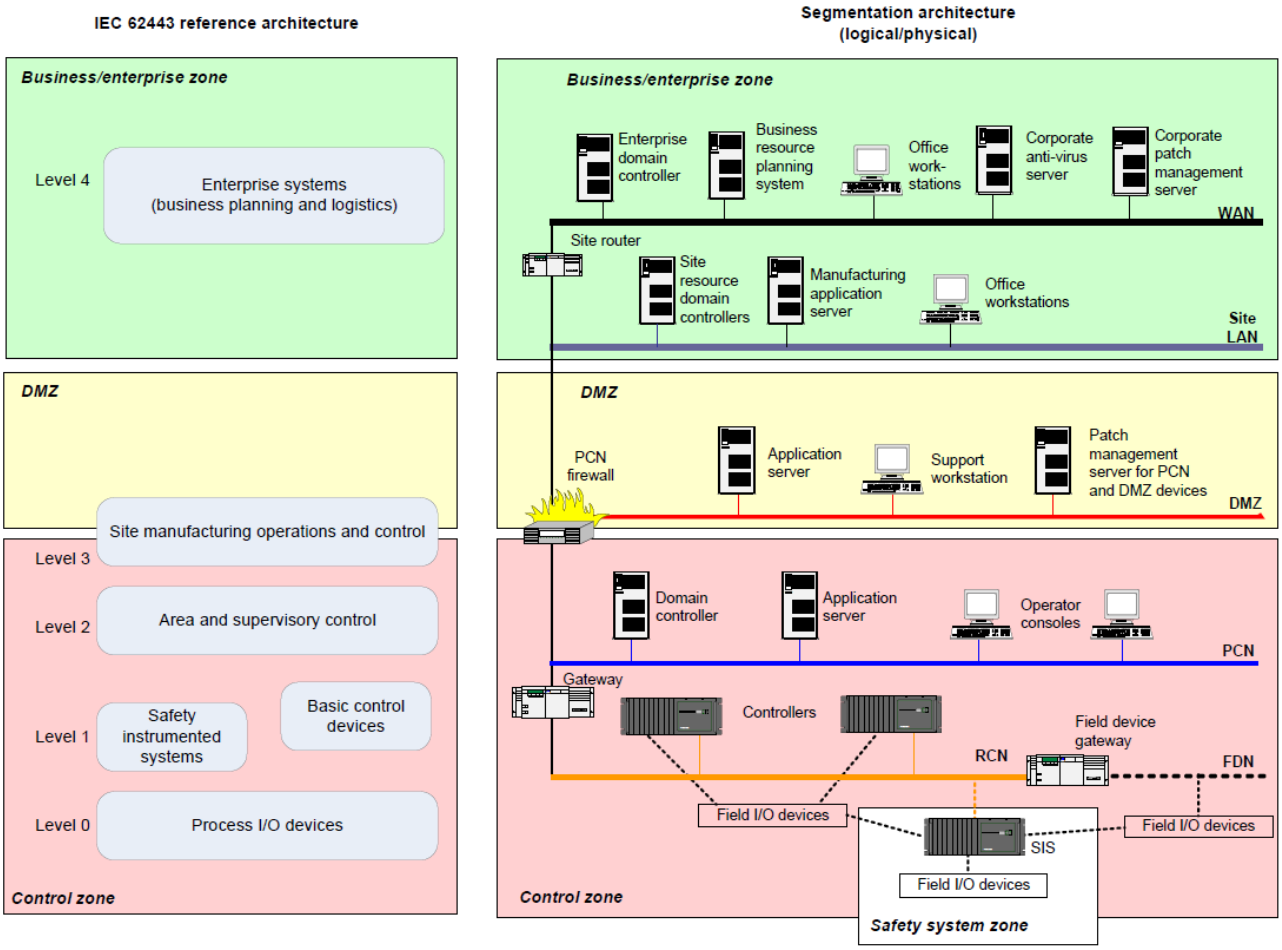


Figure 6. 3: Reference architecture alignment with an example segmented architecture (IEC 62443 2-1, 2010).

One of the primary steps is to identify the necessary conduits or zones and their risks, the typical workflow is presented in IEC 62443-3-2:2020, as presented in the figure 6.4.

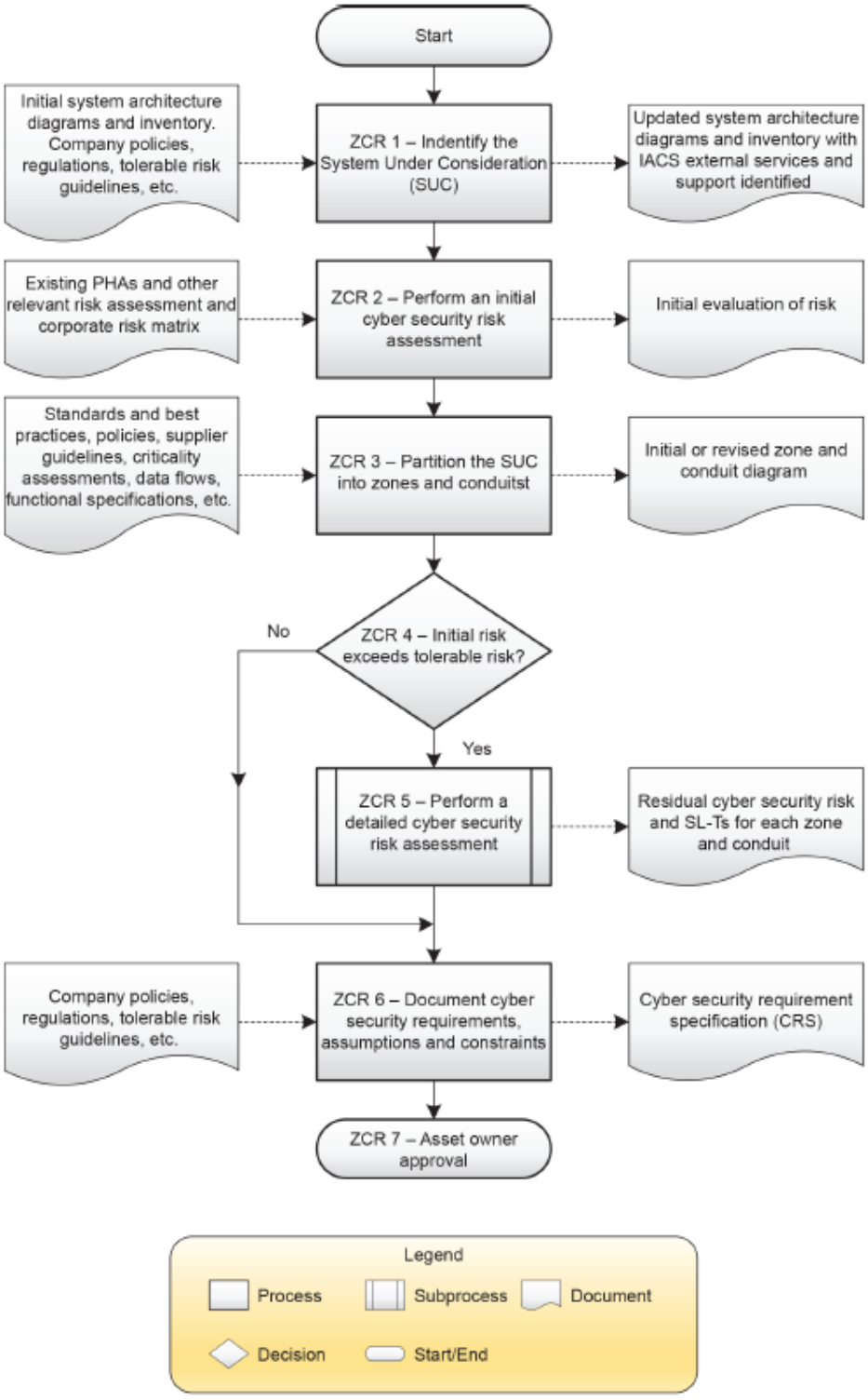


Figure 6. 4: Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk (IEC 62443-3-2, 2020).

The following step is the execution of a detailed cyber security risk assessment, action ZCR 5 in figure 6.4, with the process detailed in the workflow presented in 6.5.

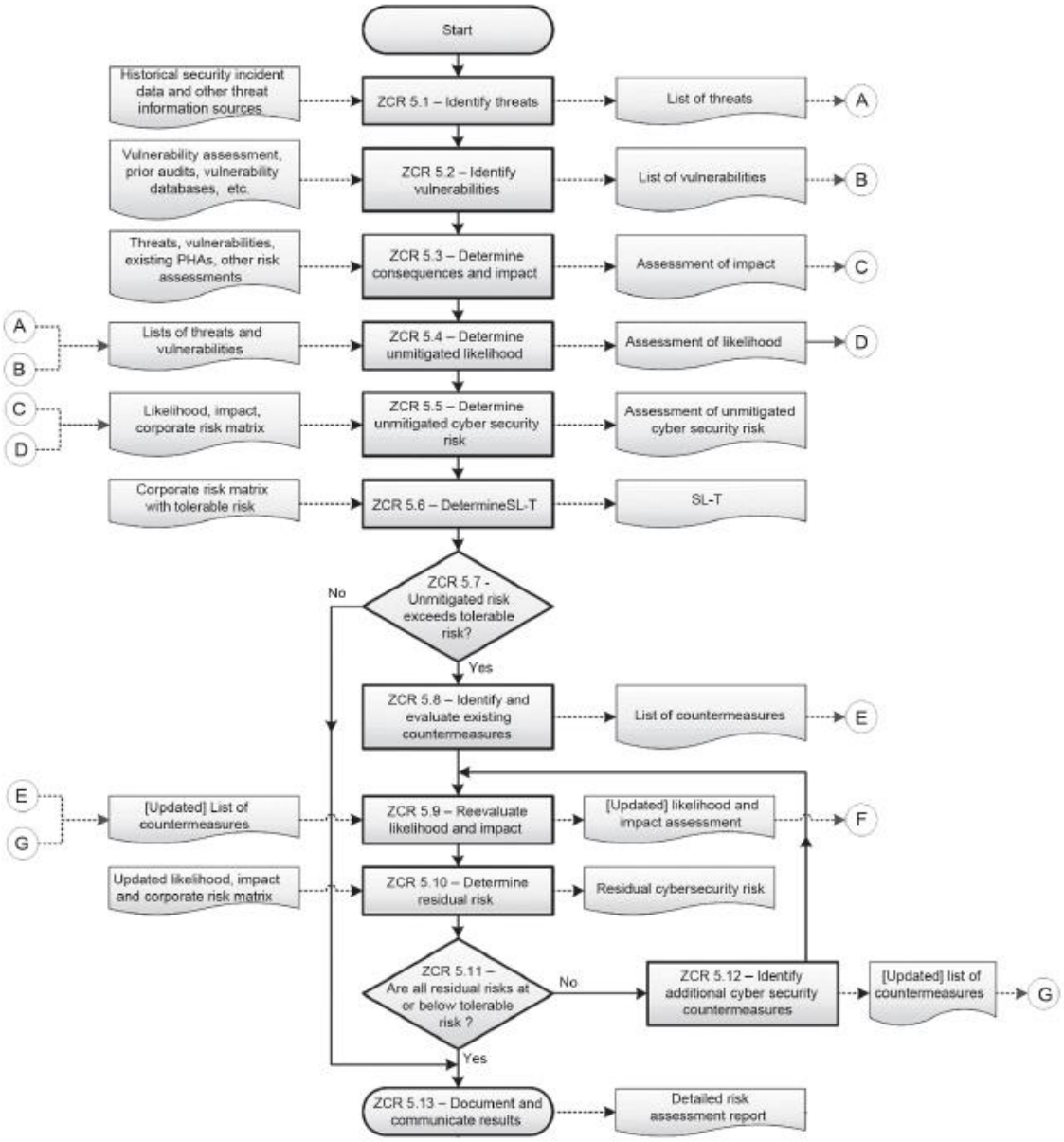


Figure 6. 5: Detailed cyber security risk assessment workflow per zone or conduit (IEC 62443-3-2, 2020).

The determination of the *Security Level – SL*, is achieved through several methods and it is dependent of the organizations approach, in some cases it is established upon the difference between unmitigated cyber security risk and tolerable risk, in other instances, is achieved through a risk matrix takin in consideration the countermeasures implied by the SL. In some cases, the decision is taken by the definition of the SL itself *(IEC 62443-3-2, 2020)*:

- • SL 1: Protection against casual or coincidental violation.
- • SL 2: Protection against intentional violation using simple means with low resources, generic skills, and low motivation.

- • SL 3: Protection against intentional violation using sophisticated means with moderate resources, Industrial Automation and Control Systems - IACS specific skills and moderate motivation.
- • SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.

To assure that the SL, is assessed during the life cycle, the model suggested by the IEC 62443 2-1:2010, during the design - assessment phases is shown in figure 6.6.

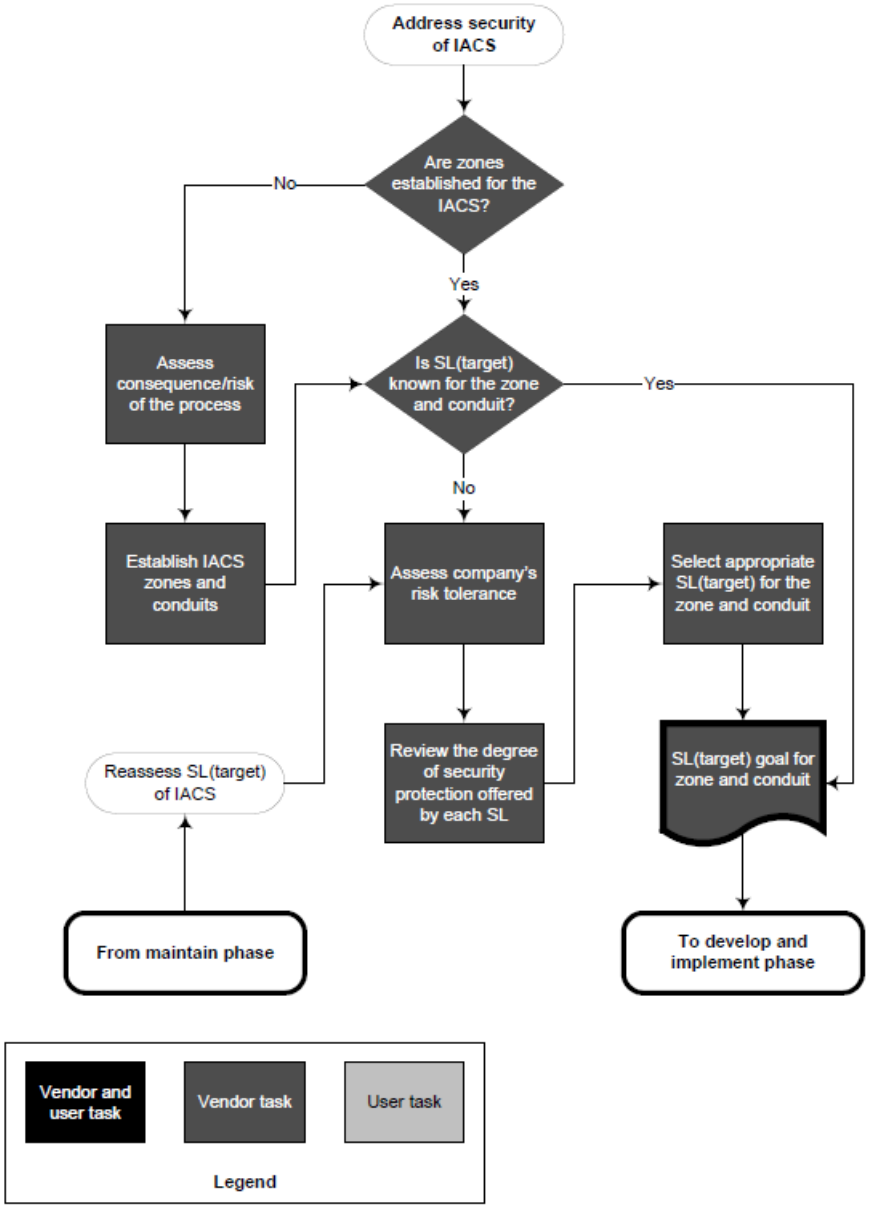


Figure 6. 6: Security level lifecycle model: Assess phase (IEC 62443 2-1, 2010).

Further expanded from figure 6.6 is the relation to the *Develop* and *Implement* phase depicted in figure 6.7.

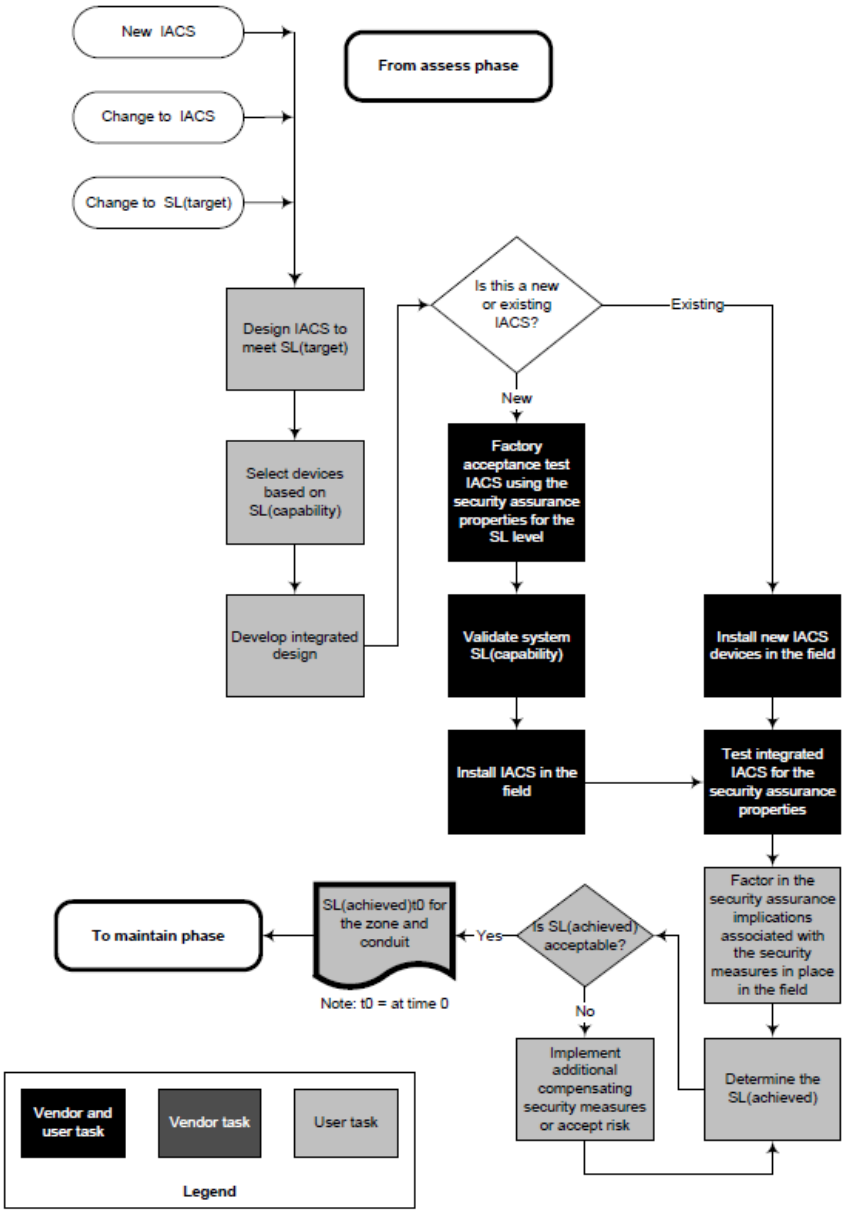


Figure 6. 7: Security level lifecycle model: Develop and implement phases (IEC 62443 2-1, 2010).

The further relation to the *Maintain* phase, translated to *Support* phase in the present lifecycle study case, will be presented in section 6.5, figure 6.8.

These relations provide guidance on how the organization can structure their approach in an orderly fashion aiding as well a systematic approach to multiple CPPS at different locations through the organization with repeatable results.

The system components acquisition is initiated in the *Development* stage, enabling the clear transmission of the project cyber security requirements to the vendor(s), but also needs to ensure compliance and executional adherence to these.

Extractions of few examples from the presented standards are presented on the table.

Table 5. 4: Example of standard application in system component acquisition activity.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the procurement phase are expressed through the individual vendor/supplier solution and test with the following IBRSs: ISBR#13: Process control, safety and support ICT systems shall have adequate, updated, and active protection against malicious software. ISBR#15: Required operational and maintenance procedures shall be documented and kept current.
IEC 62443-4-1:2019 *Industrial Communication Networks – Network and System Security – Part 4-1: Technical Security Requirements for IACS Components.*	The standard includes the Security Management – SM number 9, Security requirements for externally provided components, which states that a process shall be employed to identify and manage the security risks of all externally provided components used within the product.
ISO/IEC 27001:2013 *Information Security Management Systems – Requirements (ISMS)*	Normative Annex A.15, sub-clause A.15.1 refers to the objective of assurance of protection of the organization`s assets that is accessible by suppliers. In A.15.1.2 – Addressing security within supplier agreements, all relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Legend:

- ISBR – Information Baseline Security Requirements.

6.3 Production

In the *Production* stage it`s necessary the correct installation and configuration of the system components, requiring the necessary skilled resources but as well a detailed procedures and execution work permits. In this stage it`s highly likely that configuration adjustments are done requiring a thorough evaluation together with the designers and post cataloging of changes, which will later be used as basis for the update in the necessary operational documents.

The table 6.5 presents selected requirements extracted from the standards indicated in section 5.2.

Table 6. 5: Example of standard application in asset Production phase.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the Production phase: ISBR#6: Process control, safety and support ICT systems shall be used for designated purposes only. ISBR#9: Critical process control, safety and support ICT systems shall have defined and documented service and support levels. ISBR#10: Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety and support ICT systems and networks.
IEC 62443-2-4:2015 *Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers.*	The standard through its security requirement SP.01.01 on the solution staffing functional area indicates for training that the service provider shall have the capability to ensure that it assigns only subcontractor or consultant personnel to Automation Solution related activities who have been informed of and comply with the responsibilities, policies, and procedures required by the specification.

Legend:

- ISBR – Information Baseline Security Requirements.

The *Inspection and Test* activity ensures that the design and built systems are performing as intended, for this stage, qualified resources are required to perform the functional testing and these should be based in procedures created together with the relevant vendor, designer, operator interfaces. It is necessary to conduct the commissioning through a permit system, when accessing the different components comprising the system.
Demonstrative requirements from the standards under scrutiny are presented in the next table.

Table 6. 6: Example of standard application in asset Inspection and Test activity.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the Inspection and Test activity for the Organization for Operations: ISBR#5: Users of process control, safety and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
IEC 62443-2-4:2015 *Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers.*	The standard through its security requirement SP.10.05 on the malware protection functional area indicates that the service provider shall have the capability to ensure that for portable media that it uses for system testing, commissioning, and/or maintenance, it uses this portable media for this purpose only.

Legend:

- ISBR – Information Baseline Security Requirements.

6.4 Utilization

Organizations operational department is responsible to create and maintain procedures either through own resources or delegation to system vendor interface. It is the organization as system owner which needs to provide an operational approach of the system, using if required, the technical knowledge of other parties through formal relations.

Table 6.7 is representing standard requirements in this stage.

Table 6. 7: Example of standard application in asset Utilization phase.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the Utilization phase for the Organization for Operations: ISBR#15: Required operational and maintenance procedures shall be documented and kept current.
IEC 62443-2-4:2015 *Industrial Communication Networks – Network and System Security – Part 2-4: Security Program Requirements for IACS Service Providers.*	The standard through its security requirement SP.02.02 on the assurance functional area indicates that the service provider shall have the capability to ensure the control system components used in the Automation Solution have the ability to maintain operation of essential control system functions in the presence of system and/or network scans during normal operation.
ISO/IEC 27001:2013 *Information Security Management Systems – Requirements (ISMS)*	Normative Annex A.6, sub-clause A.6.1 refers to the objective of establishment of a management framework to initiate and control the implementation and operation of information security within the organization. In A.6.1.2 – Segregation of duties, the conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Legend:

- ISBR – Information Baseline Security Requirements.

6.5 Support

The *Support* stage is solely depended on the asset owner approach, this imposes a certain degree of abstraction in the *Support* concept, aspects as the remote accesses to sustain/upgrade the system are in many cases dependent in the organizations security culture and influence the overall adopted strategy.

From the standards evaluated in the present work, some examples are shown in the table 6.8.

Table 6. 8: Example of standard application in asset Support phase.

Standard	Relevant aspects
NOG 110: 2009 *Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases 110*	Guidelines address the following requirements for the Project Organization during the Support phase for the Organization for Operations: ISBR#15: Required operational and maintenance procedures shall be documented and kept current.
IEC 62443-2-1:2010 *Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program.*	Element 4.3.4.3, system development and maintenance, requirement 4.3.5.3.4, security policies for system development and maintenance changes states that the security requirements of a new system being installed in the IACS environment in an existing zone shall meet the security policies and procedures required for that zone/environment. Similarly, maintenance upgrades or changes shall meet the security requirements for the zone.
ISO/IEC 27001:2013 *Information Security Management Systems – Requirements (ISMS)*	Normative Annex A.11, sub-clause A.11.2 refers to the objective of prevention of loss, damage, theft or compromise of assets and interruption to the organization`s operations In A.11.2.4 – Equipment maintenance, the equipment shall be correctly maintained to ensure its continued availability and integrity.

The security level is kept in the maintenance phase through its lifecycle model from IEC 62443-2-1:2010 referenced from the originator depicted in the model presented in the figure 6.7 from section 6.2.

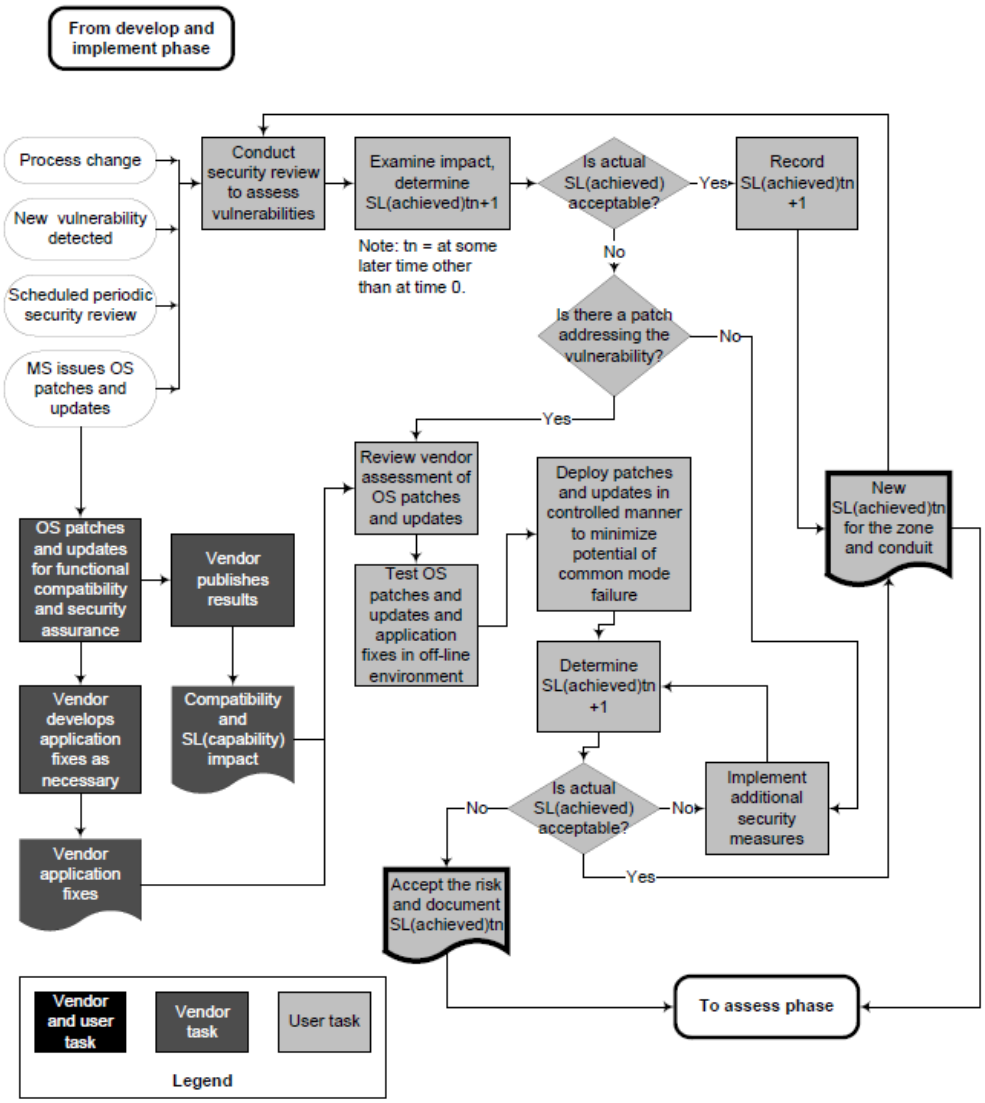


Figure 6. 8: Security level lifecycle model: Maintain phase (IEC 62443 2-1, 2010).

6.6 Retirement

The disposal of physical and virtual components in the *Retirement* stage requires careful treatment, to mitigate any disclosure of confidential information, organizations strategy avoiding any contribution towards the possibility of the creation of new vulnerabilities for assets sustaining the same principle. This is one of the factors mentioned in section 4.1.3 regarding the harvesting of information in the Cyber Kill Chain.

From the reference standards the following example is provided.

Table 6. 9: Example of standard application in asset Retirement phase.

Standard	Relevant aspects
IEC 62443-2-1:2010 *Industrial Communication Networks – Network and System Security – Part 2-1: Establishing an Industrial Automation and Control System Security Program.*	Element 4.3.4.4, information and document management, requirement 4.3.4.4.4, ensure appropriate records controls states that Policies and procedures should be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.

6.7 Summary

The present section has presented several application examples of the selected standards across the lifecycle of a Cyber Physical System. Publications from other regulation bodies, such as *National Institute of Standards and Technology – NIST*, *Internet Engineering Task Force – IETF*, etc. although being object of interest to the thematic were not included in the analysis, avoiding an extraordinary increase in the complexity and interrelationship between requirements from different proveniences.

The figure 6.9 illustrates the presented governance application during the Cyber Physical System endorsed lifecycle.

Figure 6. 9: Presented governance during Cyber Physical System lifecycle.

The concept of *System Integrator*, defined in IEC 62443-3-3:2013, as the *person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications,* is presumably applied in different stages of the lifecycle, through opportune references throughout the IEC 62443 publications, the figure 6.10 represents in principle its interaction, although a certain degree of ambiguity surrounds this entity, the perception is that the concept is applied ideally and with some responsibility adjustments from the *Concept* until the *Production* phase.

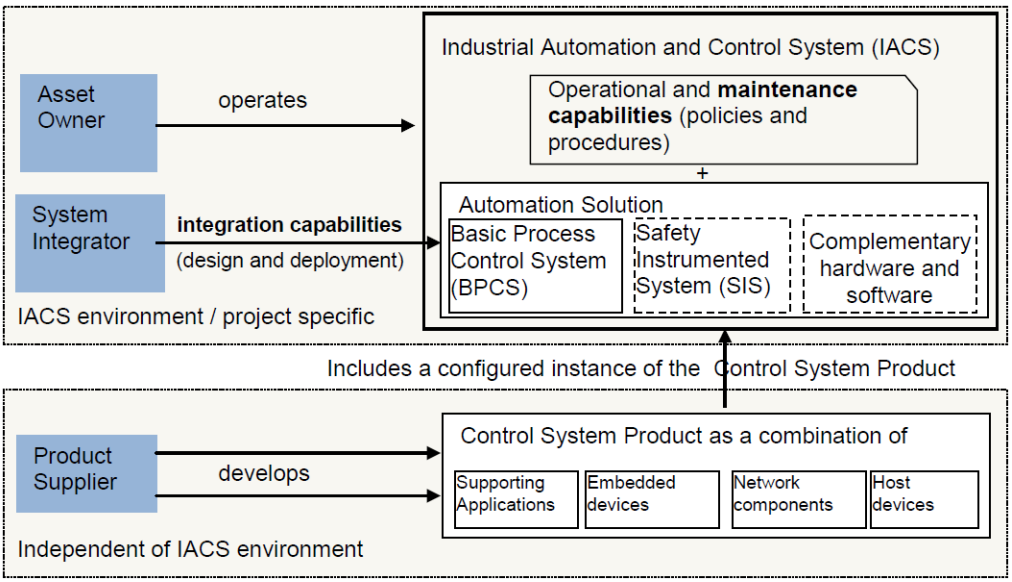


Figure 6. 10: Scope of service provider capabilities. (IEC 62443 2-4, 2015).

7 Gap analysis

Previous sections of the present essay envisaged the topics of interest and reflections about the presented concepts cross analysis and their dynamical interinfluence are summarized in figure 7.1 which the objective is to support in this section particular cases, through available references in some cases and in others through observations.
The objective is to capture captivating aspects, which upon selection shall be targeted for the development of an improved process or recommendation

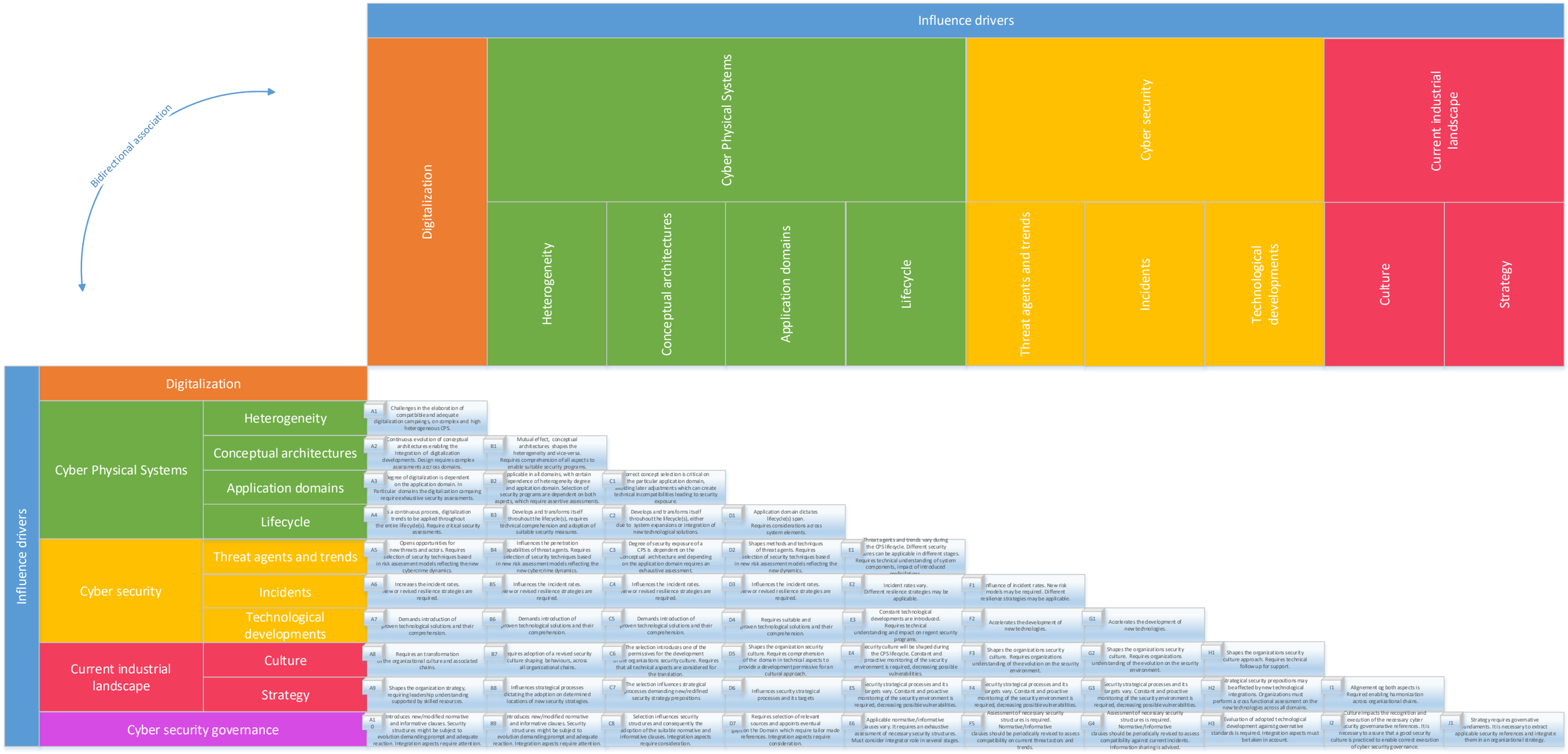


Figure 7.1: Reflections originated from concepts cross analysis.

7.1 Organizations

7.1.1 Culture

Section 4.2 brought reflections about how organizations foster a cybersecurity culture and it affects the individual as some of the incidents presented indicate incorrect security postures as the origin of the event(s).

From figure 7.1, the observations A8, B7, C6, D5, E4, F3, G2 and H1 suggest that is necessary to support a suitable and sufficient cybersecurity culture within the organization and in across all chains, and shape it as the security developments progress and as well involving the necessary methods and values in the technological integration events.

The observations are further reinforced with the insights of *Karyda (2017)*, supporting that beyond the current approaches that include security awareness programs, education, and training, it is necessary to address other aspects, namely:

- Different levels of analysis and security cultures development tailored for each individual, workgroup or teams on the organization.
- Security culture is mostly associated with security behavior addressing compliance to security and policies. When compliance remains the original objective, the comprehensive goal of raising a security culture is not fulfilled.
- Research has identified organizational aspects that influence and shape an information security culture, however their role on raising and shaping a security culture require further exploration.
- The dynamic mutual influence between the organization culture and security needs to be addressed, the organization culture may hinder appropriate change on the organization's security.
- Development of tools and metrics to evaluate the effectiveness of an information security culture.
- Research has identified the role of different internet cultures (cyber cultures) in shaping users security behavior, their impact on the information security culture needs to be addressed.

Karyda (2017) also refers to a finding, from a study conducted by the *Norwegian Center for Information Security* – NorSIS, which identifies that the cybersecurity education in Norway, fails, in great extend to educate the citizens the complex interaction between cybersecurity at the individual, societal, and national levels. In addition, states, that the compliance to internal security policies in the organizations is not likely to enable individuals to become more resilient to cybersecurity threats outside their business area of interest.

7.1.2 Strategy

Figure 7.1, observations A9, B8, C7, D6, E5, F4, G3, H2, and I1, reflect the demand for an organization strategy which involves all the necessary dynamic aspects surrounding information security, cybersecurity permissives in the strategical objectives.

O'Dwyer (2019), discloses that SMEs in Norway have been slow to prioritize IT security spending and system upgrades due to a false sense of over-confidence in the ability of their existing systems to counter the threats, based on a survey from YouGov for the NosSIS, in addition the *Danish Business Authority* – DBA, estimated that 30% of SMEs in Denmark remain vulnerable to cyber threats, being the affordability the most common reason for shelving or delaying measures to strengthen their IT security systems and employing professional expertise.

According with *Luiijf (2016)*, challenges are found on the executive level of an organization, which usually understands the primary production objectives of the organization and this focus on the business side causes a lack of interest in the underlying technological aspects of the processes that lie beyond optimal production performance and safety, i.e., that the primary business processes are monitored and controlled by an Industrial Control System – ICS, the introduction of a set of new technology related threads does not appeal to the executive level as it concerns a functional domain, not the business and profits to be made.

Deloitte (2019) observed as a remark that part of the challenge for organizations to develop their cyber risk capabilities is the own limitation of attempting to build cyber capabilities in house. Resources are hard to train and retain, executive leaderships should explore talent models and strategies to keep up with resource demands.

7.2 Governance

Figure 7.1, observations A10, B9, C8, D7, E6, F5, G4, H3, I2, and F1 suggest that considerations are required on the application of CPS governance due to the influence drivers. The present section will focus on the IEC 62443 series.

Governance constitute additional challenges for the organizations, *Huth et al. (2017)* elaborate that the significant cost associated with the compliance, which represents a key competitiveness factor, can have similar magnitudes as the adoption of the most advanced production techniques and new technologies. Overregulation or complex compliance requirements may lead to the relocation of the business to other geographical areas, limiting the regulatory risk. Another factor is the pace asymmetry between regulatory decision-making processes and industrial investment planning that contributes to increased risk for companies in addition to the information asymmetry between private and public sectors. Regulatory requirements have direct impacts on technological solutions and their adoption should be considered as metrics to model and risk evaluation in complex systems

7.2.1 Security program maturity

The *IEC 62443-1-1 (2019)*, supports, amongst others, the reflection brought by E6, addressing that due to the increasing cybersecurity risks, organizations began to realize that cybersecurity is a continuous process and not a project with identified start and stop and when such occurs the security level declines with time, as illustrated in figure 7.2 mainly due to cybersecurity risks change originated by new threats and vulnerabilities along with technological developments.

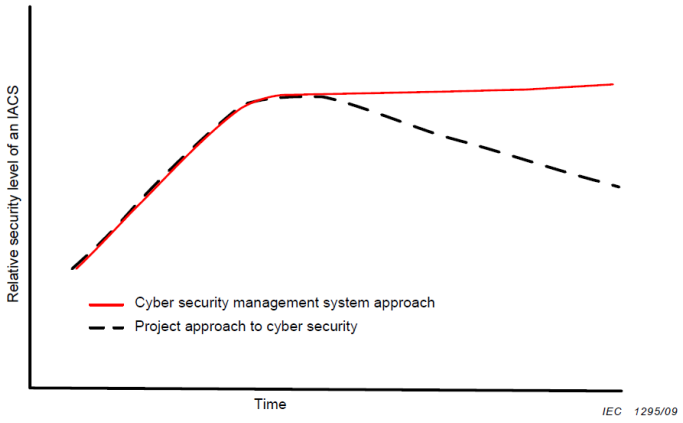


Figure 7. 2: Cybersecurity level over time (IEC 62443-1-1,2019).

It is necessary to develop and implement an organizational *Cybersecurity Management System – CSMS* across all chains, including elements to reassess risk and implement corrective actions to eliminate the tendency for security levels declination over time.

The approach is based in the organization's objectives and risk tolerance, but still subject to nuances inside the organization depending on the targeted groups, mitigating the risks according with needs and requirements.

For the CSMS success is necessary that the relevant parties inside the organization are involved, integrating all the aspects relevant for the success of the program.

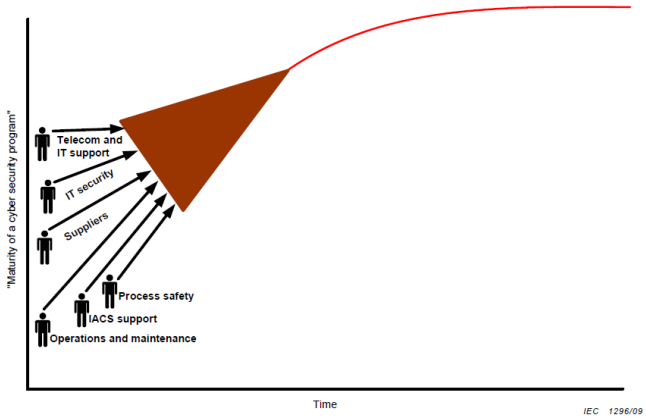


Figure 7. 3: Integration resources to develop the CSMS (IEC 62443-1-1,2019).

The integration of the relevant resources poses a challenge on the pursuit of an integrated CSMS, *Luiijf (2016)* refers to the cultural difference inside the organizations between the IT/ICT and the ICS departments, the ICS is often concerned with the availability, visibility, operability of the ICS controlled processes, the process efficiency and safety. cybersecurity, including the integrity and confidentiality aspects, are not the primary concerns. The IT/ICT on the other hand privileges the preservation of confidentiality first and then the integrity and availability
The different approaches to cybersecurity from distinct groups inside the organization lead to fragilities in the security program, which are further aggravated when the organization is composed by geographically dispersed groups of interest.

7.2.2 Interpretation

The amount of applicable regulations introduces compliance complexity to organizations, it is necessary to execute a security planning process, exemplified in figure 5.1 and tailored to the unique organization needs. In particular instances, the process is introduced in late stages of the Cyber Physical System lifecycle, namely after the concept design when developing the solution. The delayed execution could translate for instance in a late definition of the required security level for the asset, leading to possible vulnerabilities on security compliance of acquired system components, incorrect execution of risk models and, possible noncompliance of a determined SL to system as a whole. *Piggin (2013)*, further elaborates the latter, through the means of the process itself, differing from the late execution of the security planning process, on the definition of the security level the intention is to develop mathematical representations of risk, threats and countermeasures. With the increasing knowledge and experience of security incidents, threats, and countermeasures the concept will be quantified for design, selection and verification of the security level having applicability to organizations, system providers and security product providers. The immature concept requires a maturation period, and the risk of assumption of a determined security level of one particular component is not a guarantee that the security level of the system as a whole is achieved.

The utilization of the IEC 62443 series varies between organizations, industries, Cyber Physical Systems domains, and is depended on its interpretations and integration methods conjugating the array constituted for example by 3rd party deliveries, zone/conduit segregation approaches and infrastructure adopted technologies. Taking the conduits segregating the network segments as an example, it is visible that it is very dependent on the asset owner how the segregation will take place, looking at logical or physical separation of the elements is very subjective and dependent on the desired and in forehand established security level. This subjectivity becomes even more prone to misinterpretations, especially in the cases where organizations lack specialized competence on the respective technological area, and taking in consideration that on the distinct publications of the IEC 62443 series different reference topologies are presented through illustrations for development of segregated segments.

In *IEC 62443-1-1 (2009)*, it is notorious that the suggestion for segregation on the enterprise conduit to plant zones is implemented through means of a router.

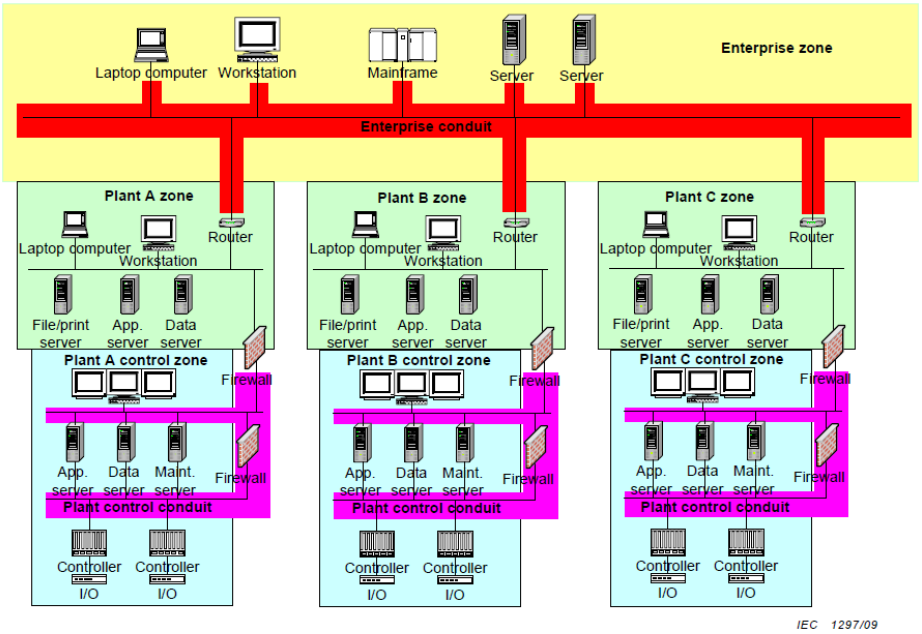


Figure 7. 4: Conduit example (IEC 62443-1-1, 2009).

The *IEC 62443-3-3 (2013)*, illustrates the conduit segregation on the enterprise level through firewall means.

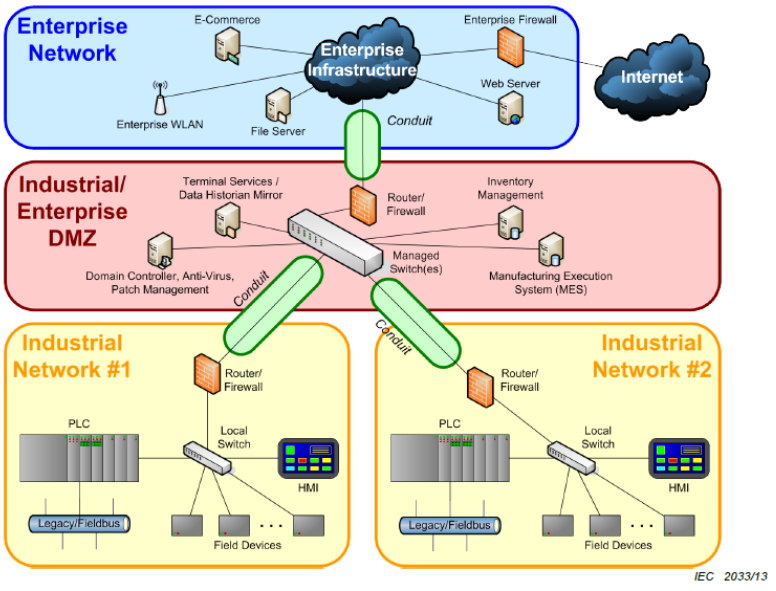


Figure 7. 5: High-level manufacturing example showing zones and conduits (IEC 62443-3-3, 2013).

The utilization of a firewall over a router poses advantages as a technological selection in terms of trusted and secure communications. The nuances between publications is susceptible to create further ambiguities.

7.2.3 Execution

The applicability of the IEC 62443 series during the Cyber Physical System lifecycle is presented in figure 7.6, adopted from *ISA (2020)* it represents the main aspects employed by organizations.

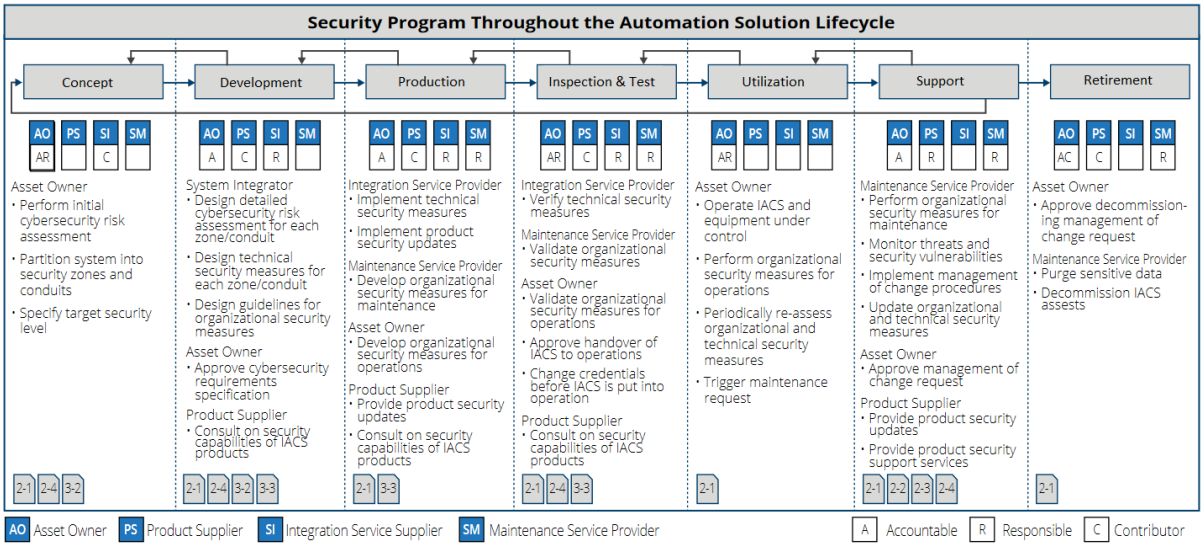


Figure 7. 6: IACS Automation Solution Security Lifecycle (adopted from ISA, 2020).

The notion of risk assessment which provides the basis of which will be determined the security level required for a particular conduit of the CPS originating the necessary allowances and constrains during the *Design* due to the security program is generally taken in early stages of the life cycle, but in many instances this evaluation should also be revisited on the *Production* phase after the 3rd party system components are provided. It is necessary from this perspective and for a robust design that additional risk assessments are exercised in additional phases, fulfilling different needs and consolidating in facto what is the risk assessment, the suggestion is that the first risk assessment is taken in a premature phase of the project, namely the *Conceptual* phase, and in addition a second exercise is performed right after the acquisition of the Cyber Physical Systems components is completed, envisaging the solutions risk and overall compliance to a system target security level. The illustration 6.7 comprehends and recommends this practice, but in many occurrences, organizations do not consider it.
It is also necessary that on the early stages of the Cyber Physical System development the transmission of such notions, example the targeted security level, is not only transmitted but also adhered by the 3rd party system components suppliers, avoiding order variations in order to meet the requirements and jeopardizing project schedules.

The system partition in particular instances is taken post 3rd party equipment selection, due to tight project schedules and poor planning leading to an adaptation of the conduit topology to the needs of the selected equipment, when the process should be exactly

the opposite, or in extreme cases to incompatibility occurrences and introduction of additional system components to overcome these same incompatibilities.

It is observed that *Systems Integrator* entity is referred on the *Concept*, *Development*, *Production,* and *Inspection & Test* phases according with *ISA (2020)*, leaving unattended the remaining stages.

7.3 Technology

Figure 7.1, observations A7, B6, C5, D4, E3, F2, G1, suggest that considerations are required on technological comprehensions due to the influence drivers.

In a technological paced environment it is imperative that organizations fully comprehend the technical aspects as the emergent solutions are commercially made available, keeping prospects of competitive advantages through the implementation of more efficient processes and at the same time keeping a resilient and secure infrastructure supporting these processes.
It is not uncommon that SMEs struggle on the perception, acquisition, and application of such developments, amongst several influencing factors, the lack of specialized resources is one of the main contributing aspects, for the comprehension of technical aspects brought by the insecurity of design on systems components for example the difficulty to have active anti-virus and host-based firewalling and execute system patching.

Huth et al. (2017) observe that ubiquitous connectivity and interoperability characteristic of heterogeneous networks and diverse systems and devices, such as the Cyber Physical Systems environments, adds complexity in the threat and vulnerability analysis leading to uneven levels of protection in interconnected systems and elements of the infrastructure increasing the attack surfaces in unknown ways. The intermingling of Cyber Physical components requires a growing implementation of complex and integrated security and risk models where the traditional domains of safety, resilience, reliability, security, and privacy once analyzed separately now require to be, in some degree, analyzed together.

The technological advances also are drivers of the governance applications, observed by *Leander et al. (2019)*, and taking as reference the *Software Defined Networks – SDN* or the microsegmentation cases as defined in section 4.3.6, these advances are gaining popularity in the cloud computing technologies, and their dynamic configuration of the network by a central node, aiming to optimize the performance based on the application is suitable for the dynamic nature of interconnection between devices and services in the Industry 4.0. These technologies seem to be conflicting with the physical and logical segregation by physical firewalls in strategic nodes as prescribed by the IEC 62443 standard.

7.4 Summary

Throughout chapter 7 observations were made, based on the presented concepts, reflecting selected and pertinent areas of improvement where deficiencies related to the cultural, strategical and governative domains were noticed. The table 7.1 summarizes the more prominent aspects of this reflections.

Table 7. 1: Gap analysis summary.

Domain	ID	Gap
Cultural	1	Cybersecurity culture is disseminated across the organization with the same approach, it requires an adaption to the different internal specialization groups/structures.
Cultural	2	Cybersecurity culture programs are based on behavioral practices/compliances, it is necessary to introduce the comprehension layers raising the awareness/cognitive levels.
Strategical	3	Insufficient recognition of the cybersecurity aspects and their importance.
Strategical	4	Built of in-house cybersecurity capabilities.
Governative	5	Insufficient integrated and continuous cybersecurity approach in the organization's substructures, convergence and harmonization of the overall security programs is deficient. All relevant organization parties are frequently non contributors on the process.
Governative	6	Reference topologies throughout the series publications aren't harmonized, leading to misinterpretations.
Governative	7	Inadequate transmission of security requirements to system suppliers.
Governative	8	Insufficient executions of risk assessments throughout the Cyber Physical System lifecycle, with particular interest for its execution after 3rd party deliveries.
Governative	9	Ambiguous and substandard application of the system role entity during the Cyber Physical System lifecycle.
Technological	10	Deficient organizational comprehension of the emergent and available technological solutions, with particular relevance for the implementation/modernization of a robust, resilient, and compatible security program.
Technological	11	Immature tailored and specifically created governative references introduced by organizations to fulfill the introduction of new technologies that may be conflicting with the traditional governance references.

8 Recommendations and expected effects

The chapter comprehends three selected and postulated recommendations of improvement based on the gaps registered in table 7.1. and their expected effects.
The adoption of the recommended practices is expected to contribute to the continuous migrations of organizations and their Cyber Physical Systems assets on the respective technologies of interest, taking in consideration the latest developments in terms of adoption of Cyber Security features, through more concise, systematic and expeditious methods.
The presented expected effects are subject of a qualitative appreciation based on projection of hypothetic expected effects through the proposition's conjectural execution.

8.1 Recommendations

8.1.1 Cyber security culture: "The knowledge driver"

The major part of the cybersecurity cultural approaches by organizations focus on the behavioral aspects of the individual towards a well-defined behavior. Compliance is important but not sufficient, it is necessary for organizations to introduce the knowledge pilar that fundaments the required behaviors. The introduction of a knowledge pilar was suggested by *Alvarez-Dionisi et al. (2019)*, to empower individuals as part of a cybersecurity culture ecosystem further as part of this observation, the additional argumentations are the substantiation of adequate behavior adaptability on security environment changes, versatility of appropriate executions in unknow scenarios, further individual comprehension of risks and practices in private context and matured risk perceptions.

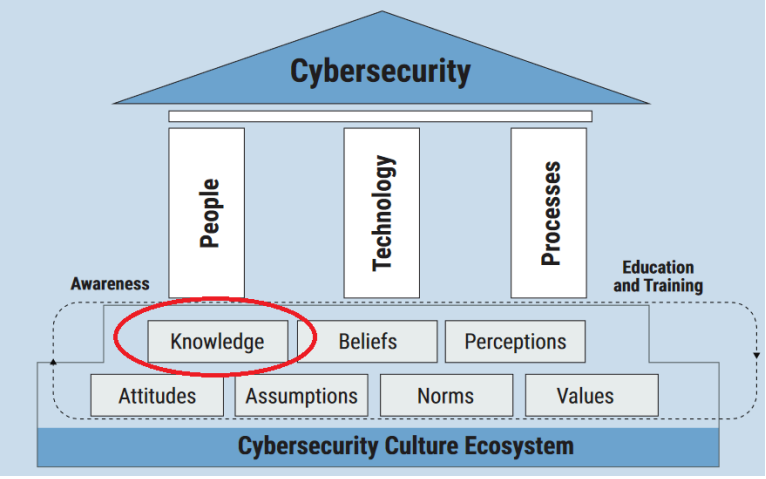


Figure 8. 1: Supporting Cybersecurity (Alvarez-Dionisi et al., 2019).

One key enabler is that organizations perceive the value of this approach and integrate it in their strategy for a cybersecurity culture program.

8.1.2 Convergence of IEC 62443 publications reference topologies

The technological circumstances surrounding the Cyber Physical Systems are inherently dynamic and, in considerable aspects, ambiguous, the proliferation of equivocal standard references should be avoided, with particular attention to the observations made in section 7.2.2, namely through the figures 7.4 and 7.5. On this particular case, the recommendation is the convergence of the referenced topologies on the IEC 62443 for improved comprehension, lower probability of misinterpretation, increased efficiency on governance application and appropriate selection of technological solutions.

8.1.3 Improved systems integrator entity engagement

One of the observations from the governance application is the role that the systems integrator entity has during the lifecycle of the Cyber Physical System. The conviction is that this entity should, in addition to the *Concept*, *Development*, *Production* stages, follow as well the *Utilization* and *Support* stages assuring that the necessary criteria have been taken in consideration when merging new technologies, protocols and subsystem internal network architectures, and ideally conjugating with execution of new risk assessments as found convenient. The figure 7.7 highlights the suggested recommendation.

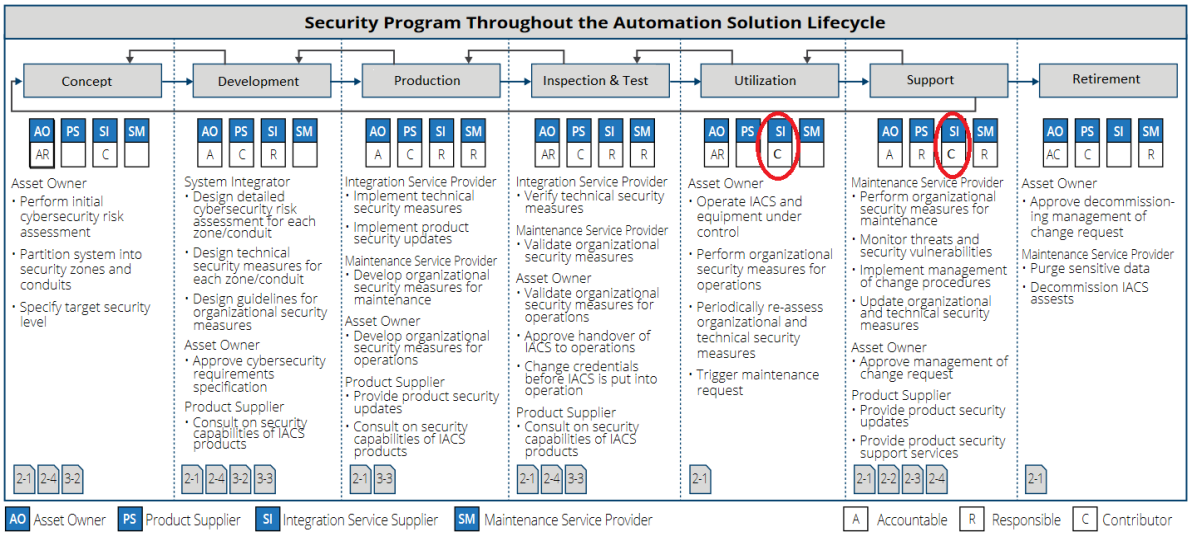


Figure 8. 2: IACS Automation Solution Security Lifecycle (adopted from ISA, 2020).

Organizations are advised to apply the entity, on the minimum extent, as informed by the relevant governance, since it is observed that frequently the entity is not considered by organizations in the *Conceptual* stage introducing additional project complexities originated by a lack of uniform technical solution and design consistency.

8.2 Expected effects

8.2.1 Augmented awareness/cognitive levels

The recommendation described in section 8.1.1, through the introduction of an "knowledge driver" enabling an evolution of the current Cyber Security culture programs is anticipated to increase and improve the individual awareness and cognitive levels substantiating in increased versatility of practices, adaptability to commute environments and, fostering not only on the workspace but as well on the private context better and more secure interaction behaviors. Organizations would benefit with this introduction through insusceptibility to risk exposure by technological migrations, which is characteristic in these environments. It is also expected that behaviors across different locations are more consistent, reducing the extension of tailor-made Cyber Security programs which accommodate the local technological applications. The projected effect is believed to contribute on the reduction of the gap's IDs 1, 2, 3 and 10 referenced in table 7.1.

8.2.2 Reduced vulnerability surface

The recommendations presented in section 8.1.2, with the convergence of the IEC 62443 publications refence topologies, translates to a reduction of possible misinterpretation upon the selection of crucial security technological components lowering the possibilities of unauthorized penetrations. The recommendation described in section 8.1.3 with an improved systems integrator entity engagement renders in a more standardized technological selection, lowering system incompatibilities and assuring correct integration methods throughout the indicated stages of the lifecycle. Both recommendations are considered to reduce, by these facts, the vulnerability surface of a Cyber Physical System, this greater degree of security is desired by organizations, specially taking in consideration the threat trends in combination with the technological environment current characterization. The projected effect is believed to contribute in the reduction of the gap's IDs 6, 7, 8, 9, 10 and 11 referenced in table 7.1.

9 Discussions

9.1 Summary

The present studies awarded the further knowledge of the latest literature and concepts dealt within the Cyber Physical Systems Cyber Security, although the theme is not new, its noticeable that only recently increased attention was provided by organizations, mainly driven by the Industry 4.0 conceptualization, digitalization, integration of the ICT technologies merging with the traditional SCADA systems and, the proliferative threat environment surrounding organizations. It culminated in this submission with the observation of the promiscuous application of concepts, inadequate technological understandings, organizational fragilities in both the cultural and strategical aspects and as well with the deficient governance application on the whole life cycle of a Cyber Physical System, all which, are driving forces that influence the overall Cyber Security performances. The present work, through the objectives enumerated in table 1.1 intended to offer a set of recommendations which practitioners can use, for both adherence upon implementation or basis for developing further evaluations and refutations of the suggestions, in essence the completion of the prepositions were achieved, further it delivered an explicit mindset of the thematic, complementing current practices and adding a clearer landscape for Cyber Security applications in Cyber Physical Systems.

9.2 Learning outcomes

The present research contributed with a clearer understanding of the main drivers influencing the Cyber Security application, although the theme was centralized in Cyber Physical Systems, the studied concepts are in large extend applicable in other distinct domains, which proves to be beneficial for utilization in other sectors. A clearer vision of the complexities and interrelation between the concepts is acquired, and this understanding is considered instrumental in both the private and professional contexts. The study on the technological developments and current solutions and practices is appraised as a multi-valued gain for future professional prospects. The observation of the governance and how it is programmed, conducted, and with its typical deployments has translated in immediate dividends, due to the utilization of the acquired knowledge on a current professional exercise.

9.3 Challenges

The substantial amount of concepts, technologies, governance references driving the Cyber Security made strenuous the selection process of the most relevant and suitable scope for development. The interrelation and association of the scope has proven to require exhaustive and in-dept reflections, which in particular cases were additionally supported by consulted references, to obtain clear interpretation boundaries. Due to the dynamic technological contexts it was necessary to sort the adequate technological solutions for the work, the process required meticulous consultation of valid sources. In the presented governance cases, the interreference clauses made the scope extraction in some moments labyrinthine.

9.4 Recommendations for future works

The registered observations throughout the research enable, but are not limited to, the following future development branches:

- Evolution of a disruptive Cyber Security technology and its influence in the current governance programs, being of particular interest the microsegmentation technology.
- Cyber Security solutions technological convergence in a system of systems.
- Cyber Security conservation on Cyber Physical System upon technological migrations.
- Organizations perception about the importance of Cyber Security adherence in the current context.

10 Conclusion

The recent and continuous reshape of catalyzing circumstances surrounding the organization's Cyber Security applications have been brought for attention, in particular and on the present, within the Cyber Physical Systems conceptualization. The areas of interest are substantial and these involving forces are not limited to this concept, the convolutions are spread across multiple domains and functional areas, requiring profound and converging commitments from distinct vertical and horizontal structures permitting a proliferation of effective security measures.

The significance of these new conceptions induces affections in contemporary Industrial Asset Management strategies, mechanisms, and perceptions generating a demand for new outlooks and evaluations.

It is anticipated that in light of these continuous and complex dynamics an increased focus is being currently triggered with new novels emerging, and with them new prospects for attenuating these fragilities can be conceived.

References

Bibliography

Accenture Cyber Threat Intelligence – Accenture CTI, 2020 Cyber Threatscape Report, Accenture, 2020.

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., Bhuiyan, M. Z. A., Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System, in, Computers & Security, vol. 74, Elsevier, 2018, pp. 323-339.

Ali, S., Balushi, T. A., Nadir, Z., Hussain, O. K., Cyber Security for Cyber Physical Systems, Springer, 2018, pp. 1-8.

Alvarez-Dionisi, L. E., Urrego-Baquero, N., Implementing a Cybersecurity Culture, ISACA Journal Volume 2 2019, Information Systems Audit and Control Association, 2019.

Bahrami, P. N., Deghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. R., Javadi, H. H. S., Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures, in, Journal of Information Processing Systems, Vol. 15, No. 14, 2019, pp. 865-889.

Biffl, S., Eckhart, M., Lüder, A., Weippl, E., Introduction to Security and Quality Improvement in Complex Cyber-Physical Systems Engineering, in, (ed), Biffl, S., Eckhart, M., Lüder, A., Weippl, E., Security and Quality in Cyber-Physical Systems Engineering, Springer, 2019, pp. 1-29.

Bossert, O., Feldmann, S., Perpetual Evolution – Rethinking the Way Digital Transformations Are Managed, in, (ed), Zimmermann, A., Schmidt, R., Jain, L. C., Architecting the Digital Transformation: Digital Business, Technology, Decision Support, Management, Springer, 2021, pp. 37-53.

Chowdhary, A., Huang, D., Sandeep, P., Software-Defined Networking and Security: From Theory to Practice, CRC Press, 2018, pp. 155-180.

Corradini, I., Building a Cybersecurity Culture in Organizations, Springer, 2020, pp. 63-86.

Dai, W., Wang, P., Sun, W., Wu, X., Zhang, H., Vyatkin, V., Yang, G., Semantic Integration of Plug-and-Play Software Components for Industrial Edges Based on Microservices, IEEE, 2019.

Deloitte, The Future of Cyber Survey 2019, Deloitte, 2019.

Echeberria, A. L., A Digital Framework for Industry 4.0: Managing Strategy, Palgrave Macmillan, 2021, pp. 1-23.

Elliot, G., Global Business Information Technology, Addison-Wesley/Pearson Education, 2004, pp. 86-125.

Fayi, S. Y. A., What Petya/NotPetya Ransonware Is and What Its Remidiations Are, in, (ed), Latifi, S., Information Technology – New Generations, 15th International Conference on Information Technology, Springer, 2018, pp. 93-100.

Fink, G.A., Edgar, T.W. Rice, T.R., Macdonald, D.G., Crawford, C.E., Overview of Security and Privacy in Cyber-Physical Systems, in, (ed), Song, H., Fink, G.A., Jeschke, S., Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Wiley, 2018, pp. 1-24.

Fink, G.A., Edgar, T.W. Rice, T.R., Macdonald, D.G., Crawford, C.E., Security and Privacy in Cyber-Physical Systems, in, (ed), Song, H., Fink, G.A., Jeschke, S., Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Wiley, 2018, pp. 129-140.

Han, M., Duan, Z., Li, Y., Privacy Issues for Transportation Cyber Physical Systems, in, (ed), Sun, Y., Song, H., Secure and Trustworthy Transportation Cyber-Physical Systems, Springer, 2017, pp. 67-86.

Huth, M., Vishik, C., Masucci, R., From Risk Management to Risk Engineering: Challenges in Future ICT Systems, in, (ed), Griffor, E., Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems, Syngress, 2017, pp. 67-82.

ISA - International Society of Automation – Global Security Alliance, Security Lifecycles in the ISA/IEC 62443 Series, Security of Industrial Automation and Control Systems, ISA, 2020.

Jana, D. K., Ghosh, R., Novel Interval Type-2 Fuzzy Logic Controller for Improvising Risk Assessment Model of Cyber Security, in, Journal of Information Security and Applications, vol. 40, Elsevier, 2018, pp. 173-182.

Jiang, J., An Improved Cyber-Physical Systems Architecture for Industry 4.0 Smart Factories, in, Advances in Mechanical Engineering, Volume 10(6), 2018, pp. 1-15.

Karyda, M., Fostering Information Security Culture In Organizations: A Research Agenda, Mediterranean Conference on Information Systems – MCIS, MCIS Proceedings 28, 2017, pp. 2-8.

Klitou, D., Conrads, J., Rasmussen, M., CARSA, Probst, L., Pedersen, B., Digital Transformation Monitor, Germany: Industrie 4.0, European Commission, EASME/COSME/2014/004, 2017.

Landoll, D. J., Information Security Policies, Procedures, and Standards: A Practitioner`s Reference, CRC Press, 2016, pp. 93-107.

Leander, B., Čaušević, A., Hansson, H., Applicability of the IEC 62443 Standard in Industry 4.0/IIoT, Proceedings of the 14th International Conference on Availability, Reliability and Security – ARES, ACM Press, 2019.

Ilic, M., Energy Cyber-Physical Systems, in, (ed), Rajkumar R., Niz, D. d., Klein, M., Cyber Physical Systems, Pearson Education, 2017, pp. 61-102.

Lee, I., Ayoub, A., Chen, S., Kim, B., King, A., Roederer, A., Sokolsky, O., Medical Cyber-Physical Systems, in, (ed), Rajkumar R., Niz, D. d., Klein, M., Cyber Physical Systems, Pearson Education, 2017, pp. 3-60.

Lee, J., Noh, S. D., Kim, H. J., Kang, Y. S., Implementation of Cyber-Physical Production Systems for Quality Prediction and Operation Control in Metal Casting, Sensors (Basel), 2018.

Lee, J., Bagheri, B., Kao, H., A Cyber-Physical Systems Architechture for Industry 4.0 Based Manufacturing Systems, in, Manufacturing Letters, Volume 3, January 2015, pp. 18-23.

Maleh, Y., Mohammad, S., Ashraf, D., Abdelkrim, H., Cybersecurity and Privacy in Cyber-Physical Systems, CRC Press, 2019, pp. 7-43.

Möller, D. P. F., Cybersecurity in Digital Transformation: Scope and Applications, Springer, 2021, pp. 47-75.

Pichler, R., Gerhold, L, Pichler, M., Seamless Data Integration ina CPPS with Highly Heteregeneous Facilities – Architechtures and Use Cases Executed in a Leraning Factory, in, Arseniev, D. G., Overmeyer, L., Kälviäinen, H., Katalinić, B., (ed), Cyber-Physical Systems and Control, Springer, 2020, pp. 1-10.

Piggin, R. S. H., Development of Industrial Cyber Security Standards: IEC 62443 for SCADA and Industrial Control System Security, Institution of Engineering and Technology Conference on Control and Automation: Uniting Problems and Solutions, 2013.

Pogrebna, G., Skilton, M., Navigating New Cyber Risks: How Business Can Plan, Build and Manage Safe Spaces in the Digital Age, Springer, 2019, pp. 13-29.

Ponnusamy, V., Regunathan, N. D., Kumar, P., Annur, R., Rafique, K., A Review of Attacks and Countermeasures in Internet of Things and Cyber Physical Systems, in, (ed), Kumar, P., Ponnusamy, V., Jain, V., Industrial Internet of Things and Cyber-Physical Systems, Advances in Computer and Electrical Engineering Book Series, IGI Global, 2020, pp. 1-24.

Prasad, R., Rohokale, V., Cyber Security: The Lifeline of Information and Communication Technology, Springer, 2020.

PwC - Pricewaterhouse Coopers, 24th Annual Global CEO Survey, A leadership agenda to take on tomorrow, PwC, 2021.

PwC - Pricewaterhouse Coopers, Cyber Threats 2020: A Year in Retrospect, PwC, 2021.

Rooyakkers, A., Galpin, S., Markovic, C., Weismiller, J., Intrinsic Cyber Security Fundamentals, in, Bedrock Automation OSA White Paper Series, Chapter 3, Bedrock, 2016.

Rødseth, H., Elefteriadis, R. J., Successful Asset Management Strategy Implementation of Cyber-Physical Systems, in, Liyanage, J. P., Amadi-Echendu, J., Mathew, J., (ed), Engineering Assets and Public Infrastructures in the Age of Digitalization, Proceedings of the 13th World Congress on Engineering Asset Management, Springer, 2020, pp. 15-22.

Salkin, C., Oner, M., Ustundag, A., Cevikcan, E., "A Conceptual Framework for Industry 4.0", in, (ed), Ustundag, A., Cevikcan, E., Industry 4.0: Managing the Digital Transformation, Springer, 2018, pp. 3-23.

Schreider, T., Cybersecurity Law, Standards and Regulations, Rothstein Publishing, 2020, pp. 159-194.

Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, Raghimi, O., ENISA Threat Landscape Report 2018: 15 Top CyberThreats and Trends, European Union Agency for Network and Information Security, 2019, pp. 116-124.

Sharma, S., Lone, F. R., Lone, M. R., Machine Learning for Enhancement of Security in Internet of Things Based Applications, in, (ed), Zahra, S. R., Chishti, M. A., Security and Privacy in the Internet of Things, CRC Press, 2020, pp. 95-108.

Sonalker, A., Griffor, E., Evolving Security, in, (ed), Griffor, E., Handbook of System Safety and Security. Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems, Syngress, 2017, pp. 67-82.
Stallings, W., Cryptography and Network Security: Principles and Practice, Pearson, 2017, pp. 42-43.

Stallings, W., Effective Cybersecurity: A guide to Using Best Practices and Standards, Addison-Wesley Professional, 2018, pp. 207-234.
Sullivant, J., Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency, Elsevier, 2016, pp. 10-18.

Tawalbeh, L. A., Tawalbeh, H., Lightweight Crypto and Security, in, (ed), Fink, G. A., Song, H., Jeschke, S., Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Wiley, 2018, pp. 243-261.

Törngren, M., Asplund, F., Bensalem, S., McDermid, J., Passerone, R., Pfeifer, H., Sangiovanni-Vincentelli, A., Schatz, B., Characterization, Analysis, and Recommendations for Exploiting the Opportunities of Cyber-Physical Systems, in, (ed), Song, H., Rawat, D. B., Jeschke, S., Brecher, C., Cyber-Physical Systems. Foundations, Principles and Applications, Academic Press 2017, pp. 3-14.

Vielberth, M., Pernul, G., A Security Information and Event Management Pattern, in, 12th Latin American Conference on Pattern Languages of Programs (SLPLoP), 2018.

Wang, L., Wang, X. V., Cloud-Based Cyber Physical Systems in Manufacturing, Springer, 2018, pp. 243-259.

Wegner, A., Graham, J., Ribble, E., A New Approach to Cyberphysical Security in Industry 4.0, in, (ed), Thames, L., Schaefer, D., Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, Springer, 2017, pp. 59-72.

Wu, L., Sun, Y., Guaranteed Security and Trustworthiness in Transportation Cyber-Physical Systems, in, (ed), Sun, Y., Song, H., Secure and Trustworthy Transportation Cyber-Physical Systems, Springer, 2017, pp. 2-22.

Zhang, Z., Li, X., Wang, X., Cheng, H., Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0, in, (ed), Thames, L., Schaefer, D., Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, Springer, 2017, pp. 127-171.

Standards

IEC 62443-1-1, Industrial Communication Networks, Networks and System Security, Part 1-1: Terminology, Concepts and Models, International Electrotechnical Commission, 2009.

IEC 62443-2-1, Industrial Communication Networks, Network and System Security, Part 2-1: Establishing an Industrial Automation and Control System Security Program, International Electrotechnical Commission, 2010.

IEC 62443-2-3, Industrial Communication Networks, Network and System Security, Part 2-3: Patch Management in the IACS Environment, International Electrotechnical Commission, 2015.

IEC 62443-2-4, Industrial Communication Network, Network and System Security, Part 2-4: Security Program Requirements for IACS Service Providers, International Electrotechnical Commission, 2015.

IEC 62443-3-1, Industrial Communication Networks, Network and System Security, Part 3-1: Security Technologies for Industrial Automation and Control Systems, International Electrotechnical Commission, 2009.

IEC 62443-3-2, Industrial Communication Networks, Network and System Security, Part 3-2: Security Risk Assessment for System Design, International Electrotechnical Commission, 2020.

IEC 62443-3-3, Industrial Communication Networks, Network and System Security, Part 3-3: System Security Requirements and Security Levels, International Electrotechnical Commission, 2013.

IEC 62443-4-1, Industrial Communication Networks, Network and System Security, Part 4-1: Secure Product Development Lifecycle Requirements, International Electrotechnical Commission, 2018.

IEC 62443-4-2, Industrial Communication Networks, Network and System Security, Part 4-2: Technical Security Requirements for IACS Components, International Electrotechnical Commission, 2019.

ISO/IEC 27001, Information Security Management Systems, Requirements (ISMS) International Organization for Standardization, International Electrotechnical Commission, 2013.

ISO/IEC 27002, Information Technology, Security Techniques, Code of Practice for Information Security Controls, International Organization for Standardization, International Electrotechnical Commission, 2013.

ISO/IEC 27003, Information Security Management System Implementation (ISMS) Guidance, International Organization for Standardization, International Electrotechnical Commission, 2017.

ISO/IEC 27004, Information Technology, Security Techniques, Information Security Management – Monitoring, Measurement, Analysis and Evaluation, International Organization for Standardization, International Electrotechnical Commission, 2016.

ISO/IEC 27014, Information Technology, Security Techniques, Governance of Information Security, International Organization for Standardization, International Electrotechnical Commission, 2013.

ISO/IEC TR 27016, Information Technology – Security Techniques, Information Security Management, Organizational Economics, International Organization for Standardization, International Electrotechnical Commission, 2014.

ISO/IEC 27017, Information Technology, Security Techniques, Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services, International Organization for Standardization, International Electrotechnical Commission, 2015.

ISO/IEC 27018, Information Technology, Security Techniques, Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, International Organization for Standardization, International Electrotechnical Commission, 2019.

ISO/IEC 27032, Information Technology, Security Techniques, Guidelines for Cybersecurity, International Organization for Standardization, International Electrotechnical Commission, 2012.

ISO/IEC 27033-1, Information Technology, Security Techniques, Network Security, Part 1: Overview and Concepts, International Organization for Standardization, International Electrotechnical Commission, 2015.

ISO/IEC 27034-1, Information Technology, Security Techniques, Application Security, Part 1: Overview and Concepts, International Organization for Standardization, International Electrotechnical Commission, 2011.

ISO/IEC 27035-1, Information Technology, Security Techniques, Information Security Incident Management, Part 1: Principles of Incident Management, International Organization for Standardization, International Electrotechnical Commission, 2016.

ISO/IEC 27036-1, Information Technology, Security Techniques, Information Security for Supplier Relationships, Part 1: Overview and Concepts, International Organization for Standardization, International Electrotechnical Commission, 2014.

ISO/IEC 27037, Information Technology, Security Techniques, Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence, International Organization for Standardization, International Electrotechnical Commission, 2012.

ISO/IEC/IEEE 24748-1, Systems and Software Engineering – Life Cycle Management, Part 1: Guidelines for Life Cycle Management, International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronic Engineers, 2018

NOG 104, Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems, rev. 06, Norwegian Oil and Gas Association, 2016.

NOG 110, Recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement, and commissioning phases, rev. 02, Norwegian Oil and Gas Association, 2009.

NOG 123, Recommended guidelines for classification of process control, safety and support ICT systems based on criticality, rev. 01, Norwegian Oil and Gas Association, 2009.

Webography

Banerjea, N., NotPetya: How a Russian malware created the world`s worst cyberattack ever, Business Standard, 2018, viewed 05/04/2021, <https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html>

Briggs, B., Hackers hit Norsk Hydro with ransomware. The company responded with transparency, Microsoft, 2019, viewed 05/04/2021, <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>.

Griffin, R., Chiglinsky, K., Voreacos, D., Was It an Act of War? That`s Merck Cyber Attack`s $1.3 Bilion Insurance Question, Bloomberg in Insurance Journal, 2019, viewed 05/04/2021, <https://www.insurancejournal.com/news/national/2019/12/03/550039.htm>.

Hydro, The cyber attack on Hydro in brief, Hydro, 2019, viewed 05/04/2021, <https://www.hydro.com/Document/Index?name=General%20cyber-attack%20presentation%20April%2012.pdf&id=28255>.

IEC Standards, viewed 25/04/2021, <https://www.iec.ch/homepage>.

ISA Standards, viewed 25/04/2021, <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>.

ISO Standards, viewed 25/04/2021, <https://www.iso.org/home.html>.

Knake, R. K., Why the SolarWinds Hack Is a Wake-Up call, Council on Foreign Relations, 2021, viewed 06/04/2021, <https://www.cfr.org/article/why-solarwinds-hack-wake-call>.

Nides, D., SolarWinds explainer: An overview of the software supply chain attack used against SolarWinds, KPMG, 2021, viewed 06/04/2021, <https://advisory.kpmg.us/blog/2021/solarwinds-explainer.html>.

Norsk Olje & Gas, viewed 25/04/2021, <https://www.norskoljeoggass.no/en/>.

O'Dwyer, G., Nordic SMEs lack the money needed for Cyber Security, Computer Weekly, 2019, viewed 28/05/2021, < https://www.computerweekly.com/news/252473811/Nordic-SMEs-lack-the-money-needed-for-cyber-security>.

Panda Security, An attack with the new LockerGoga ransomware in Norway, Panda Security, 2019, viewed 05/04/2021,

<https://www.pandasecurity.com/en/mediacenter/news/lockergoga-ransomware-norway/>.