Integral Industrial Cyber-Security,

a target operating model

Name: Erwin Bos
Student number: S1789813

Institution: Cyber Security Academy, The Hague
Submission date: 12 January 2018

1st Supervisor: Prof. dr. ir. J. van den Berg
2nd Supervisor: Drs. D. de Geus

ABSTRACT

Industrial environments are undergoing a digital transformation known by the concept of Industry 4.0. Production facilities, machinery, the internet of things, cloud services and corporate information systems merge in the form of cyber-physical systems. With the new opportunities and challenges that arise, so are new security risks introduced due cross sector hyper-connectivity. While each component of a cyber-physical system can be secure in isolation, real live examples, such as Stuxnet and the Wanna-cry ransomware attack are a powerful reminder of the (new) risks we face which can't be dealt with in a silo'd approach. This thesis supports manufacturers with managing the security risks which arise, by the design of a target operating model to integrally govern security, and to bridge the strategic security intend of manufacturers with daily security operations. The presented target operating model addresses identified challenges by embedding a governance body on a strategic level, and a management body at the tactical level with a clear distinguish between process and hierarchal accountabilities/responsibilities. Within the presented model, the core of the daily security operations exists of a single process based approach, build around the security of endpoints, communication & connectivity, and data. Finally, the model presents the configuration of a single headed overarching security organisation, supported by information systems, trusted suppliers and partners, utilised locations and the capability to measure and report on progress.

ACKNOWLEDGEMENT

The process of this thesis is a textbook example of the expression that it's not only about the destination but moreover about the journey. I experienced this journey as an interesting and meaningful contribution from the beginning till the end. But, I couldn't complete this journey without the support of many. First of all, I would like to thank my supervisors Jan van den Berg and Dennis de Geus for their support. Next to the lecturers of the Cyber Security Academy, I would like to express my appreciation to Mireille Snels (Tutor) and supporting staff for their assistance during this journey. While written independently from my employer, I could also not have complete this thesis without his support. I'm also grateful for the support and feedback received from my colleagues, and those who participated in the interviews. Knowledge and experience needs to be shared, therefore a special thanks to my fellow students for the meaningful discussions and giving an insight in their experiences. Last but not least, I would like to acknowledge the support, endless patience, and acceptance for not being there from those I care most.

1. INTRODUCTION

1.1. BACKGROUND

The first industrial revolution was triggered around 1800 by the Scottish engineer J. Watt, who improved the steam-engine by using less resources and delivering more power. Steam-powered machines entered the factories and a new era had begun. In the late 1800s, the second industrial revolution took place by the introduction of multiple new technologies including electricity, moving production lines and mass production. As the industrialisation evolved, business grew, competition increased, the capital assets of the upper class increased, and the middle class emerged.

From the 1970s onwards electronics and Information Technology (IT) made their entrance to automate production lines and digitise manufacturing. In today's manufacturing environment electronics evolved to Programmable logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA) systems, or for example Industrial Control Systems (ICS). These type systems are all around us, from controlling our water supply, bridges and waterways until delivering our baggage at the arrival hall at the airport. These systems have become common good to monitor and control (industrial)processes and their supporting equipment. Also information systems with software providing capabilities for resource management, quality control, data analytics or computer aided design have become default in the manufacturing space. Besides manufacturing as a whole, the products manufactured have also become digital, from the toothbrush with position monitoring that interact with our smartphones to magnetic resonance imaging (MRI) scanners at medical facilities which utilises cloud based environments, where clinical data send by medical equipment from all over the world is collected, stored and analysed.

Where the early industrial revolutions led to an increased incentive for safety and security in general, the introduction of electronics and IT within manufacturing, introduced in their turn additional disciplines of security [1]:

- Product Security, aimed at building and delivering safe and secure products;
- ICS Security, aimed at the correct and undisturbed functioning of equipment and machines;
- Information Security, aimed at protecting corporate information and resources.

Over time these three disciplines of security have evolved. Nowadays often the term Cybersecurity is used, incorporating these three disciplines together with other areas of interest. As technology progresses, ICS, corporate information systems and commercial products becomes interconnected. This interconnectivity has not only changed manufacturing or industry operations, but also the security risks faced. More connected operations create more potential entrance points for security threats, whereas the risks can be physical, digital, internal or external, malicious or unintentional [2]. Security is as strong as it weakest link, to this end, in stead of isolation, managing the security threats among multiple disciplines within manufacturing, requires an integrated approach [3].

1.2. THE FOURTH INDUSTRIAL REVOLUTION

Nowadays the interconnectivity between products and systems within manufacturing is transcended by connectivity throughout the internet. In addition, the introduction of the Internet of Things (IoT) and Cloud related services within manufacturing creates a new revolution: the fourth industrial revolution, often referred as Industry 4.0, Industrial Internet of Things or Smart Factories. Within this concept machinery parts will monitor and evaluate their own performance and, if applicable, be able to order their own spare parts. By real-time, cloud based, data analytics safety and efficiency increases at the factory floor, and beyond. Production facilities, machinery, IOT, cloud services and corporate information systems will merge in the form of Cyber-Physical Systems (CPS). These systems will blur the line between physical and digital and will be capable of autonomously exchange information, triggering activities and controlling each other independently [4].

Whereas inter-company connectivity already increased the security risks due the number of entrance points, CPS are globally connected, throughout the public internet, across multiple stakeholders within end-to-end supply chains. Whereas the need for security within the area of information systems, professional and commercial products, ICS and already within CPS is apparent, the problem is often that security of these areas is governed in silos, without a cohesive approach or overview [3, 5].

1.3. INDUSTRIAL SECURITY RELEVANCE

While the up-come of CPS in manufacturing increases, research among 100 largest U.S. manufacturers in fabricated metal, food processing, machinery, plastic and rubber, and transportation equipment sectors in 2017, identified that 96% of manufacturers see security of CPS as one of the top risks [6]. One of the earlier examples of a security breach in the area of merged ICS and IT dates from 2000. A consultant, on a water project at Maroochydore in Queensland Australia was refused a full-time job. The consultant obtained, via the wireless network, access to the control systems and managed to release one million litres of sewage into the river and coastal waters. Besides an estimated financial impact above $1.0 million dollars, there was a significant environmental impact as over 500 meters of open drain in a residential area was polluted, and flowed into a tidal canal. More recent in 2014, Georgia-Pacific, a tissue and paper towel company with approximately 35.000 employees and 200 facilities was hacked by a former system administrator. The former administrator maintained its secured remote network connection and was able to reach ICS of a production facility. The attack lasted for 14 days and caused around $1.1 million dollars in damage [7]. Probably more familiar to the general public are the notorious Stuxnet virus and the Wanna-cry ransomware attack. The former, although designed sophisticatedly, attacked computer controls within a nuclear facility through a combination of ICS and IT. Next to environmental risks, it could have placed an entire society at risk [8]. Wanna-cry, the latter, demonstrated how important it is to get security out of the silo'd approach. The ransomware affected not only personal computers but also for example Point of Sale (POS) systems at large

glossary stores, and Hospitals impacting people's safety as medical devices affected, ambulances were diverted and operations cancelled. These real-life examples are a powerful reminder of the threats and risks we face. The impact of a security breach within CPS not only affect business interests, but might also impacting the environment, society as a whole, or even cause injury or loss of human life.

1.4. RESEARCH APPROACH

1.4.1. Current research efforts on industrial security

The field of industrial security regarding environments where production facilities, machinery, IOT, cloud services and corporate information systems are merged is not novel, as is the field of (business) operating models. Research efforts in the past, regarding industrial security, has focused on the security of the individual aspects in isolation. Although current research applies a more end-to-end approach and considers industrial security as a whole, the artefacts delivered are focused around the frameworks, standards and measures, closely related to the daily security operations. Besides an academic lecture on security governance [9], operating models for industrial security, which incorporate the bridge between strategy and daily operations, are not found. Available related work, and theoretical frameworks on the individual aspects, where applicable or of influence, are discussed throughout the dedicated chapters within this research study.

1.4.2. Research goals and deliverable

The goal of this research is to support manufacturers with managing the security risks that arise with CPS within the concept of the fourth industrial revolution. As there is gap in the availability of artefacts to bridge a firm's strategy and daily security operations, this research delivered a operating model to integrally govern security, incorporating the main areas of attention, such as but not limited to: information security, product security or for example physical security.

1.4.3. Research questions

To develop a operating model, the following questions are asked:

1. What is a cyber-physical system?
2. What is the security challenge within a cyber-physical system?
3. What are the design requirements to address the security challenge identified in previous questions?
4. How can can a target operating model address the identified security challenge within in a cyber physical system
5. Taken the previous questions into account, what could a target operating model for cyber-physical security looks like?
6. Does the developed target operating model supports manufacturers with managing the security risks that arise with CPS within the concept of the fourth industrial revolution?

1.4.4. Research scope

This research is aimed to support manufacturers with managing the security risks which arise among the seamless integration of hardware, software and networking capabilities to sense and control physical components in their support of manufacturing tangible goods [4]. These end-to-end, global interconnected systems are the foundation of CPS within the concept of the fourth industrial revolution. Manufacturers come in many varieties and shapes, each with its own products, services and characteristics. The impact of a security breach within CPS, besides the general business interests of manufacturers, could also impact aspects such as environment, society, or cause injury or loss of human life [4]. As such, in case during this research study a reference manufacturer is required, a breach in the security at this reference manufacturer should therefore have also (potential) impact at all aspects, such as peoples health or safety. To this end, as a reference, a (virtual) manufacturer is chosen within the sector of medical devices.

Development of security controls in support of security risks regarding CPS are excluded. Finally, the development of an implementation approach, or the implementation of the actual developed target operating model are out of scope as well of this research.

1.4.5. Research methodology

The methodology for research is aligned to the 'Design Science Framework' within the discipline of Information Systems [10]. Within this discipline, the framework enables the development and evaluation of artefacts aimed at to solving identified organisational problems.

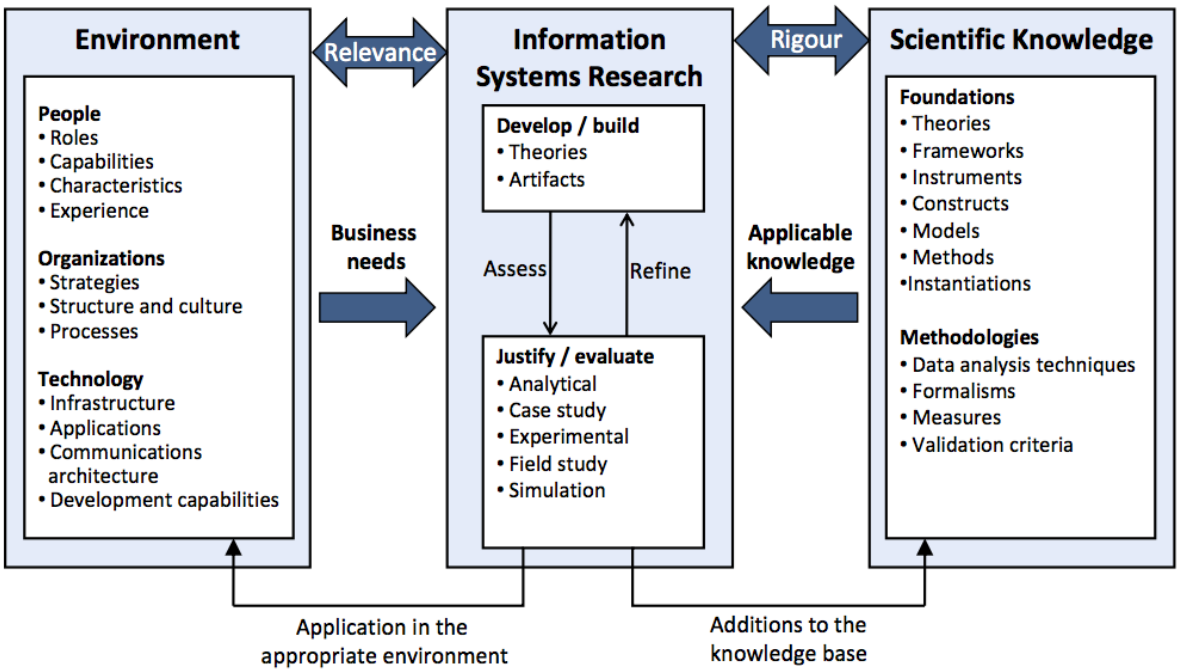

Figure 1: Design Science Framework by Hevner [10].

This research originated by an organisational problem whereby a gap resided in the availability of artefacts in support of resolving it. First of all, the environment wherein the problem remained was identified and analysed. Taking into account the technology, organisation, and people aspects, the main challenge was identified. Next after assuring that the gap in available artefacts was still present, and thereby the research remained relevant, the business needs or design requirements were identified. This took place by means of interviews with industry experts, combined with analysis of existing academic research, frameworks, models, and methods. Next the artefact, to solve the identified problem, was developed which resulted into a preliminary model. For this, the earlier analysed theories, framework etc. were synthesised and applied. Next, the developed artefact was refined based upon an analysis and assessment of the coherence and compliance of the artefact to the identified requirements. Refinement itself took place by applying additional models and methods, which resulted into the final artefact. Finally, the developed artefact is evaluated and recommendations for follow-up are made.

The presentation of this research is aimed at an audience at the tactical and strategic level which are familiar with elements like mission, vision, strategy, and operating models to achieve these elements.

1.5. OUTLINE OF THIS THESIS

For this thesis the following outline has been applied: By this chapter, chapter one, the main topic “Industrial Security” is introduced together with the relevance of this research, its goals, deliverables and the methodology applied. By chapter two the phenomenon of cyber-physical systems is discussed including its challenges with regards to security. Within chapter three the main design requirements are identified to coop with the security challenges faced within cyber-physical systems. Within chapter four a preliminary model is presented, followed by the design of a more extensive model in chapter five. Within chapter six reflection takes place on research contribution and the application of the model, followed by conclusion and recommendations.

2. CYBER PHYSICAL SYSTEMS (CPS)

2.1. INTRODUCTION

Within traditional manufacturing environments, machinery process raw materials to components or end-products. A CPS is based upon combining machinery, which today includes electronics and computation power, with physical actions and processes in the real world. Within the concept of Industry 4.0, these kind of machinery within a production line, production lines within a factory, factories within a supply chain, and supply chains among sectors become integrated and interconnected [11].

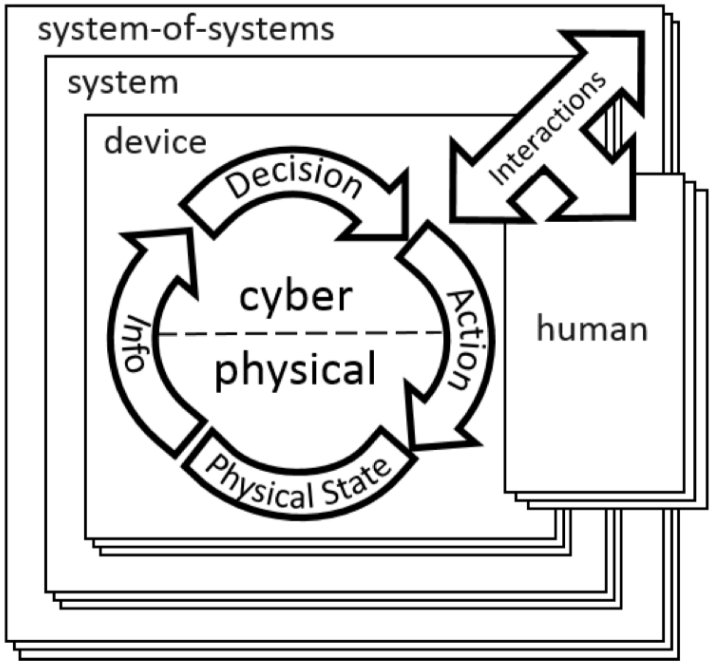

Figure 2: Conceptual model of a cyber-physical system [12].

A concept model of a CPS is visualised in figure 2. The CPS can be an individual device interacting with its environment, or consist of multiple interacting devices forming a system. Multiple systems, in their turn, forms a system of systems (SoS) which can also be applied recursive. For the remainder of this thesis the following definition of a CPS is applied [12]:

"*Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfil time-sensitive functions with varying degrees of interaction with the environment, including human interaction.*"

2.2. INTEGRATION OF CYBER-PHYSICAL SYSTEMS

2.2.1. Vertical integration

In the run-up to a deployment of CPS across multiple supply chains and multiple sectors, today CPS often remain, due to the novelty and as such its maturity, within the borders of a factory or company. Here, CPS are characterised by a vertical integration of heterogeneous components.

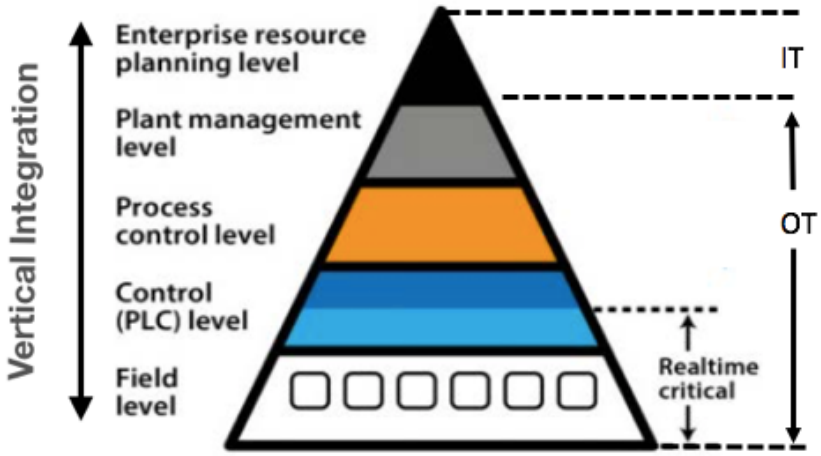

Figure 3: Vertical integration of a cyber-physical system [53].

At the lowest level, the field level, remains the sensors and actuators which interact with the physical world. These sensors and actuators are in their turn controlled (remotely) by Programmable Logic Controllers (PLC). Supervisory, Control & Data Acquisition (SCADA) systems visualises and manages the production processes, whereas Manufacturing Execution Systems (MES) support in managing all operations at plant level. These systems combined are often referred as Industrial Control Systems (ICS) or Operational Technology (OT). The security of OT is aimed at the correct and undisturbed functioning of equipment and machines [1]. At the highest level the planning and logistics of the entire organisation takes place by Enterprise Resource Planning (ERP) systems. These systems are often referred as Information Technology (IT) and also includes systems supporting sales, human resources or for example finance. Here the priority of security is not the undisturbed functioning but moreover aimed at protecting of the confidentiality and integrity of corporate information and resources [1, 13]. An overview of the main differences between IT and OT, which influences the security priorities, is presented in table 2.

Table 1: Overview of difference between IT & OT, based upon [13]

Information Technology & Operational Technology		
Category	IT Systems	OT Systems
Performance requirements	Response must be consistent	Response is time critical
	Strict requirements for throughput	Average throughput is acceptable
	Delay and fluctuations may be acceptable	Delay and fluctuations are not acceptable.
Availability requirements	Restart is acceptable	Restart is not acceptable due to the availability requirements of industrial processes
	Deviation from availability can be tolerated depending on the requirements.	Unavailability needs to be scheduled days or week in advance
Risk management	Confidentiality and Integrity has highest priority	Safety and security of people and assets are most important.
	Fault tolerance is less important, highest risk relates to disruption of business operations	Fault tolerance is critical, even a minor disruption can be unacceptable.Main risk is loss of life, equipment and production capacity
Time criticality	Less critical with interaction during emergencies	Reaction on human interference is crucial
	Access to system resources can be limited and management on the required level.	Access must be controlled strictly and not interfere the interaction between human and machine
Exploitation and changes	Used with default operating systems	Operating systems are device specific
	Upgrading or changes are manageable and routine activity for a system manager.	Upgrading or changes requires a stepped approach involving many stakeholders across the chain.
Resource Limitation	Enough resource available to support application of third-parties for additional functionality	Resources are exactly sized for the original function to be carried out
Communication	Default communication protocols	Many patented private communication protocols
	Mainly cable networks and local wireless networks	Multiple type of networks including radio, satellite or for example Infrared
	Networks typically build on application of IT technology	Network are complex and require specific technical knowledge of the devices used.
Support	Many different support organisations available	Limited variety of support organisations available
Life-cycle	Short life cycle (3-5 years)	Life-cycle between 15-20 years

2.2.2. Horizontal integration

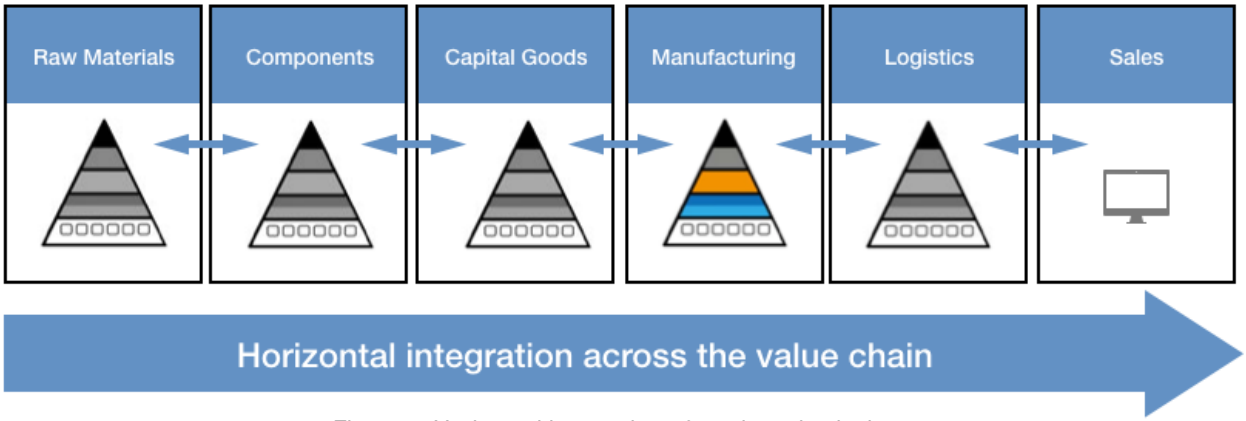

Figure 4: Horizontal integration of a cyber-physical system.

By horizontal integration a CPS transcends the manufacturing walls. Predictive or real time sales within the upstream supply chain can trigger a CPS downstream. The CPS within the manufacturing environment is directed to start the production of tangible (consumer) assets. Based upon the customer demand, the configuration of the CPS within the manufacturing environment can be adapted instantly. As the configuration of the products to produce can differ, this may require different raw materials or multiple components. Based upon available (onsite) stock the CPS within manufacturing can trigger a downstream CPS to process raw materials, which in return can trigger logistics to assure transport of the materials. This horizontal integration, upstream and downstream, of individual or multiple CPS takes place across singe and multiple supply chains among different sectors, creating a complex network. The majority of the horizontal integration takes place at the business level where ERP systems, belonging to the IT domain, exchanges information. Until recently, before the rise and adoption of cloud computing, these systems exchanged information often through private, Internet Protocol (IP) based, networks. The technologies, policies and practices used to protect the ERP systems could also be applied to their networks and interfaces in support of information exchange [14].

2.2.3. Lateral integration

Lateral integration of CPS reflects the concept of Industry 4.0 today. The classical architecture of horizontal systems is replaced by distributed manufacturing services and embedded intelligence at every layer, being horizontal and vertical.

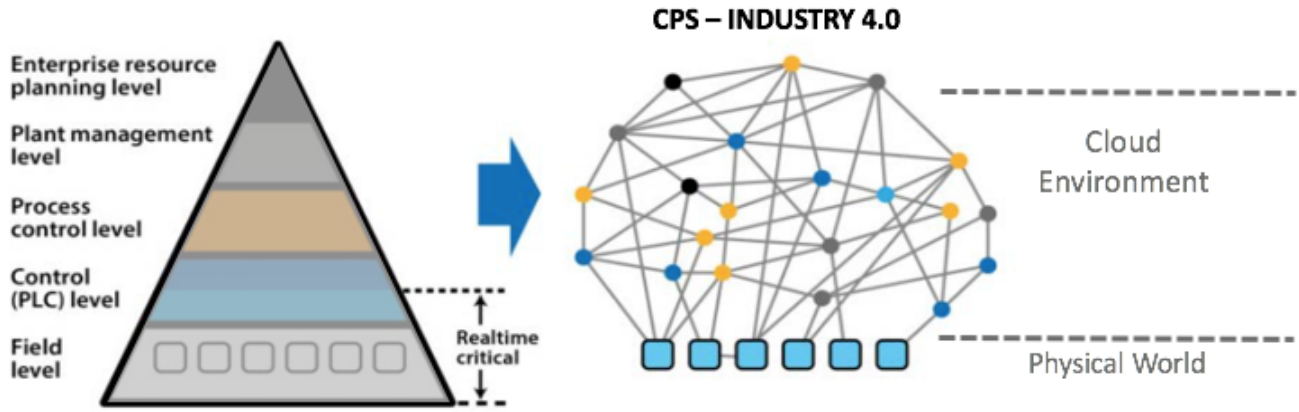

Figure 5: Lateral integration of a cyber-physical system, based upon [53].

Distributed manufacturing services are enabled by the introduction of cloud based computing. Cloud based computing “is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [15]". Intelligence is embedded not only by adding sensors and actuators to machinery within the factory, but within all kind of devices throughout the supply-chain including the end product being fabricated.

At the lowest level, the control level a distinguish can be made between two parts. The first part entails physical control layer which consist of common PLC’s. Due criticality and timing of the feedback loops as such, this layer remains close to the actual the sensors and actuators at the physical layer. The second part of the control level, which controls, with reduced performance the lower level, is brought to a cloud environment [16]. The upper levels, starting from the process level all the way to the enterprise level, still exists but are also all being brought to cloud environments where communication takes places by (multiple) public networks. In addition the products to be manufactured are, during their operational life-cycle, connected to the same cloud platforms creating a complex network of networks, and a complex system of systems.

“Within the concept of Industry 4.0 realtime critical components remain at the physical layer. All other layers from the less critical control level layer until the enterprise level are all brought to a cloud environment.”

2.3. GENERAL SECURITY OF CYBER-PHYSICAL SYSTEMS

Predictions are that the number of connected devices within enterprises, government and infrastructure will, on an average, more than triple the upcoming three years at a compound annual growth rate of around 10% [17]. The emerging hyper-connectivity across machinery, networks, cloud environments and applications increases the vulnerabilities and threats for malicious attacks exponentially [18].

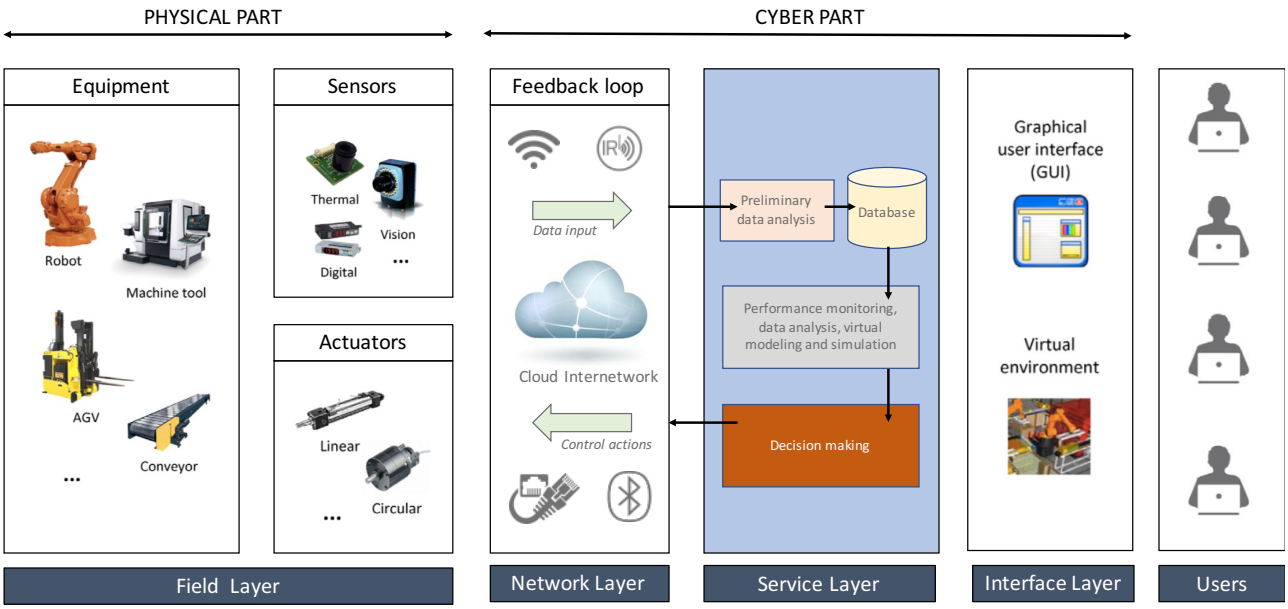

Figure 6: Architecture of a cyber-physical system within a manufacturing firm, based upon [62].

Previous chapter showed that the classical architecture of CPS ,existing of OT and IT, is replaced by distributed manufacturing services and embedded intelligence. Figure 6 visualises this new architecture within a general manufacturing environment. Only the parts that are time critical remain at the (physical) field layer. The remaining parts of the control systems (OT) and the enterprise systems (IT) merge into cloud environments.

2.3.1. Security and its adversaries

Whether it's physical security, information security or for example OT security, we tend to address risk with proactive, preventive and repressive (reactive) measures. Although often passed, the first step is to consider who the adversaries or actors might be. In general we have the random attackers and insiders but who are specifically targeting the cyber-physical systems [19]? Having this insight would refine the specific systems or architectural layers at risk and support strategy development, assignment of resources and priorities. The following paragraphs will discuss the security of each architectural layer independently, regardless of its the adversary or actor.

2.3.2. Security at the field layer

The security challenge starts at the lowest level of equipment, sensors and actuators. Here, chips and electronics are used which can originate from multiple vendors across the world. These parts are, from a security perspective other than within the health and safety domain, not regulated. Today there is for example no regulation against hard coded usernames and default weak passwords. The security challenge at this layer can be divided into two levels [20]:

1. "The equipment level: physical security protection, access control, authentication, nonrepudiation, confidentiality, integrity, availability, and privacy.
2. The actuator and sensing level: confidentiality, data source authentication, device authentication, integrity, and availability."

2.3.3. Security at the network layer

The network layer connects all systems and layers together through multiple means. Not only provide the network layer connectivity within the individual CPS, but it can also connects multiple CPS cross sector. According to research by [20] the main security challenges within this layer are:

- "Overall security requirements, including confidentiality, integrity, availability, privacy protection, authentication, group authentication, keys protection, etc.;
- Privacy leakage: Since some devices are physically located in untrusted places, which cause potential risks for attackers to physically find the privacy information such as user identification, etc.;
- Communication security: It involves the integrity and confidentiality of signalling in communications;
- Over-connected: The over-connected device may run risk of losing control of the user. Two security concerns may be caused: (1) DoS attack, the bandwidth required by signalling authentication can cause network congestion and further cause DoS; (2) Keys security, for the over-connected network, the keys operations could cause heavy network resources consumption;
- MITM attack: The attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the attacker controls the entire conversation, and
- Fake network messages: Attackers could create fake signalling to isolate/misoperate the devices from the CPS."

2.3.4. Security at the service layer

Within this layer information exchange between multiple cps is provisioned, data is being stored and processed in support of automated decision making. It's at this layer where the traditional OT and IT systems reside. The security requirements here are [20]:

- "Authorisation, service authentication, group authentication, privacy protection, integrity, security of keys, nonrepudiation, anti-replay, availability, etc.;
- Privacy leakage. The main concern in this layer involves privacy leakage and malicious location tracking;
- Service abuses. In CPS the service abuse attack involves: (i) illegal abuse of services; (ii) abuse of unsubscribed services;
- Node identify masquerade;
- DoS attack;
- Replay attack, the attacker resends the data;
- Service information sniffer and manipulation, and
- Repudiation in service layer, it includes the communication repudiation and services repudiation."

2.3.5. Security at the Interface and user layer

The Interface layer bridges the CPS with its users. Although the security challenges depends on the application within the service layer, the basic security requirements within this layer are related to [20]:

- Physically security protection;
- Access Control;
- Confidentiality;
- Data integrity;
- Availability;
- Authentication, and
- Non-repudiation.

2.4. MAIN SECURITY CHALLENGE OF CYBER-PHYSICAL SYSTEMS

Historically, security of each layer within a cyber-physical system is dealt with as a silo of concern. For each layer of concern multiple standards and best practices are available to address the identified security requirements. Next to the process of manufacturing itself, other business processes, like supply-chain management or products life-cycle management also become digital and integrates with the same cloud environment as the cyber-physical systems. And in addition, also the products to be manufactured becomes digital, and forms a cyber-physical system of its own, resulting into a hyper-connected, complex system of systems. With a mix of systems consisting of cloud environments and networks build upon landlines, low power wireless, infrared, cellular and for example satellite, the challenge is to protect all data streams which could affect confidentiality of business information as well as critical information about equipment control [18]. Next,

CPS generates a large amount of data which combined with cloud technologies and so-called big data analytics can provide new insights and opportunities. One opportunity already identified and applied is the application of predictive maintenance. Making all this data cross sector available for search and analysis will limit for example encryption capabilities, and in return present multiple threats to data at rest and in transit.

Hyper-connectivity causes many interfaces between layers of machinery, networks, cloud environments and applications. While each layer can be secure in isolation, challenge within cyber-physical systems for manufacturing environments is the security of all the interfaces between the layers, across the cyber physical chain.

Although having each layer secure in isolation, and supported by interview findings which are further elaborated in paragraph 3.2, the main challenge here is not the interface itself, but arise with the governance of security across the entire cyber physical chain.

3. DESIGN REQUIREMENTS

3.1. INTRODUCTION

Previous chapter identified that by means of lateral integration the majority of what constitute a cyber-physical system is brought to (public) cloud environments, which causes cross sector hyper-connectivity between networks and systems. The emerge of this hyper-connectivity brings many interfaces between machinery, networks, cloud environments and applications.This hyper-connectivity introduces new threats and vulnerabilities across the cyber-physical chain.

3.2. INTERVIEWS ON REQUIREMENTS

In addition to the literature review and an analyses of real live examples, interviews were held with content matter experts, each having their background in one or multiple areas of cyber-physical systems. To assure that every expert could elaborate on their own area of expertise, use was being made of semi-structures interviews. Additional information on the interviewees and the questions can be found in appendix A. After introduction of the topic the interviewees were asked, with respect to their area of attention within cyber-physical systems, about their challenges and dependencies. The majority mentioned, either directly or indirectly, the notion of end-to-end governance and management of the elements that constitute a cyber-physical system. The interviewees confirmed the finding in previous chapter that managing the security of the individual layers or silos is not a main challenge. **The main challenge regarding the security of the interfaces in-between, concerns governance in relation to accountability and responsibility, as these are either unclear, or if addressed, the interest doesn't match the interest from all stakeholders.** By asking questions to the manner in which governance and management currently takes place, or should be organised, the interviewees referred to the application of unified methods supported by standards, and coordination between the different layers. Although application of unified methods and coordination in-between could be beneficial, this doesn't mean that the security of cyber-physical systems is being brought out of its silo'd approach. Recent example such as the Wanna-cry ransomeware attack demonstrated the need for governance from an end-to-end perspective, as systems were compromised while security of the individual components and layers was in place. Requirement to take into account is that security shouldn't be the sum of the individual layers, but rather the result of an end-to-end approach.

3.2.1. An end-to-end approach

An end-to-end approach sound legit, but what does it entails? End-to-end can take a number of forms. It can be addressed horizontally from a stakeholder perspective where (I)component builders provide hardware, software and services, (II)System builders integrate the components, and (III)the operational users who uses the systems for its intended purpose[4]. From a vertical layered perspective, end-to-end encompasses the lateral integration of the physical world and the technology used e.g. from the sensors and actuators up till the layer of cloud-based services, applications and all interfaces in

between. Through a third lens, end-to-end can be approached from the perspective of the product life-cycle of a cyber-physical system, starting with research and design, sourcing, make, distribute, service and end-of-life. Within an integrated environment neither of these viewpoints can be ruled-out, and one is not more important than the other, although, the perspective of layers and its interfaces in-between is more dominant, with regards to the identified security challenge of cyber-physical systems. After all, cyber-physical systems are a merger of existing elements where the majority of security aspects, in isolation, are already addressed. End-to-end, to this matter, will be approached horizontally, from the perspective of layers and their interface in-between.

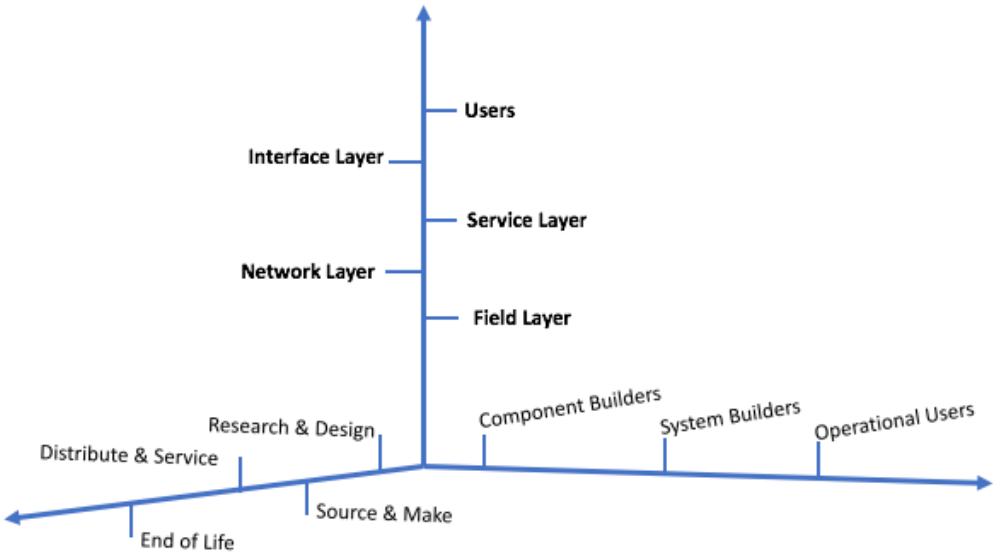

Figure 7: Different axes to approach end-to-end security of a cyber-physical system.

Having defined an end-to-end approach doesn't mean the other identified viewpoints are out of scope. By applying synthesis, a distinction can be made between a technical perspective and a socio-technical perspective. The technical perspective entails all the technology components used during the life cycle, individually and as a whole. The socio-technical perspective entails the interaction between all (human)actors, storage & data processing systems and the machinery. These two perspectives align with the work of [21], who developed a layered model to address the topic of cybersecurity. Within this work the authors [21] identified a third layer on top: The governance layer, which corresponds to the main requirement of governance and management by the interviewees.

Development of security controls in support of security risks and requirements, as identified in chapter two are out of scope of this research, though described in detail in the work of [22]. Nevertheless, when designing an operating model the technical perspective and socio-technical perspective needs to be addressed. The following chapter will focus on identifying the requirements of the main challenge, being end-to-end governance & management.

3.3. REQUIREMENTS FOR GOVERNANCE AND MANAGEMENT

Governance is also a term that is used broadly and has many definitions depending on the content in which it's being used. With regards to this research the scope is set in support of manufacturing firms. Within a firm, governance, also known as enterprise governance , can be defined as [23]:

"The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly"

Here, enterprise governance entails a framework of two areas. The first area relates to corporate governance which addresses items such as oversight, roles, control assurance and risk management. The second area is about business governance, and is focussed around items like strategy, value creation and resource utilisation [23].

3.3.1. Governance of cyber-physical system security

The security challenge of cyber-physical systems, including its governance, is widely recognised [3, 5], whereas the availability of artefacts for the governance of security within cyber-physical systems lags this insight. Academic endeavours addresses either cyber-physical systems and the concept of industry 4.0 as a whole, or addresses the governance of information technology in general [24]. In the research study "IT governance for Cyber-Physical Systems: The case of Industry 4.0" the authors reviews the implications of cyber-physical systems on the governance of information technology, but no applicable model, specific for cyber-physical systems or dedicated to security, is discussed [24]. On a conceptual level, the authors do make a reference to an existing framework for the governance of information technology, being COBIT 5. This framework, together with the standards and frameworks listed below are, based upon the interviews with subject matter experts, the most mentioned and applied artefacts for governing security in relation to technology in general:

- ISO38500
- ISO 27001, ISO 27014
- NIST Framework for Cybersecurity

3.3.2. Applied governance standards explained

In the absence of dedicated artefacts, the listed standard and frameworks above, including COBIT 5, will be discussed. These are for now the best available and moreover applied practices for governance from a technology and security perspective.

ISO 38500

This standard, fully written “ISO/IEC 38500, Information Technology - Governance of IT for the organisation” is published by the International Organisation for Standardization (ISO) and the International Elctrotechnical Commission (IEC). The objective of this standard is defined as “to provide principles, definitions, and a model for governing bodies to use when evaluating, directing, and monitoring the use of information technology” [25]. Based upon this objective, key elements of governance to take into consideration of this research are: evaluating, directing and monitoring. These elements are also the foundation whereupon the ISO governance model is build.

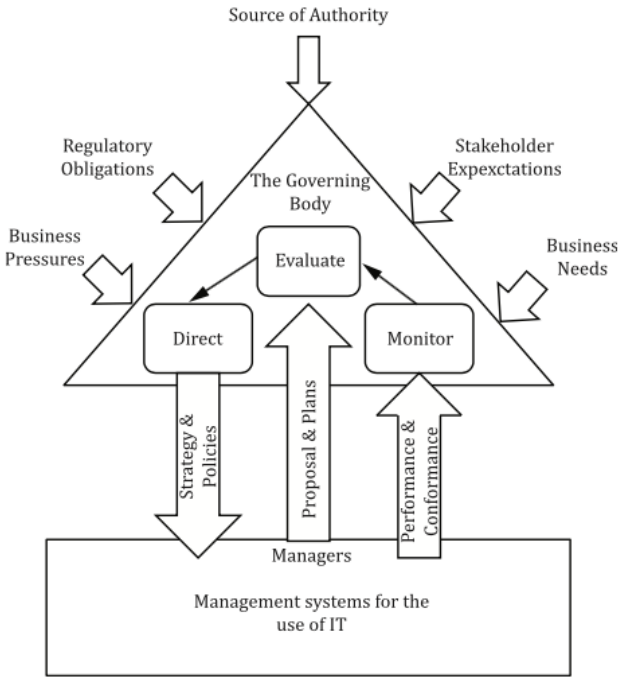

Figure 8: ISO38500 Governance model for IT [25].

Here, evaluation is concerned about the current and future state of information technology. It includes plans, proposals, and arrangement of supplies, while taking the business needs and interested parties into account. Directing is about providing guidance and assign responsibility for the implementation of information technology strategies and policies. Monitoring in the end, is related to review the performance by appropriate measurement. Governance is defined by the ISO as a system of directing and controlling, and governance of information technology as “the system by which the current and future use of information technology is directed and controlled” [25]. Finally, the standard provides six principles of preferred behaviour to apply when evaluating, directing and monitoring:

1. Responsibility;
2. Strategy;
3. Acquisition;
4. Performance;
5. Conformance, and
6. Human Behaviour.

For each statement the standard provide a description of what should happen, but the answer on the question how, when or whom is not addressed within the standard.

COBIT 5

The Information Systems Audit and Control Association (ISACA) publishes the COBIT 5 framework, where COBIT stands for Control Objectives for Information and related Technology. ISACA defines governance as “Ensuring that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives” [26]. Governance within COBIT is based upon five principles [27]:

1. Meeting stakeholder needs;
2. Covering the enterprise end-to-end;
3. Applying a single integrated framework;
4. Enabling a holistic approach, and
5. Separating governance from management.

Meeting the stakeholders need is about creating value, an element which we also identified within business governance, and the evaluation task within the ISO38500. The second enabler, covering the enterprise end-to-end is the aspect that governance shouldn’t be addressed in sole isolation but aligned to, and in support of other governance domains. This means for example that governance should not only address information security, product security or security of operational technology, as well that it should also align with enterprise governance, business governance, financial governance or other processes within the organisation. A Single Integrated Framework, principle 3, refers to the fact that COBIT is aligned to other standards and framework. In practise this means the standards for information technology like ISO2700, ITIL or TOGAF can be used in combination with COBIT. Here COBIT can be used as an overarching approach. Principle four, a holistic approach is aimed at taking into account multiple interacting components. To this end ISACA has defined seven categories of enablers [27]:

1. Principles, policies and frameworks;
2. Processes;
3. Organisational structures;
4. Culture, ethics and behaviour;
5. Information;
6. Services, infrastructure and application, and
7. People, skills and competencies.

Lastly, presented in figure 9, COBIT identifies, as within ISO 38500, the elements of evaluation, directing and monitoring. In addition it also advocates for a management layer, but deliberately splits this layer from the governance layer. The management layer is focussing on Planning, Building, Running and Monitoring, and provides and end-to-end coverage. Planning within this concept entails the Alignment, planning and organisation of information technology, building is also covering the acquirement and implementation, running is hereabout delivery, service and support of information technology, and lastly monitoring incorporates evaluation and assessment.

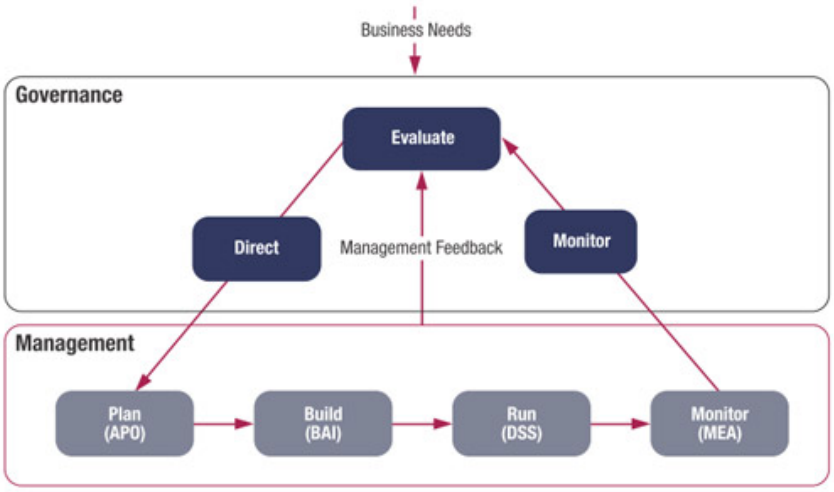

Figure 9: COBIT Layered governance model for IT [27].

ISO27001 and ISO27014

These standards are, as the ISO38500, also published by the ISO and IEC organisation. The ISO27001 is a standard which describes a process-based approached to assure the confidentiality, integrity and availability of information. This standard is part of a series of standards, known as the ISO27000 series. Each standard within this series addresses a specific topic. While governance is part of the ISO27001, the ISO27014 is dedicated to the topic governance. As such for this research the focus will be on the ISO27014. The full name of this standard is “Information technology - Security techniques - Governance of information security”. The definition of governance is aligned to the earlier definitions identified: “Governance of information security is a system by which an organisations’s information security activities are directed and controlled” [28]. The objectives of information security governance are build around three building blocks:

1. Strategic alignment;
2. Value delivery, and
3. Accountability.

The first, strategic alignment is about aligning the business objectives and its strategy with the strategy and objectives of information security. Value delivery concerns delivering value to (a)the governing body, and (b)to its stakeholders. Accountability entails ensuring that information risk is being adequately addressed [28]. To govern information security, the governing body performs exact the same activities as identified before: evaluate,

direct and monitor. These activities together with the following six principles form the governance of information security throughout this standard [28]:

1. Establish organisation wide information security;
2. Adopt a risk based approach;
3. Set the direction of investment decisions;
4. Ensure conformance with internal and external requirements;
5. Foster a security-positive environment, and
6. Review performance in relation to business outcomes.

For each of these principles the standard provides a short description of what should be undertaken.

NIST framework for cyber-security

NIST is the National Institute of Standards and Technology within the United States. The framework for cyber-security provides an approach for managing security risks within an organisation. To this end it's the opposite of e.g. the COBIT Framework which originates from an audit perspective. The NIST framework supports organisations in applying best practices and principles of risk management [29]. The core of the framework is build around five functions:

1. Identify;
2. Protect;
3. Detect;
4. Respond, and
5. Recover.

Identify is focussed on understanding the organisation is support of managing risks related to systems, assets, data and capabilities. Protect is about implementing measures to assure the availability or delivery of critical information technology services. Detect is all around the capability to identify security events. Once detected, respond assures that appropriate action is taken, whereas recover focusses recovering services and providing resilience capabilities. Governance of information security is not a function in itself, rather an outcome of undertaking the "Identify" functionality. In detail, this function is aimed at understanding the context of the organisation, and the resources in support of critical products, services or processes. By identifying related security risks, supports the organisation in providing focus and prioritise efforts, aligned with strategy and business needs. The outcome this function, among others, is governance. Here, governance is defined as[29]: "The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber-security risk". To achieve the outcomes associated with governance, a reference is made to other standards and frameworks, of which the earlier discussed ISO27000 Series and the COBIT 5 framework.

3.3.3. Analysis of applied governance standards

Within all of the discussed standards and frameworks, three main areas of attention keeps reoccur explicitly:

1. Context;
2. Directing, and
3. Monitoring.

The context, or organisational context, is where alignment takes place with the business strategy, the business objectives and the needs of stakeholders. In particular should be noticed that the organisational context is important in all notions, to be able to deliver value to all stakeholders. Here, the value is not limited to a secure environment per se. Directing is the area where direction, or strict guidance, is provided about the derived strategy and objectives for security. In parallel, directing also entails in all examples the proper allocation of resources and prioritisation of activities. The last area found in common, is around monitoring. In additional scientific literature, the area of monitoring is often mentioned together with audit and control. Also through the lens of governance, audit and control is applicable as monitoring is aimed at providing assurance that the derived strategic security objectives are achieved.

Regardless of the topic to be governed, within all, governance is positioned as sub-topic in support of enterprise governance. As such, it remains not in sole isolation but aligns and/or integrates with other business domains that are governed. A distinction can be made between the governing body and the management body. The majority addresses this difference implicit, while the COBIT 5 framework describes this explicit. The governing body determines the “What?” question at the strategic level. It’s here where long-term decisions are taken which also determine the future state. The “How?” question is addressed at the tactical level by the management body (not to be confused with the operational level where daily operations takes place). The management body determines how the strategy and objectives are reached, and addresses topics like processes, coordination and planning. **While having a governance and management body identified, in practise (based upon the interviews) a difference or gap can be discerned between the alignment of the strategic and tactical level.** The original aim of this research is based upon the fact that there is a gap between strategy and daily operations. Within the governance concept, although not excluded, managing is separated from governing, while managing is positioned between strategy and operations. Based upon this finding, for the remainder of this research, the management body and it’s related areas of attention will explicitly be positioned as integral part of governance.

Several of the standards and frameworks addresses multiple principles, which details out preferred behaviour to guide the governance process. While similarities can be identified, for now these are not further analysed as first insights shows that these do not contribute

with regards to aim of this research, but rather support the directing and managing bodies involved. Aside principles, within each standard or framework the notion of scope can be derived. On the highest level four levels of scope can be identified:

1. Organisational;
2. People;
3. Process, and
4. Technology.

“Organisational”, not to be confused with an organisation is the collective name for not only the strategy and objectives themselves, but also entails related policies and derived control frameworks to measure performance and compliance. People relates to the workforce, theirs skill, how they are organised and the culture within. Processes are the procedures and ways activities are undertaken and technology refers to all hardware, software and information in support of managing the security risks, although this does not automatically include the hardware, software and systems that builds up a cyber-physical system.

The findings, on the areas of attention, the levels of directing and controlling, and the levels of scope, are supported by previous research efforts on governance [30]. A consolidated overview of previous research efforts in the field of governance, dedicated to information technology, shows three dimensions with similar elements as identified within previous paragraphs. Based upon the analysis of the governance standards above, aligned to the findings of [30], table 2 provides a consolidated overview of the dimensions and elements, to take into account when developing an operating model.

Table 2: Consolidated overview of elements for governing cyber-physical system security.

Required elements to address in a model for Governing CPS Security		
Dimension	Element	Keywords
Level	Strategic	What, long-term, future state, senior management
	Tactical	How, short-term, middle management
Attention Area	Context	alignment, business objectives, stakeholder, creating value
	Directing	Guidance, prioritisation, allocation
	Monitoring	Audit, control
Scope	Organisational	Policy, strategy, objectives, principles
	People	Workforce, skills, structure, culture
	Process	Procedures and activities
	Technology	Hardware, Software and Information

Based upon the literature study and the findings within this chapter, the following definition for governance of cyber-physical system security is applied for the remainder of this research:

"Governance of cyber-physical system security is the system by which strategic directions and tactical objectives, regarding organisation, people, process and technology are defined, communicated, embedded and controlled; with the goal of managing security risks that arise within the span of cyber-physical systems"

3.4. MAIN DESIGNS REQUIREMENTS

The challenge that arise within the concept of the fourth industrial revolution, is the emerging hyper-connectivity across machinery, networks, cloud environments and applications, which leads to many interfaces in-between. With a traditional silo'd approach, these interfaces remain underexposed. Integrated governance of cyber-physical system security can provide a system with the goal of managing the security risk that arise. Where table 2 provided an overview of the elements to take into account, within table 3 these elements are translated into an easy to use, functional description of the requirements for an operating model, with governance embedded into it.

Table 3: Main design requirements for an operating model for cyber-physical system security.

MAIN DESIGN REQUIREMENTS	
#	**Requirement**
1	The model must take into account the technology components used during the life cycle, individually and as a whole (including the integration of IT and OT).
2	The model must take into account the interaction between all (human)actors, systems and machinery.
3	The model must address the future state of cyber-physical system security.
4	The model must address how this future state is achieved.
5	The model must provide alignment with business objectives, stakeholder, and create value.
6	The model must foresee in providing guidance, prioritisation of activities and allocation of resources.
7	The model must foresee in providing assurance that the derived strategic security objectives are achieved.
8	The model must address policies and derived control frameworks to measure performance and compliance.
9	The model must address the required workforce, their skills and structure.
10	The model must foresee in the processes to manage cyber-physical security.

4. A PRELIMINARY MODEL

Now the main design requirements are known, a preliminary model can be drawn (figure 10). At the base all the identified layers, such as the field layer, network layer, service layer, etc., are found, together with their interfaces in-between, which are represented by the red triangles. Next to these technology oriented layers, the user layer is positioned. The user layer partly covers the requirement for a socio technical layer, as users are only a small part of the actors involved in the interactions with a cyber-physical system. On top of the base level, the required governance aspects are addressed.Governance takes place at a strategic level and at a tactical level. At the strategic level, the governing body (represented by 'A') defines *what* needs to be done by determining the context, aligned to corporate governance and business governance (represented by 'B'). The former, corporate governance, addresses items such as oversight, roles, control assurance and risk management. The latter, business governance, is focussed around items like strategy, value creation and resource utilisation [23]. Subsequently, the governing body 'A' allocate resources, prioritise activities, and controls (direct and monitor) the management body to assure that strategy and objectives are achieved. The management body (represented by 'C') resides at the tactical level. This body determines *how* the strategy and objective are reached (plan, build, run, monitor), and takes into account the organisational, process, people and technology aspects (represented by 'D').

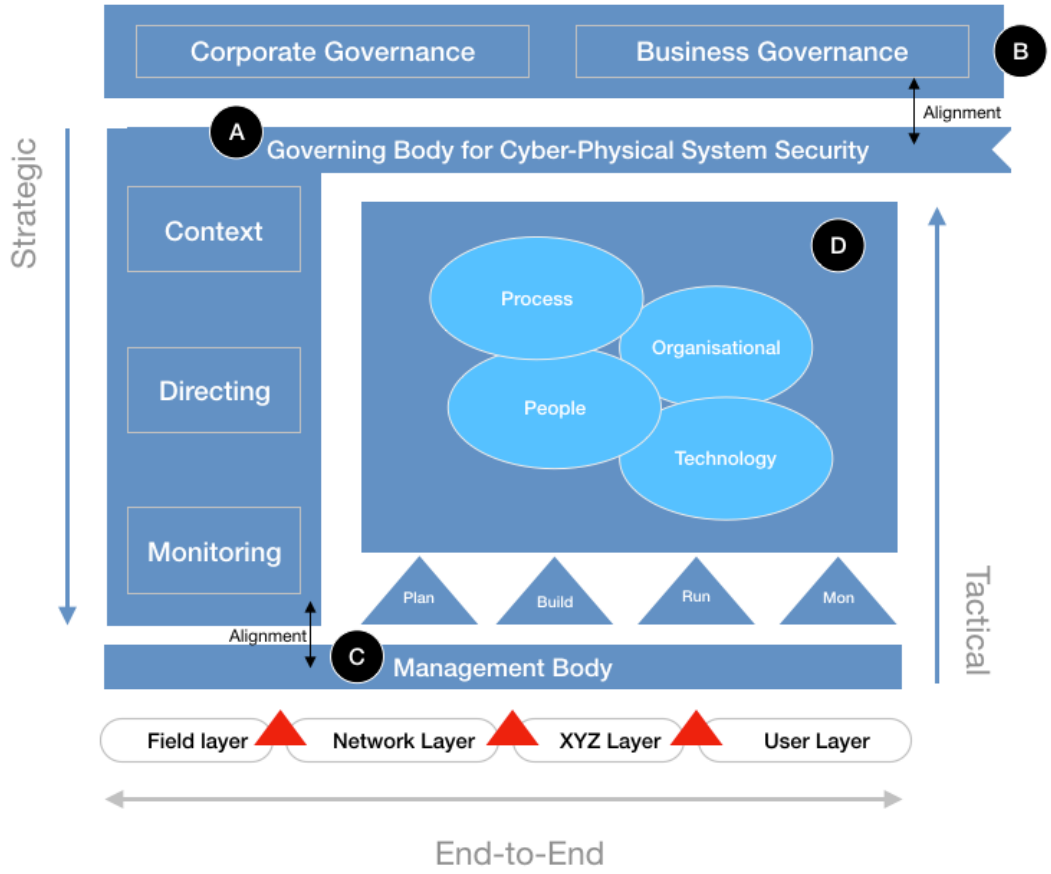

Figure 10: A preliminary model to govern cyber-physical system security.

While this preliminary model takes into account an end-to-end perspective, the alignment with the business, the strategy and objectives (*what*), and *how* these are achieved, the model remains at a high abstraction level and is applicable to various environments. The main identified design requirements are touched, but for example the organisational, process, people and technology aspects are not made explicit, causing a gap between the strategic intent and the security operations related specifically to cyber-physical systems within manufacturing firms. To this end **the model needs to be evolved to an operating model which not only identifies, but also addresses the composition and configuration of all the aspects.**

5. DESIGNING AN OPERATING MODEL

5.1. INTRODUCTION

Models that addresses the composition and configuration of the process, people or for example the organisational perspective, in support of strategy and objectives, are referred as operating models. In support of evolving the preliminary model to a final operating model, the following paragraph will first discuss the concept of operating models.

5.2. OPERATING MODELS

A first survey across literature shows that the term “operating model” or “target operating model” is often used in the same notion as “business model”. When taking a closer look at the term ‘business model’, multiple scientific contributions can be found. Nevertheless, among these contributions there is no unified or accepted definition of the term found. Where a strategy is aimed at reaching a firm’s vision, a business model provides insights in creating and capturing customer value. Where the preliminary model developed in chapter four, demonstrated a gap in the composition and configuration of the process, people, technology and organisational aspects, Blenko, et al (2014) identified five missing elements within business models to convert strategy to results, being: The structure of the organisation, the roles and responsibilities, governance, ways of working and capabilities [31]. In addition, Murphy, et al. (2016) states that an (extended) operating model is required to successfully execute on a firm’s strategy. Their model is based upon four core elements: Design principles, governance, culture and values, and processes [32]. These elements are in return supported by the approach of Martino, et al. (2015) who distinguishes three main models: (I)The business model that describes the area regarding the target customers, (II)The operating model describing (a)the design of the organisation, (b) the processes, (c)Information and technology, and (d)physical assets. Finally, their approach entails people(III). The people model is aimed at development, deployment, and performance management [33]. Based upon the research on operating models and business models, for the remainder of this research, the following definition of a target operating Model is applied:

‘A Target Operating model is a simplified description of interrelated elements of an organisation, such as, but not limited to: technology, processes and people, that are important for executing the strategy in the near future, to successfully deliver the organisations value proposition’.

5.2.1. Place of the target operating model

Joyce and Paquil (2016) introduced a triple layered business model canvas that supports in generating multiple types of business value. This triple layered canvas introduces two new dynamics: horizontal and vertical coherence. At the horizontal level, the value creation can be made more explicit for each value creating flow, and vertically the different types of values are interconnected and aligned [34]. To grasp the relations between business models and target operating models, an overview of these has been drawn (figure 11). The highest level, level 1, positions the business model of an organisation as a whole. It's here where, in the definition of a business model, the rationale is found on how an organisation creates and captures customer value. The second level is hierarchically linked to the first level in support of the overarching business model. Depending on the organisation in scope, at this level the rationale of value creation of a business unit, function or for example department is described. Where at the first and second level use is being made of Osterwalder & Pigneur (2010) business model canvas, the target operating model is positioned at the third level. The third level is more explicit, and details how the key partners, activities and resources support the value proposition at the second level. It is at this level where composition and configuration of the process, people, technology and the organisational aspects are addressed in support of cyber-physical system security.

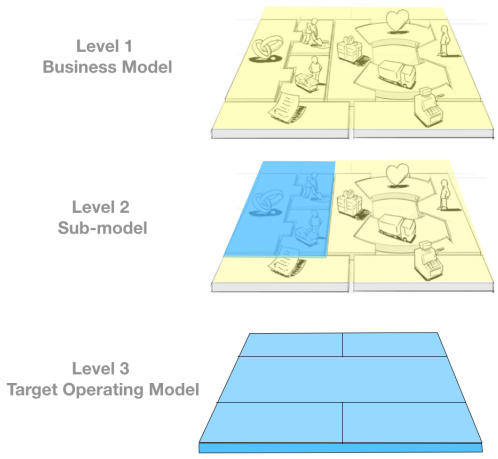

Figure 11: Relation between business models and operating models, based upon [34].

5.2.2. Target operating models for security

Within the body of Scientific Knowledge, artefacts focussing on target operating models, related specific to the concept of Industrial Security and cyber-physical systems have not been found. Interviews with industry experts also didn't identified operating models in this area. The majority of interviewees did mention a general security model provided by The Information Systems Audit and Control Association (ISACA). From a general security viewpoint, a second model could be identified, which is based upon the concept of 'Bimodal IT' [35].

ISACA's business model for information security

The first model found [36] is build around the elements Organisation, People, Process and Technology. Through the organisation element the enterprise as a whole is examined. The strategy and objectives are mapped to the fundamentals of confidentiality, integrity and availability (CIA). The process element details the (security) processes, being the activities, practices and procedures, to support the organisations achieve its strategy. The element people represents all human-resources within the entire organisation which can

influence or are affected by information security. The last element, technology, is not only related to a tangible asset. Technology as presented within this model also incorporates the related technical skill and knowledge that impacts information security. These four elements are in their turn linked through so-called dynamic interconnections, being: culture, emergence, governing, architecture, enabling and support and human factors. According to the author, this model provides a holistic, dynamic solution for the design, implementation and daily management of information security, where it specifically assist in ensuring the CIA aspects of information assets. Although widely used within the information security community of practise, the model is restricted to information assets, and only takes the CIA criteria into consideration.

Bi-model IT based security model

This model, presented in appendix B, is based upon the so-called concept of 'Bimodal IT', whereas this concept is defined as [35]:

"*Bimodal IT refers to having two modes of IT, each designed to develop and deliver information- and technology-intensive services in its own way. Mode 1 is traditional, emphasising safety and accuracy. Mode 2 is non-sequential, emphasising agility and speed. Each mode has all the people, resources, partners, structure, culture, methodologies, governance, metrics, and attitudes toward value and risk that its operation requires. New investments are deployed through one of the two modes, depending on the balance of needs. When the balance changes, existing investments and operations move between the two modes. The most mature version of Mode 2, Enterprise Bimodal, is not just about the IT organisation; it encompasses a fast, agile mode of doing business.*"

The presented operating model [37], is a complete detailed model representing the mode 1, mode 2 and common security operations within a security organisation. At the tactical level the governance, external requirements, architecture, culture and people, methodologies (policies, frameworks and standards) are addressed. At the operational level, capability organised security processes and capability organised services are addressed. Economics on the usage of this model within security are at this point in time not available. Tough there are school of thoughts which drops the support for the bi-modal concept in general [38], as the speed of change is faster than both operating modes are able to deliver.

5.2.3. Analysis of target operating models

When analysing the previous work on target operating models, the average number of elements defined within a model is five. To obtain insights in the most applied elements within previous work, the models and their elements are placed in a matrix table (appendix C). If an element, according its general description, is used within another model, this element is assigned with one point. If an element is *exactly* the same as within another model, an additional 10 points is assigned per similarity.

This resulted in the following top five elements for target operating models: Governance, capabilities, processes, organisation, and people & culture. Table 4 provides an overview how these elements support the value proposition from the viewpoint of Osterwalders & Pigneurs (2010), broadly accepted business model canvas.

Table 4: Top five elements in support of a value proposition.

Identified Elements	Osterwalders & Pigneurs Value Proposition		
	Key Partners	**Key Activities**	**Key Resources**
Governance	X		
Capabilities		X	
Processes		X	
Organisation			X
People & Culture			X

To be workable, a model is best when it's simplified. With the Business Model Canvas, Osterwalder and Pigneur made a visual representation of their work. In the extend of this canvas, Cambell, et al., (2017) created a specific canvas visualising operating models. This canvas for operating models utilises the business model canvas. To this end it groups the business model canvas into (I)a front end, entailing the customer areas and the channels, (II)a mid-section representing the value, (III) a foundation which is referred as the financial system, covering the cost structure and revenue streams, and (IV) a back-end called operations, covering the original key partners, key activities, and key resources [39]. Having created a more abstract view on the business model canvas, the developed operating model canvas by Campbell, et al., (2017) takes care of the back-end of the business model canvas. The operating model canvas (right part of figure 12) is build upon the following areas [39]: Processes, Organisation, Locations, Information, Suppliers, and a Management System, where processes are the heart of the model.

By the use of a value chain map, the operating processes are displayed which are required to create and deliver the value proposition. By means of the organisation, the people who do the work and how they are organised are identified. Next, the location part

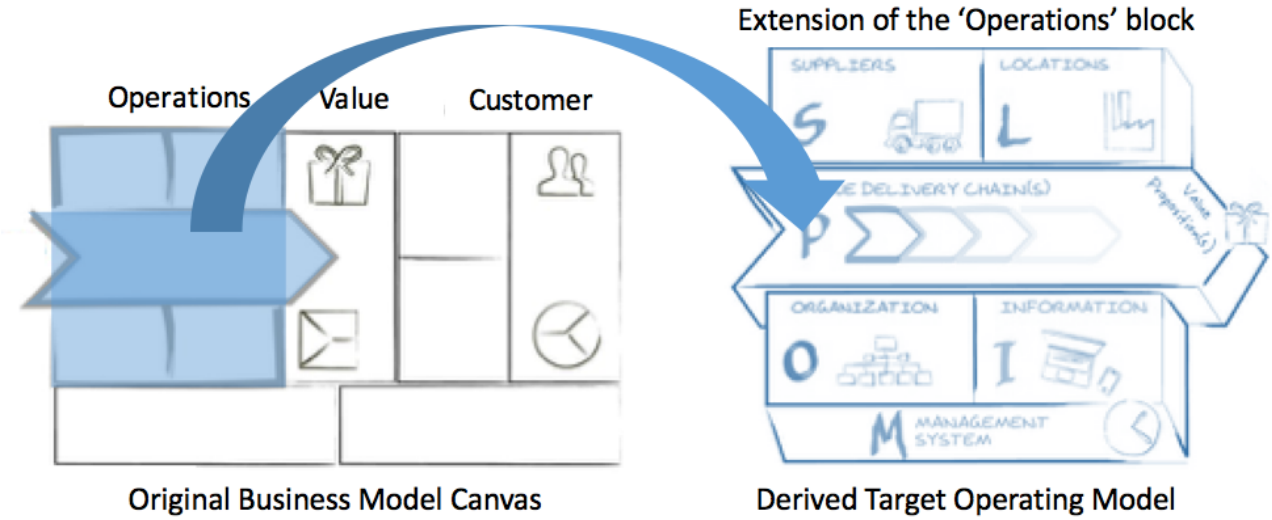

Figure 12: Target operating model derived from business model canvas, based upon [39].

is used not only to visualise where people are located, but also where important assets are located and why. The information group is used to identify which information technology is used in support of the value chain. By the suppliers group 'transactional' and 'collaborative' suppliers are identified, as well as it supports in decisions around insourcing and outsourcing of activities. Lastly, the management system describes how the organisation is governed on a daily base. Table 5 provides an overview how the target operating model canvas is linked to the top 5 identified elements of an operating model, and the elements of the back-end in the extend of the business model canvas.

Table 5: Overview of linkage between the top 5 elements, target operating model canvas and the business model canvas.

		Campbell, et al., Operating Model Canvas					
	Element	**Process**	**Organization**	**Location**	**Information**	**Suppliers**	**Management System**
Top 5 identified elements	Governance					X	X
	Capabilities	X					
	Processes	X					
	Organisation		X				X
	People & Culture		X				
Back-end elements	Key Partners					X	X
	Key Activities	X					
	Key resources		X	X	X		

While publication of the operating model canvas is dated 2017, the work on the model started earlier. Still the model is relative novel. While at this point in time no additional scientific research is available on this model, the model is an extension to, and in support of the broadly accepted business model canvas by Osterwalder and Pigneur. Next, taking into account the endorsements of the model by community experts, the contributing authors and the coverage of the model as presented table 7, this operating model canvas will be used to evolve the preliminary model presented in chapter 4, in order to composite and configure all elements.

5.3. APPLICATION OF THE TARGET OPERATING MODEL CONCEPT

Campbell's (2017) operating model canvas consist of 5 areas which are build around processes and capabilities which are required to create and deliver the value proposition The areas within the operating model canvas go by the acronym of "POLISM", which stands for:

- **P**rocesses;
- **O**rganization;
- **L**ocations;
- **I**nformation;
- **S**uppliers, and
- **M**anagement System.

Using these areas, the following paragraphs will analyse the meaning of these from the viewpoint of cyber-physical system security.

5.3.1. Security process analyses

Value Proposition

By means of the processes the value proposition is delivered. The value proposition drives the operating model, but is not part of it [39]. This value proposition is part of the larger, overarching, business model. The value proposition, or in other words the products and services, differ per sector, company, and per customer segment. To this end the value proposition can also vary and differ per department or function, to which security as a whole is delivered to. The value of security itself has been topic of interest in various academic research efforts. Here, the value is often presented in the context of Return Of Investment (ROI). While ROI measures the gain and loss of an investment, the majority schools of thoughts addresses ROI within security from the viewpoint of loss prevention. In this perspective you could argue that if the main value of security is loss prevention, are threats the main driver for security? Threats utilises vulnerabilities which together drives risk. Risk affects the business interest, including but not limited to the value proposition. Risk is one of the main pillars within security, today there is almost no standard, framework or best practise for security which doesn't utilises the notion of risk. But as risk from this viewpoint is linked to threats, the value proposition remains in the area of cost savings. In today's realm of a firm's digital transformation, the application of

technology and use of information will exponentially increase, as such will also the associated risks. But these risks can also create opportunities[40], such as competitive advantage and operational efficiency. Apple for example, uses security and privacy as competitive advantage. Providers of internet delivers spam filters and ant-virus software to their customers as competitive advantage [40]. Digital transformation in healthcare introduces new risks, where from an opportunity viewpoint operational efficiency can be increased within e.g. diagnose, treatment, or for example recovery supported by home-monitoring. Going back to the notion of cyber-physical security, the main stakeholder goal, in support of the value proposition, is to provide confidence that the system performs as expected regarding its threats in terms of environmental disruptions, human errors, systems faults and attacks [4]. While important to identify when creating a company specific operating model, creating a general applicable value proposition for cyber-physical systems is out of scope for this research. To this end, a scientific definition that captures the value proposition from the viewpoint of cyber-physical systems is not achievable. Nevertheless, based upon previous findings, the following elements will directly or indirectly be part of the value proposition regarding cyber-physical systems:

- Competitive advantage;
- Operational efficiency;
- Providing confidence regarding threats.

Endorsing the elements that constitute the value proposition, and taking into account the notion and definition of governance, the objective of cyber-physical system security can be defined as “managing security risks that arise within the span of cyber-physical systems”. Having a better understanding of the value proposition, and the objective of cyber-physical system security, we can analyse the capabilities required to manage cyber-physical system security. Based upon the these capabilities the supporting process can be identified.

Capabilities

Processes and capabilities are often used in the same notion. Within this analysis capabilities represents “what” is being done to manage cyber-physical security, and processes entails “how” it’s being done. Cyber-physical security must be considered as a whole and thereby become the result of its various areas of attention. At the highest level the following capabilities reside [4]:

- Assurance of security;
- Assurance of safety;
- Assurance of reliability;
- Assurance of resilience, and
- Assurance of privacy.

Here assurance means the recording and assessment of evidence that supports the existence and operational effectiveness of the activities that support the respective capability. Based upon the work of [4], the security capability relates to “protecting the cyber-physical system from unintended or unauthorised access, change or destruction. Safety refers to operating without causing unacceptable risk of physical injury or damage to the health of people, either directly or indirectly , as a result of damage to property or to the environment. Reliability is the capability of the cyber-physical system or its components to operate under stated conditions for a specified period of time. Resilience is defined as is the capability of a system that behaves in a manner to avoid, absorb and manage dynamic adversarial conditions while completing the assigned missions, and reconstitute the operational capabilities after causalities. Finally, privacy is the right to control or influence what related (personal) information is collected, processed, and stored and by whom, and to whom that information may be disclosed”.

Processes

Threat Intelligence & Risk Management

At the base of the main standards and best-practises available for security, safety, reliability, resilience and privacy lies the concept of risk management. In general, risk management is the process of identifying and managing uncertainties on objectives [41]. Within the field of cyber-physical system security often the term threat is used instead of uncertainty. For the remainder of this research the term ‘threat’ is applied, knowing that this term limits the notion of creating opportunities by risk. Risk management starts by setting the context. The context is often described in terms of objectives. Objectives can be related to the capabilities of security, safety or reliability within a system, but also to the performance of the system as a whole. Either way the context is always related to the strategic intend and the value creation. In addition, as already mentioned in paragraph 2.3.1, it’s important to determine who the adversaries or actors might be. Through this approach the focus is sharpened to those areas which are critical to the organisation. As such it’s important to have an intelligence cycle in-place to assure risks can be framed properly on a continues base. Once all these factors are known, the risks can be identified and analysed. At this point, the threats and vulnerabilities are analysed together with the likelihood and impact. This leads to an initial risk scoring, for example high, medium and low. Next needs to be evaluated: questions to be asked are what is a acceptable risk tolerance and are there already controls in place? Once known, a response strategy can be chosen. In general the responses can be categorised into: accept, transfer, mitigate or avoid the risk. When the risk is accepted then the business case indicated that the cost to mitigate the risk is higher than dealing with the risk. Transfer is applied when risks have a small likelihood of occurring but a high impact. Next to applying business continuity or resiliency, part of the risk is transferred to a third-party, for example by buying insurance. Mitigation is selected when the likelihood of occurring is high, but the impact small. When activities have a high likelihood of occurring and a high impact, its best to respond by avoiding or stop the activity. Finally, within risk management the risks needs to be monitored as risks may vary over time, and

communicated to its stakeholder. This general approach from setting the context till monitoring is reflected in all five identified capabilities. In the work “On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education” [21], the authors endorse the concept of addressing risks within two layers:(i)at a technical layer and (ii)at the socio-technical layer. These two layers are identical to the layers identified in paragraph 3.2.1 for applying an end-to-end approach. Applying this concept to risk management within cyber-physical systems, support the first and second identified requirements in chapter 3, paragraph 3.4 on main design requirements. Being recognised within every identified capability, **risk management, including threat intelligence, is the first process within the concept of a target operating model.**

Protection
When mitigating risk, reasonable and cost- effective controls must be implemented. Overall, the cyber-physical system needs to be protected. Controls to protect cyber-physical systems are not restricted to technology, they are a combination of controls aimed at technology, processes and people as a whole (e.g. users, vendors, partners, integrators etc.) Awareness for example is one of the non-technical controls aimed at people. Due the importance of awareness, it’s discussed separately within this chapter. Taking into account the aim of the controls, a distinguish can be made into three core processes [4, 42]:

- Endpoint protection;
- Communication & Connectivity protection, and
- Data Protection.

Endpoint protection is the process of design, development and implementation of preventive and defensive measures at a technical, process and people level to protect components and devices at the field layer, and within the cloud environment.

Protection of endpoints is one thing, but endpoints must communicate with each other and it are the interfaces in-between which are part of the main security challenge. Communication and connectivity protection provides on the one hand physical security of access to the network, and on the other, supported by cryptographic measures, the information flow in the network including the interfaces in between.

Data protection is the process concerned with the integrity, confidentiality and availability of data throughout the entire system. It includes data at rest and in use, but it also encompasses configuration data, monitoring data and for example management data. The process of data protection does not stand alone, but supports to this matter the process of endpoint protection and communication and connectivity protection.

The second process within the concept of a target operating model is Protection, encompassing the processes of protecting endpoints, communication & connectivity, and data.

Detection
Nowadays it's generally acknowledged that 100% security remains a noble goal. Security risks will remain and failure can always occur. Nevertheless, failure in protection doesn't automatically have to lead to losses [19]. A malicious actor can gain access to the network without having directly access to data or information. By means of intrusion detection, which is closely related to threat intelligence, the actor can be noticed and as a reaction excluded from the network or the breach can be contained. As such, detection is about monitoring and analysing the current state of security. Here, monitoring captures all data gathered by the endpoints, the interfaces, communications, and from component builders and integrators [42]. By means of analysing the gathered data, vulnerabilities, threats, and breaches are identified. **Security monitoring and analyses, as part of detection, is the third process within the concept of a target operating model**.

Reaction
Detection alone won't stop a malicious actor or prevent new discovered vulnerabilities of being utilised. Detection requires a reaction, where in some cases a well-thought decision of 'doing nothing' can also be a proper reaction. **Reaction is the fourth process within the concept of a target operating model.** According the work of [42] a distinguish can be made in three types of main reactions:

- Proactive based, aimed at mitigating threats upfront of an upcoming attack;
- Reactive and recovery based, these provides instant response to breaches and attacks in progress. This includes the notion of monitoring the intruder during the breach without immediately interfering with, or alarming the intruder. But once interfered, and if applicable, also critical operations needs to be recovered within, up-front, agreed timeframes;
- Analysis based to investigate the root cause of vulnerabilities and exploits after a breach or attack.

Compliance
So far, from all identified processes it's the risk management process which supports all of the capabilities. The processes of protection, detection and reaction are mainly in support of the resilience, reliability and security capability as they directly affect the system's ability to meet the functional expectations. Privacy and safety, on the other hand, relates more to the ability to be compliant with the expectations about the impact on the environment as a whole [4, 42]. In addition, depending on the industry, regulatory requirements for example Service Organisation Controls 2 (SOC2), General Data Protection Regulation GDPR, Sarbanes-Oxley (SOX) or Health Insurance Portability and Accountability Act (HIPAA) and so on may apply. Compliance is closed related to the

earlier identified assurance functionality. Although the process activities are mainly the same, In the perspective of this research, compliance is moreover focusing on adherence to external regulatory compliance, and assuring the existence and operational effectiveness of any topic. Combined **compliance and assurance is the fifth process to be added.**

Awareness

Processes within Campbell's (2017) operating model canvas are the core of the value proposition. While the former identified processes are critical to manage the security risk within cyber-physical systems, this doesn't mean these are the only one. Multiple supporting processes may exist within the realm of security, for example related to finance or human resources. Security awareness is one of the processes which can either be supportive or critical to the value proposition depending to the school of thought. Scholars and academic are divided to the contribution of awareness to security as 70% of security breaches are technology related [19]. Having previously identified a socio technical layer where actors reside and to be inclusive, for now **awareness is added as the final process in support of the value proposition.**

Based upon Porter's (1985) value-chain model, figure 13 visualises the main processes in support of the value proposition of cyber-physical system security. A distinguish is made in primary processes which directly affect the system's functionality, and secondary processes which are in support, thought critical in managing the security risks that arise.

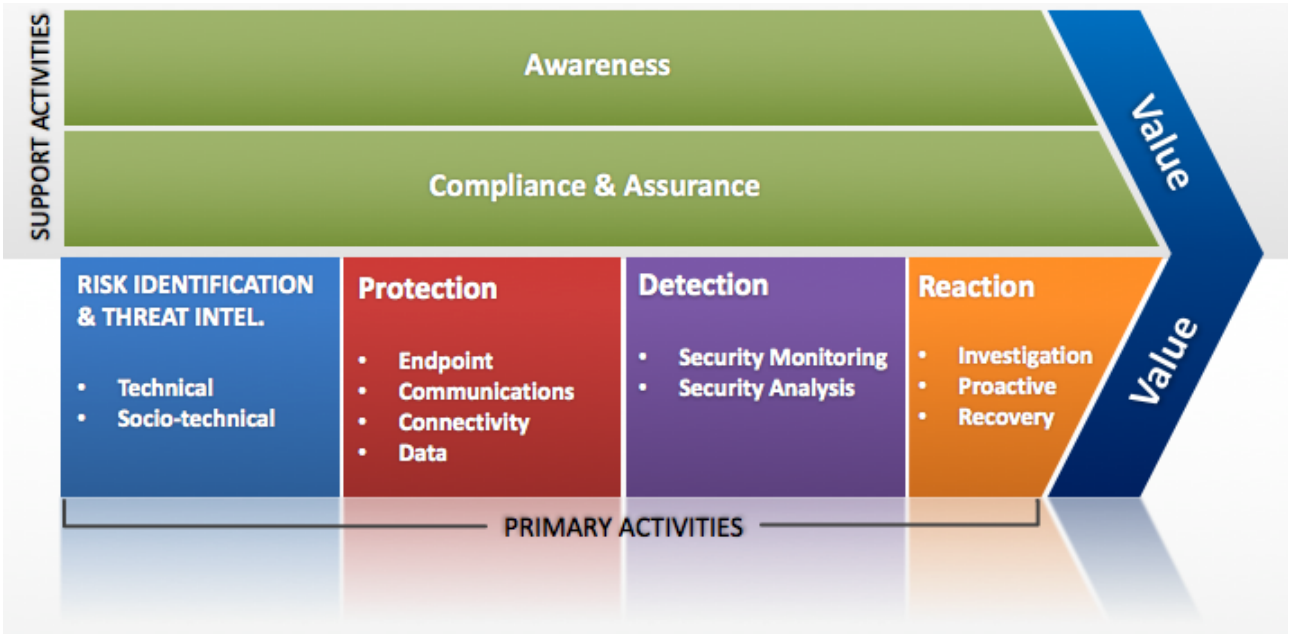

Figure 13: Processes in support of the value proposition of cyber-physical system security.

5.3.2. Security organisation analyses

The organisation building block within the target operating model concept is, unlike the identified requirement for organisational aspects, limited to the structure on how people are organised. The manner how organisations can be structured has been well described by various research and publications, e.g. by the work of Keuning and Epping (2004), Strikwerda et al. (2008) or Daft et al (2017). In practise an organisation structure is often visualised by its hierarchy. Well known hierarchal structures are for example the ‘line organisation’, ‘line-staff organisation’, ‘project organisation’, ‘process organisation’, and the ’matrix-organisation’. The former two are characterised by a vertical structure. Within vertical structures the staff is focused on specific tasks instead of the overall goals. People tend to work within the the walls of their department, causing a silo’d approach [43], which is one of the identified shortcomings we want to avoid within cyber-physical system security. The project organisation is characterised by specific goals and deliverables, where projects have a defined beginning and a fixed end. The project organisation brings together different disciplines in order to deliver on the pre-defined results. Within the earlier analysed security approach based upon Bi-model IT, multiple elements of the project organisation are embraced. Pitfall within is that the interest of the project doesn’t have to reflect the interest of security and vice versa. In addition, as projects have a fixed end, how to address for example detection and react during the life-cycle of a cyber-physical system? The process organisation is characterised by horizontal organisation, here the focus is about ‘customer’. Within a process oriented organisation line-managers become process owner who controls process deliverables. Borders between departments become vague and staff is being deployed in multidisciplinary teams [43]. While a silo’d approach is prevented, pitfall is that process managers do not receive the corresponding mandate as line management still claim their authority, or that not all tasks or activities are assigned to a process and fall between the cracks. Finally within a matrix organisation people are grouped by function or area of expertise, and from that area assigned to one or multiple projects. To this matter multiple reporting lines exists: one to the hierarchical manager, and one to the project manager of the assigned project(s). This approach is similar to the project organisation approach, although the conflict of interest seems less applicable, power struggles arise between functional management and project management [44]. Each type of organisation structure has its own advantages and disadvantages, that are all applicable within the realm of cyber-physical security. While, on a granular level, the design of a company specific organisation structure is a science of its own and would require additional research, on a general level, the design of a structure is feasible. A general structure must at least prevent working in a silo’d approach, support the constant speed of change within business, and balance interests of all stakeholders e.g. of those concerned with a cyber-physical system used for manufacturing and those concerned with the system being manufactured. In previous paragraph processes were identified in support of the value proposition. The processes are designed around the cyber-physical systems as a whole, structuring the organisation based upon these processes would prevent the silos such as

the security of information technology (IT), security of operational technology (OT), or security of the products being manufactured (product security). To prevent that activities remain untouched, as they are not directly part of a core process, would still require hierarchal management next to process management. The combination of a process structure and hierarchy structure is not novel, failure in practise is common due to the fact that the process and organisation structure is not designed at the same time. An integrated design of a hierarchy based and process based structure is visualised in appendix D, and achievable by applying the following design principles [43]:

1. All organisational functions are covered by one core process
2. All workforce functions are assigned to one or more process roles.
3. Management responsibilities are assigned as follows:
    - general en hierarchal responsibilities according the company structure.
    - process responsibilities, by assigning ownership, according the process structure.

By the first design principle all functions are covered by one core process. Figure 14 visualises this coverage for the processes identified in previous paragraph. By this approach it's prevented having departments without a process, or having departments with double functions. Next to the primary and secondary processes that are specifically critical for the value proposition, additional processes may be required. In general security is supported by a process for the development and maintenance of policies [45], and based upon progressive insights, a process to functionally manage the technology resources used in support of all security processes. This process is also known as Functional Application Management (FAM). Next, with regards to the notion of a bimodal approach and increasing speed of business [38, 46], a third supporting process is required. Where business's continuously seeking to reduce their time to market, concepts like 'Business Technology' and 'Agility' take the overhand, leaving the slower traditional information technologies approaches behind [38]. An analysis of the impact of these concepts to the realm security shows the need for the ability to support rapid development and rollouts of technology by application of the so-called 'DevOps' concept. This concepts entails combining, cross departments, multiple design steps into a single automated process. The presented organisation structure by figure 14 is already pre-sorted to this by leaving the approach on having separate departments for the security of products, information technology, cloud or operational technology, instead security and its functions are

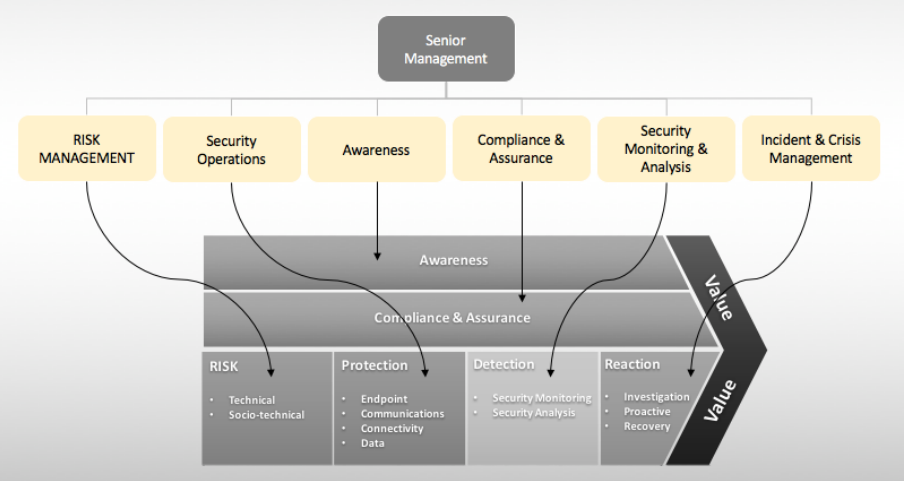

Figure 14: Organisational functions mapped to key processes.

process oriented. Still must be assured that security-experts have a seat at the table with other teams and departments involved in the design process. To plan and control security resources in line with strategic objectives and the overall security capacity to deliver, the function and process of portfolio management is added to the security organisation structure. Embedding a sustainable ‘DevOps’ approach within security requires more than being process oriented and applying portfolio management. It requires long-term change of soft-skills and culture among security experts [47]. Facilitating the change management process toward ‘DevOps’ is, for now, out of scope of this research.

By the second design principle, for each of the identified functions within the organisation structure, a formal description of accountabilities, responsibilities and tasks must be available. The roles deriving from the process structure describe the accountabilities, responsibilities and task on a more granular level. Assurance of the alignment between the organisation structure and the process structure requires seamless alignment between the available task description [43]. The third design principle requires a clear distinguish between process and hierarchal accountabilities/responsibilities. To balance the interests of all stakeholders and main areas of attention within the security domain, a Chief Security Officer (CSO) is positioned at the highest level within the security organisation structure. The CSO has mainly general management accountabilities, such as the strategic direction, the mission, vision or for example critical enabling success factors. Directly positioned below the CSO are the line-managers. The line-managers direct the work-staff. Aspects of the accountabilities and responsibilities of the line-managers are related to hiring, development and firing. Finally, the process accountabilities and responsibilities are assigned. Within the organisation functions the roles of process owners, process manager and subject-matter experts are assigned, The roles relates to the development, implementation and control of the earlier identified security process [43]. Figure 15 visualises the final, general, organisation structure to be applied within the target operating model. The presented structure takes into account the prevention of working in a silo’d approach, the support to the speed of change, and the balancing act between the interest of the main stakeholders. A matrix-process structure is created due to the intrinsic interwovenness between the primary and secondary processes in respect of the value proposition, and the general supporting processes. As every interface is detailed within the process structure, conflict of interest and power struggles are avoided [43].

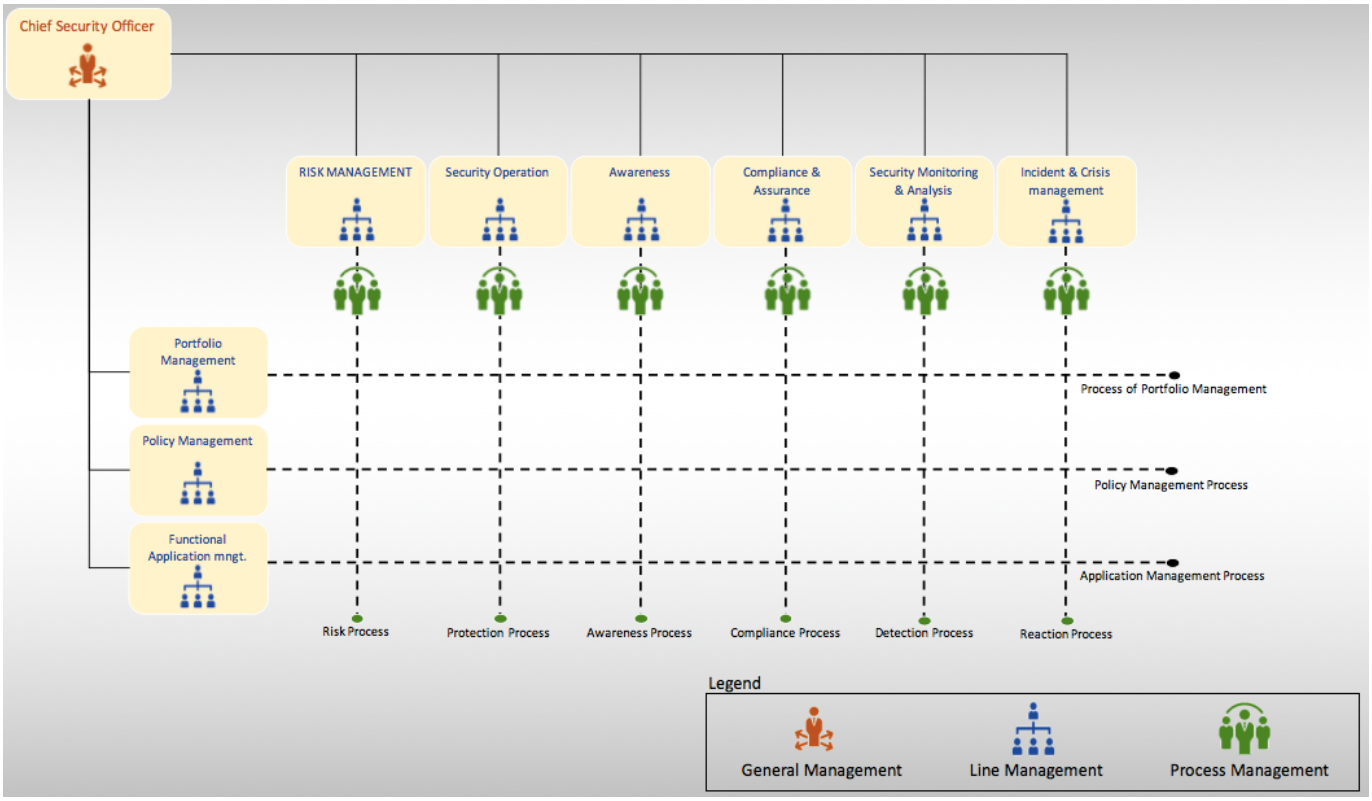

Figure 15: Organisation structure to be applied within the target operating model for cyber-physical security.

5.3.3. Security location analyses

This building block relates to where the work is located and what (tangible) assets, are requirement to execute on the defined activities. The authors of the target operating model concept [39] refers to regions, countries, buildings, and if applicable even floors. From a security perspective the location can be analysed through two different lenses. First, the place of execution can be important with regards to the geographic time zone. Threats, vulnerabilities or breaches are not restricted to local office hours. Having the ability to split e.g. the security monitoring and analysis activities across two opposite time-zones, like Europe and the USA, can provide 24 hours of coverage. On the other hand, when the security staff is located in an opposite time-zone from the business or fro example the technology department, could work against the required agility and speed of business. Secondly, the location of the cyber physical systems to be secured, can be of importance. Different regions or countries may have different rules and regulation for the data/information being stored, processed or exchanged.

5.3.4. Security information analyses

Information is about the information technology, or applications, required to support each identified security process. The choice of applications to use, differs per organisation as the strategy, budgets and maturity also differs per organisation. To this end, no detailed overview can be generated at this point in time. On a more general level, the following type of applications are often utilised within security environments [48]:

- GRC applications to support in managing security policies, security controls, risk management, business continuity management and management of compliance;
- Data management and analysis applications to provide for insights in data and support decision management;
- IAM application to support in identity and access management;
- Applications for patch management and patch deployment;
- Real-time threat monitoring applications;
- Mobile and cloud security solution in support of mobile security and secure cloud access ;
- Endpoint detection and response applications, and
- Firewall solutions to support in managing traffic and firewall optimisation.

Security functions can make use of an IT blueprint or application landscape to identify their necessary (and unnecessary) technology and applications, and act accordingly. These kind of overviews are regular designed and maintained, and thus available, by enterprise and business architects. If not, use can be made of 'TOGAF'. This stands for "The Open Group Architecture Framework", and is a broad accepted and applied framework for design and maintenance of these application architectures and overviews.

5.3.5. Security supplier analyses

Almost every business depends directly or indirectly on suppliers. Suppliers can deliver raw materials, components or supplies. For manny of these established markets exist, as such, the relationship with these suppliers can be 'transactional' [39]. Within the area of cyber-physical systems the relationship, e.g with component-builders and system-builders, exceeds the aspect of transactions only. Aggregation of trust on parts, component and organisational level, by all actors including suppliers, is a key requirement within the life-cycle of a cyber-physical system [4]. Depending on the application, change rate and the number of suppliers, a framed area can be reserved within the supplier building-block. Within this area, in support of collaboration and agility, the trusted component and system builders, which provides continuous assurance, can be positioned.

Apart from the viewpoint of a cyber-physical system, the security function itself can also have transactional and collaborative oriented relationships. As security spans the entire supply-chain, partnerships with the security functions of upstream and downstream partners are essential. Additionally, outsourcing of specialised capabilities or processes, for example like security monitoring an analysis, is not unusual. A supplier matrix supports in identifying the suppliers, relationships and if applicable the reasoning for outsourcing [39]. At the horizontal axe is determined if it is a key activity in delivering value. Vertically is determined how good the organisation or function can do this activity compare to others. If the activity is key and the organisation or function is doing it better than others, the activity remain. If others ca do it better, a collaborative agreement is

brought in place. If the activity is not key and other are doing it better, than it's being outsourced, otherwise, if it doesn't distract, the activity remains [39].

5.3.6. Security management system analyses

The management system is, by the authors of the target operating model concept, considered additional to the previous discussed core elements. This building block describes the governance aspects, which is already extensively covered within chapter three, and addressed by the preliminary designed model. In the extend of the governance aspects, the authors of the target operating model concept pay attention to what scorecard is used to measure progress. Development of indicators for security is a research field on its own, and not in scope of this research. Hence, in this perspective it's about measuring and reporting achievements on pre-defined strategy and objectives. Measurement, and more specific reporting depends on the tools and methods that are already embraced within the respective organisation. With regards to a target operating model, the concept is derived from the business models by Osterwalders & Pigneurs (2010). The business model canvas, on the other hand, is influenced by the four perspectives of the Balanced Scorecard approach by Kaplan and Norton (1992). The Balanced Scorecard, which relates back to the notion of governance, supports organisations in monitoring the performance of organisations by scores through four different lenses. Projected to the area of security, the four areas are [49]:

- **Value,** which expresses the strategy and objectives in relation to the value proposition;
- **Customers** is an expression of how the security process owners believes the security team should look to its target customers and the actors within the cyber-physical system, in order to achieve its strategic objectives;
- **Operations** is an expression of the identified capabilities at which the security team needs to excel in order to look the way the process owners believes it should to its stakeholders
- **Learning and growth** is an identification of the security staff and processes that will enable the security team to be excellent at the identified processes.

5.4. FINAL TARGET OPERATING MODEL

The preliminary model in chapter four sketched the outlines for the governance and management of cyber-physical system security. In previous paragraphs, the target operating model canvas is applied to the domain of security, in support of identifying the composition and configuration of related aspects such as processes, technology and organisation structure. Combined in figure 16, these aspects together with the preliminary model form the final target operating model for cyber-physical security. Where previous within this research there was a distinguish between primary processes, secondary processes, and general supporting processes, within the final model the primary and secondary processes are combined as they directly influence the value proposition. The general processes remains being supportive.

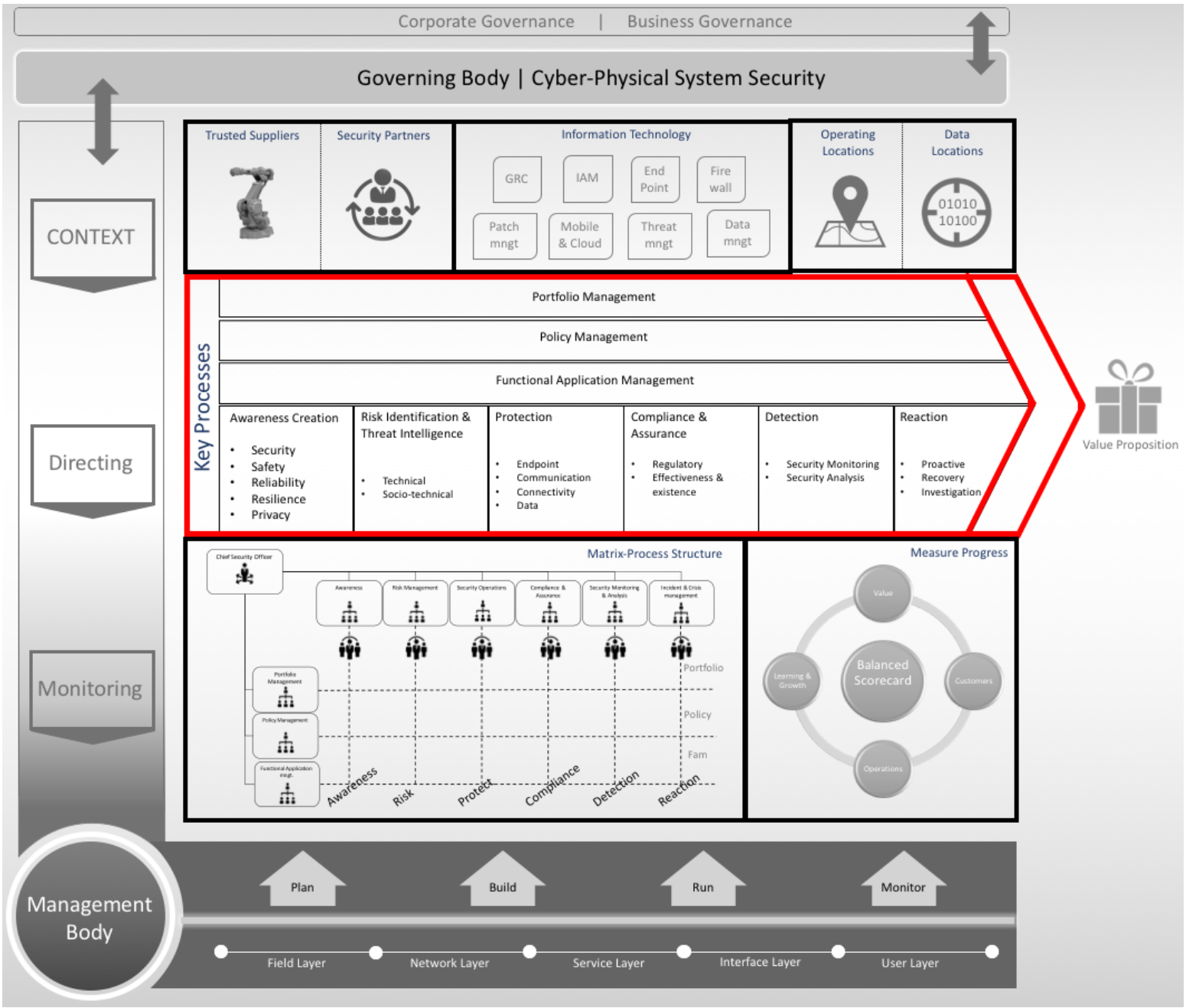

Figure 16: Final target operating model for cyber-physical security.

6. REFLECTION, CONCLUSION AND RECOMMENDATIONS

6.1. REFELECTION

6.1.1. Reflection on the applicability of the model

Ideally, the effectiveness and applicability of the model is tested in practice. This would, without arguing how to measure effectiveness and applicability, require a target environment for deployment of the model. Although the arise of the security challenge within cyber-physical systems is acknowledged, and the concept of the fourth industrial revolution is embraced, no environment has been found where this concept has been fully deployed. The majority of the manufacturers assessed, are in the phase of experimenting and developing small parts of the concept. As such, the major changes in the approach and governance as part of the developed model, has been presented to and evaluated with industry experts who participated in the initial interviews. Interesting findings are:

- Without touching the process orchestration, various large companies are planning on governing and directing multiple areas of security by a single entity, as proposed within the developed model;
- Organising security horizontally as one single process seems difficult to grasp, while concepts as ‘agile’ and ‘devops’ are recognised. A counter desk approach seems to be ingrained.
- Deployment of the model, which entails the integration of the different areas like IT and OT, will encounter resistance. Although not scientific underpinned, during the interviews and evaluation this was already sensible as key positions could disappear or people needed to hand in autonomy and control.
- Although not within a manufacturing environment, and neither within the concept of the fourth industrial, one example is found afterwards where central governance and a single process approach, as proposed within the developed model, proved to be successful.

6.1.2. Reflection on the research contribution

This research contributed by developing a model to integrally govern security of cyber-physical systems. The goal was to support manufacturers with managing the security risks that arise with cyber-physical systems, within the concept of the fourth industrial revolution. This goal has been achieved by the design of a target operating model which fully aligns to ten identified main design requirements. Following paragraph provides an overview how these requirements are fulfilled.

6.1.3. Reflection of adherence to the design requirements

Requirement #1

The model must take into account the technology components used during the life-cycle (individual and as a whole, which includes for example the integration of information technology (IT) and operational technology (OT). This requirement is addressed by organising security horizontally. Instead of each type of component having their own security department with the risk of underexposure of the interfaces, security is organised per capability independent of its application. By means of a horizontal configuration of security capabilities and processes, the life-cycle of a cyber-physical system, from design until end-of life, is also addressed. This because the horizontal security processes applies regardless of the operating status during its life-cycle.

Requirement #2

The model must take into account the interaction between all (human)actors, systems and machinery. At the foundation of the model a distinguish is already made between layers of physical artefacts and users. The focus on interaction is amplified by managing the risks from a traditional technical perspective, and on top from a socio-technical perspective. Finally, to prevent that the realm of actors is limited to the end-users, the developed model specifically takes into account the component and system builders, in terms of suppliers and partners.

Requirement #3

The third requirement is aimed at addressing the future state of cyber-physical system security. The developed model itself support in reaching the future state, whereas the definition of the desired future state is assured by the positioning of a governing body. The governing body defines the future state in alignment with the strategic intent of the organisation as a whole.

Requirement #4

To address how the future state is achieved, the designed model defines how for example the organisation, processes, and technology are configured and managed by a management body.

Requirement #5

The model must provide alignment with business objectives, stakeholders and create value. To create value the designed model is build around the organisations value proposition. As seen with retirement three and four, governance is embedded within the model to assure alignment on strategic and tactical objectives.

Requirement #6

The model must foresee in providing guidance, prioritisation of activities and allocation of resources. This requirement is for-filled by the positioning of a governing body, who has these as its main responsibility.

Requirement #7

The model must force in providing assurance that the derived strategic security objectives are achieved. Also here the governing body is responsible by having monitoring as one if its main responsibilities next to directing and setting the context for security.

Requirement #8

The model must address policies and derived control frameworks to measure performance and compliance. Within the designed model, policies and compliance are identified as key processes in support of the value proposition. In addition, a management body is assigned with the responsibility to monitor on these items, supported by a balanced scorecard.

Requirement #9

The model must address the required workforce, their skills and structure. The organisation structure has its own dedicated place in the designed model. The required workforce and their detail skills are company specific based upon its core values. To this end these are not visualised within the designed model. When applied to a specific company these can be taken into account.

Requirement #10

The model must foresee in the process to manage cyber-physical security. The designed model is based upon the capabilities required to provide security. The processes are derived from these capabilities, in support of the value proposition.

6.2. CONCLUSIONS

The purpose of this research was to develop a target operating model, that supports manufacturers with managing the security risks that arise with cyber-physical systems, related to the concept of the fourth industrial revolution. This research confirmed that within cyber-physical systems risk arises, whereby many of these risks are not novel in the realm of security. Though, the majority of components which entails a cyber-physical system are being connected and brought to cloud environments, causing increased hyper-connectivity among. This hyper-connectivity within and between cyber-physical systems creates new interfaces, and these new interfaces in their turn creates new security risks which needs to be managed. In manny traditional approaches, security is organised in silos where each area (e.g. information security, product security, OT security, etc) acts as an individual counter desk. Each counter desk has its own accountabilities, as such the main challenge is who has the accountability and responsibility for the new risks between the counters, as this is either unclear or doesn't

match the interest of all stakeholders. Current available models are either restricted to the silos (or counter desks) for which they were originally designed, or can't match the required speed of business introduced by new digital business concepts. The main elements of a model to support manufacturers with managing the (new) security risk that arise are:

- A governing body for cyber-physical system security which defines at the strategic level what needs to be done, aligned to the business strategy, business objectives and stakeholder needs;

- A single process based approach:
  - aimed at the value proposition of security;
  - Integrating the different areas for example IT and OT;
  - entailing the technical perspective and socio-technical perspective, and
  - build around the security of endpoints, communication & connectivity, and data.

- A process based organisation structure, including a management body with a clear distinguish between process and hierarchal accountabilities/responsibilities, who determines how the security strategy and objectives are reached by planning, building, running and monitoring the daily security operations, and

- To balance the interests of all stakeholders and all process domains within security, an overarching, single headed Chief Security Officer (CSO) is assigned at the highest level within the security function.

6.3. RECOMMENDATIONS

With regards to this research, the following recommendations may be considered:

- Due to the unavailability of a reference site to extensively test the effectiveness and applicability of the designed model, consider to engage with a broader audience of policy makers, standardisation institutes and industry experts to (1)reflect by workshops on the impact and consequences of the model, and (2)to assure access to a pilot site once an appropriate one becomes available and (3)to endorse the developed model supported by a broad community.

- Further research may be considered on (1)the design of security controls for the new risks at the interface layers, (2)for re-defining the value proposition of security by taking into account opportunities within digital strategies and (3)on how to embed the designed model, integrate multiple area's and transform traditional security functions to more agile environments, taking into account the management of change.

BIBLIOGRAPHY

1. Watson, P., Corporate vs. Product Security, in Infosec Reading Room. 2013, SANS Institute: Online. p. 15.
2. Rockwell Automation Industrial Security, Protecting networks and facilities against a fast-changing threat landscape. 2016. 13.
3. E. Luiijf, B.J.t.P., Cyber Security of Industrial Control Systems. 2015, The Hague: TNO. 57.
4. The Industrial Internet Consortium, The Business Viewpoint of Securing the Industrial Internet - Executive Overview. 2016, Object Management Group: online.
5. Nuth, T. Fighting for holistic, OT security. 2017 22-07-2017]; Available from: http://www.controleng.com/single-article/fighting-for-holistic-it-ot-security/45dbca23df2ae67234aa2bed6a185102.html.
6. BDO USA, 2017 BDO Manufacturing Riskfactor Report. 2017, BDO: online. p. 14.
7. Pierluigi Paganini. Former employee hacked paper maker Georgia-Pacific and caused $1m damage. 2017 [cited 2017 12-08-2017]; Available from: http://securityaffairs.co/wordpress/56396/cyber-crime/paper-maker-georgia-pacific-hacked.html.
8. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. in IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society. 2011.
9. Dennis de Geus, Business & Organizational models: Security operating model for a digital enterprise. 2017: Cyber Security Academy, The Hague.
10. Hevner et al, Design Science in Information System Research. MIS Quarterly, 2004. 28(1): p. 75-105.
11. William Smit, et al., Industrial Internet of Things: Noodzaak voor Industrie, kans voor IT-sector. 2016, ABN AMRO Sector Advisory & Sustainability: Online. p. 22.
12. CPS Public Working Group. Framework fo Cyber-Physical Systems. 2016 May 2016; Available from: https://pages.nist.gov/cpspwg/.
13. Lodewiek Janses and Nanno Zegers. Digitale beveiliging van industrial control systems. 2014 [cited 2017 25-09-2017]; Available from: https://www.deitauditor.nl/informatiebeveiliging/digitale-beveiliging-van-industrial-control-systems/.
14. Hugh Boyes. Cyber security attributes for critical infrastructure systems. [Internet] 2017 [cited 2017 16-09-2017]; Available from: http://www.cybersecurity-review.com/articles/cyber-security-attributes-for-critical-infrastructure-systems/.
15. National Institute of Standards and Technology (NIST). The NIST Definition of Cloud Computing. [online] 2015 [cited 2017 25-09-2017]; NIST Special Publication 800-145:[Available from: http://csrc.nist.gov/publications/PubsSPs.html#800-145.
16. Givehchi, O. and J. Jasperneite, Industrial Automation Services as part of the Cloud: First experiences. 2013.
17. Louis Colombus. Roundup Of Internet Of Things Forecasts And Market Estimates. Tech 2016 [cited 2017 29-09-2017]; Available from: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#353e3cd9292d.
18. Beecham Research. Beecham Research's IoT Threat Map. Shaping the IOT Feature 2015 [cited 2017 13-09-2017]; Available from: http://www.beechamresearch.com/news.aspx?id=1089#.
19. Winkler, I. and A.T. Gomes, Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. 2016: Syngress Publishing. 260.
20. Li, S., Chapter 1 - Introduction: Securing the Internet of Things, in Securing the Internet of Things. 2017, Syngress: Boston. p. 1-25.
21. Jan van den Berg et al., On (the Emergence of) Cyber Security Science and it Challenges for Cyber Security Education. 2015.
22. Romdhani, I., Chapter 9 - Confidentiality and Security for IoT Based Healthcare, in Securing the Internet of Things. 2017, Syngress: Boston. p. 133-139.
23. Gillian Lees, Enterprise Governance, in Topic Gateway series. 2007: online.
24. Savtschenko, M., F. Schulte, and S. Voß, IT Governance for Cyber-Physical Systems: The Case of Industry 4.0, in Design, User Experience, and Usability: Theory, Methodology, and Management: 6th

International Conference, DUXU 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I, A. Marcus and W. Wang, Editors. 2017, Springer International Publishing: Cham. p. 667-676.
25. International Organization for Standardization, ISO/IEC 38500, Information technology - Governance of IT for the organziation. 2015, ISO: Online. p. 15.
26. ISACA. Glossary. 2017 [cited 2017 06-102017]; Available from: https://www.isaca.org/Pages/Glossary.aspx?tid=1443&char=G.
27. Information Systems Audit and Control Association (ISACA), Transforming Cybersecurity using COBIT 5. 2013: Online.
28. International Organization for Standardization, ISO/IEC 27014, Information technology - Governance of information security. 2015, ISO: Online. p. 18.
29. National Institute of Standards and Technology (NIST). Framework for improving Critical Infrastructure Cybersecurity. 2014 02-12-2014; Available from: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
30. Simonsson, M. and P. Johnson, Defining IT governance - A consolidation of literature, in Trita-EE. 2005, KTH Royal Institute of Technology.
31. Marcia Blenko, Eric Garton, and Ludovicia Mottura. Winning Operating Models That Covert Startegy to Results. 2014 [cited 2017 19-08-2017]; Available from: http://www.bain.com/publications/articles/winning-operating-models-that-convert-strategy-to-results.aspx.
32. Annie Murphy, Jamie Kirwin, and Khalid Abdul Razak, Operating models: Delivering on strategy and optimizing processes. 2016, Ernst & Young LLp: Online.
33. Pascal Martino, Patrick Laurent, and Basil Sommerfeld. Target Operating Model at a glance. 2014 [cited 2017 04-09-2017]; Available from: https://www2.deloitte.com/lu/en/pages/strategy/solutions/target-operating-model.html.
34. Joyce, A. and R.L. Paquin, The triple layered business model canvas: A tool to design more sustainable business models. Journal of Cleaner Production, 2016.
35. Mary Mesaglio and Somin Mingay, Bimodel IT: How to Be Digitally Agile Without Making a Mess, in Gartner Executive Programs. 2014, Gartner Inc.: Online. p. 55.
36. Rolf M. von Roessing, The Business Model for Information Security. 2010, ISACA. p. 73.
37. Dennis de Geus, Business & Organizational models: Security opertaing model for a digital enterprise. 2017: Cyber Security Academy, The Hague.
38. Time Sheedy and M. Guarini, Speed And Innovation Drive CIO Succes: Bimodal Dinosaurs Won't Be Able to Lead Their Companies To Succes. 2017, Forrester Reserach Inc.: Online.
39. Andrew Campbell, Mikel Gutierrez, and M. Lancelott, Operating Model Canvas: Aligning operations and organization with strategy. 2017: Van Haren Publishing, Zaltbommel. 210.
40. Roel van Rijsewijk, Cyberrisico als Kans. 2016, Amsterdam: Boom Uitgerevers.
41. International Organization for Standardization and International Electrotechnical Commission, Risk Management: Principles and guidelines. ISO31000:2009. 2009.
42. The Industrial Internet Consortium, Industrial Internet of Things Volume G4: Security Framework. 2016, Object Management Group: online.
43. M.A. Nieuwenhuis. The Art of Management. 2010 [cited 2017 20-11-2017]; Available from: www.123management.nl.
44. S.M. Davis and P.R. Lawrence, Problems of Matrix Organizations, in Harvard Business Review. 1978, HBR: Online.
45. Jennifer L. Bayuk, Security through Process Management. 1996, National Institute of Standards and Technology: Online. p. 11.
46. Dennis de Geus, Business & Organizational models: Security opertaing model for a digital enterprise. 2017, Cyber Security Academy: Lecture.
47. Tas Bindi. DevOps succes factors: Culture, API's, and security. Riding the DevOps Revolution [Internet] 2017 [cited 2017 22-11-2017]; Available from: http://www.zdnet.com/article/devops-success-factors-culture-apis-and-security/.

48. Capella University. 7 Essential Information Security Tools. 2016 [cited 2017 23-22-2017]; Available from: https://www.capella.edu/content/capella/infosec/home/2016/08/7_essential_informat/.
49. Derek Brink. A Strategy Map for Security Leaders: Applying the Balanced Scorecard Framework to Information Security. Security Intelligence 2016 [cited 2017 23-11-2017]; Available from: https://securityintelligence.com/a-strategy-map-for-security-leaders-applying-the-balanced-scorecard-framework-to-information-security/.
50. Ernest Mueller. What is devOps. 2010 [cited 2017 29-12-2017]; Available from: https://theagileadmin.com/what-is-devops/.
51. International Organization for Standardization and International Electrotechnical Commission, Information technology - Security techniques - Guidelines for cybersecurity. ISO27032. 2012.
52. Jonathan Rasmusson. Agile in a Nutshell. 2014 [cited 2018 07-01-2018]; Available from: http://www.agilenutshell.com.
53. Monostori, L., et al., Cyber-physical systems in manufacturing. CIRP Annals - Manufacturing Technology, 2016. 65(2): p. 621-641.
54. Nate Lord. What is SOX compliance. 2017 [cited 2018 07-01-2018]; Available from: https://digitalguardian.com/blog/what-sox-compliance.
55. Roberto Minerva, A.B., Domenico Rotondi,. Towards a definition of the Internet of Things (IoT. 2015 [cited 2018 2-1-2018]; Available from: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.
56. SANS. Glossary of Security Terms. 2017 [cited 2017 27-12-1017]; Available from: https://www.sans.org/security-resources/glossary-of-terms/.
57. The Industrial Internet Consortium, Industrial Internet of Things Volume G8: Vocabulary. 2017, Object Management Group: online.
58. The Open Group and The SABSA Institute, Integrating Risk and Security within a TOGAF Enterprise Architecture. 2016, The Open Group: Online. p. 33.
59. U.S. Department of Health and Human Services. Science Education. 2017 [cited 2017 28-12-2017]; Available from: http://www.iiconsortium.org/vocab/index.htm.
60. Unknown. Point of Sale. 2017 [cited 2017 19-12-2017]; Available from: https://en.wikipedia.org/wiki/Point_of_sale.
61. Beal, V. Stuxnet. Unknown [cited 2018 02-02-2018]; Available from: https://www.webopedia.com/TERM/S/stuxnet.html.
62. Wang, L. and A. Haghighi, Combined strength of holons, agents and function blocks in cyber-physical systems. Journal of Manufacturing Systems, 2016. 40(Part 2): p. 25-34.

APPENDIX A: INTERVIEW OVERVIEW

OUTLINE

The chosen for the interviews is the semi structured interview whereby all answers are elaborated on by asking additional questions according the five times “W” and one time “H” methodology. The content of the interview is as follows:

Introduction

Introduction about author and the Master Programme
Explain the relation between this thesis with regards to authors employer.
Elaborate on confidentiality

General Background

What is the area of attention of your department?
What is your function within this department?
What us currently your main focus?
What are the main challenges and/or dependencies you encounter?
Are there currently specific standards/frameworks being applied?

Main Topic

Introduction to cyber-physical systems as a whole
What is the role of your function & area of attention with regards to cps?
What are, according to you, in the perspective of cps, the main challenges?
How to address these challenges?
Explain the identified challenge within research study
Do you recognise this challenge in general and/or within your own organisation?
How is/or could this be addressed?
How are your current activities being governed?
- Who is involved
- What is being governed
- How does it takes place (standards, frameworks)

With regards of governance, are there any gaps or challenges?
Explain the outlook of coordination, collaboration or perhaps integration within CPS security, not digital but also physical related. How do you envision this concept?

Closure
Summary
Remaining question
End interview

INTERVIEWEES

Table 6: Overview of persons interviewed in support of this research.

DATE	Name (reference)	Area of expertise	Sector
5 April 2017	Interviewee A	Product security	Manufacturing
6 April 2017	Interviewee B	Information security strategy	Manufacturing
15 May 2017	Interviewee C	Information security governance	Manufacturing
22 May 2017	Interviewee D	Information security risk	Manufacturing
23 May 2017	Interviewee E	Information security policies	Manufacturing
13 June 2017	Interviewee F	Product security	Manufacturing
16 August 2017	Inteviewee G	Product security	Manufacturing
11 September 2017	Interviewee H	Health and Safety	Manufacturing
20 September 2017	Interviewee I	Physical security	Manufacturing
10 October 2017	Interviewee J	Smart manufacturing / Industry 4.0	Manufacturing
10 October 2017	Interviewee K	Smart manufacturing / Industry 4.0	Manufacturing
11 October 2017	Interviewee L	Information security (CISO)	Manufacturing
07 December 2017	Interviewee M	Information security (CISO)	Manufacturing

Due to confidentiality, the participants in the interviews have been anonymised.

APPENDIX B: BI-MODEL BASED SECURITY MODEL

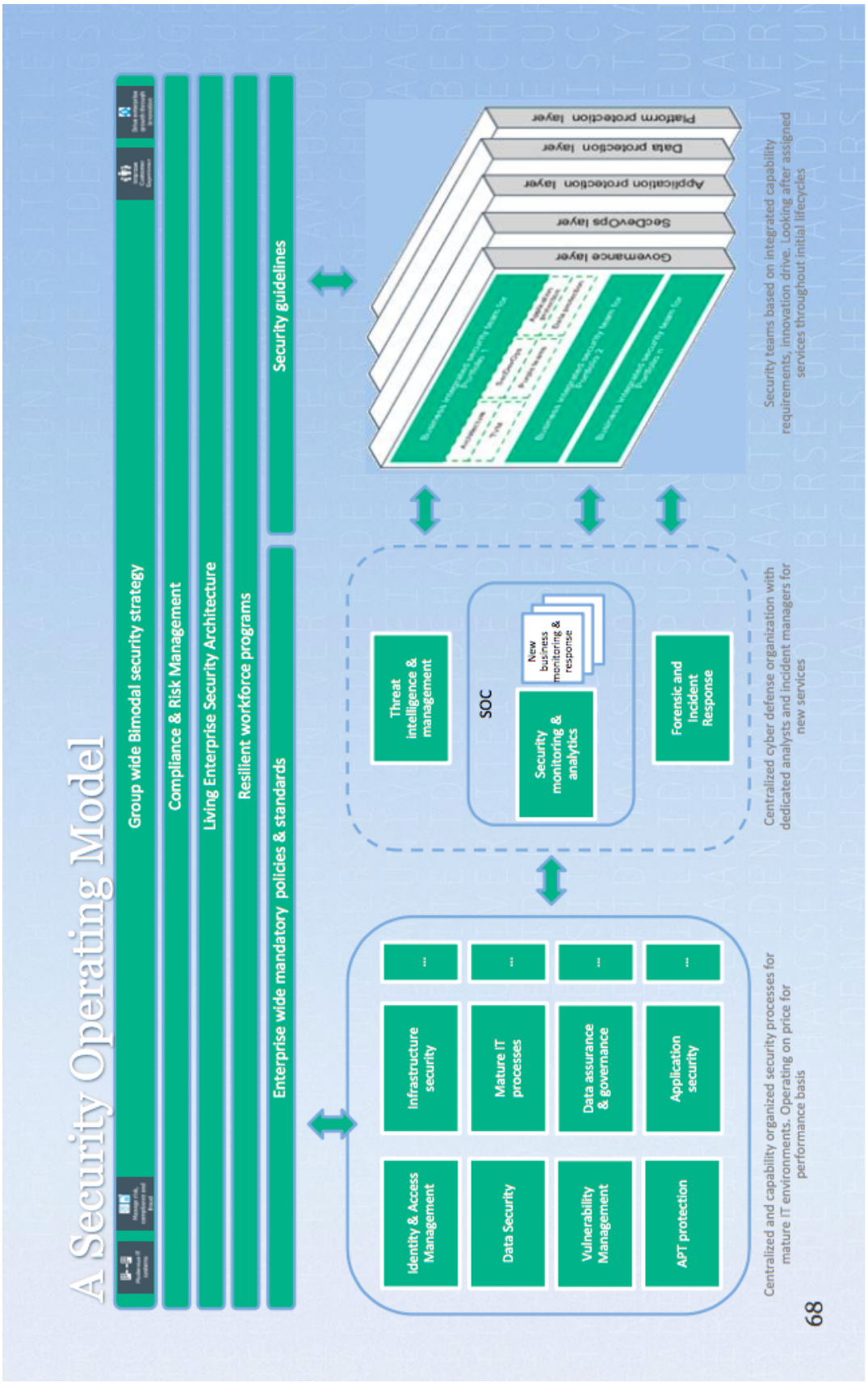

Figure 17: Security operating model, based upon Bi-model IT. Obtained from [9].

Table 7: Overview of similarities within different operating models

		Murphy, et al.				ISACA				Lindgart			Geus						Martino Deloitte				Amount X	Commonality X 10	total
		Design Principles	Culture and values	Governance	Processes	People	Process	Technology	Organization	Value Chain	Cost model	Organization	Governance	External requirements	Architecture	Culture & People	Methodologies	Capabilities	Organisational design	Process	Information Technology	Physical Assets			
Bain & Company	Structure								X				x						x				3	0	3
	Accountabilities								X			x	x						x				4	0	4
	Governance			X					X				x						x				4	20	24
	Ways of work		X				X									x	x			x			5	5	5
	Capabilities				X		X			x								x		x			5	10	15
Murphy, et al.	Design Principles													x									0	0	0
	Culture and values					x										x							2	10	12
	Governance								x			x	x						x				5	-	-
	Processes						x			x								x		x			4	20	24
ISACA	People											x				x							1	10	12
	Process									x								x		x			3	-	-
	Technology														x						x		2	2	2
	Organization											x	x						x				3	10	13
Lindgart	Value Chain																	x		x			2	2	2
	Cost model																						0	0	0
	Organization												x				x		x				3	-	-
Geus	Governance																		x				1	-	-
	External requirements																						0	0	0
	Architecture																				x		1	1	1
	Culture & People																		x				1	-	-
	Methodologies																						0	0	0
	Capabilities																			x			1	-	-

APPENDIX D: INTEGRATION OF ORGANISATION ROLES

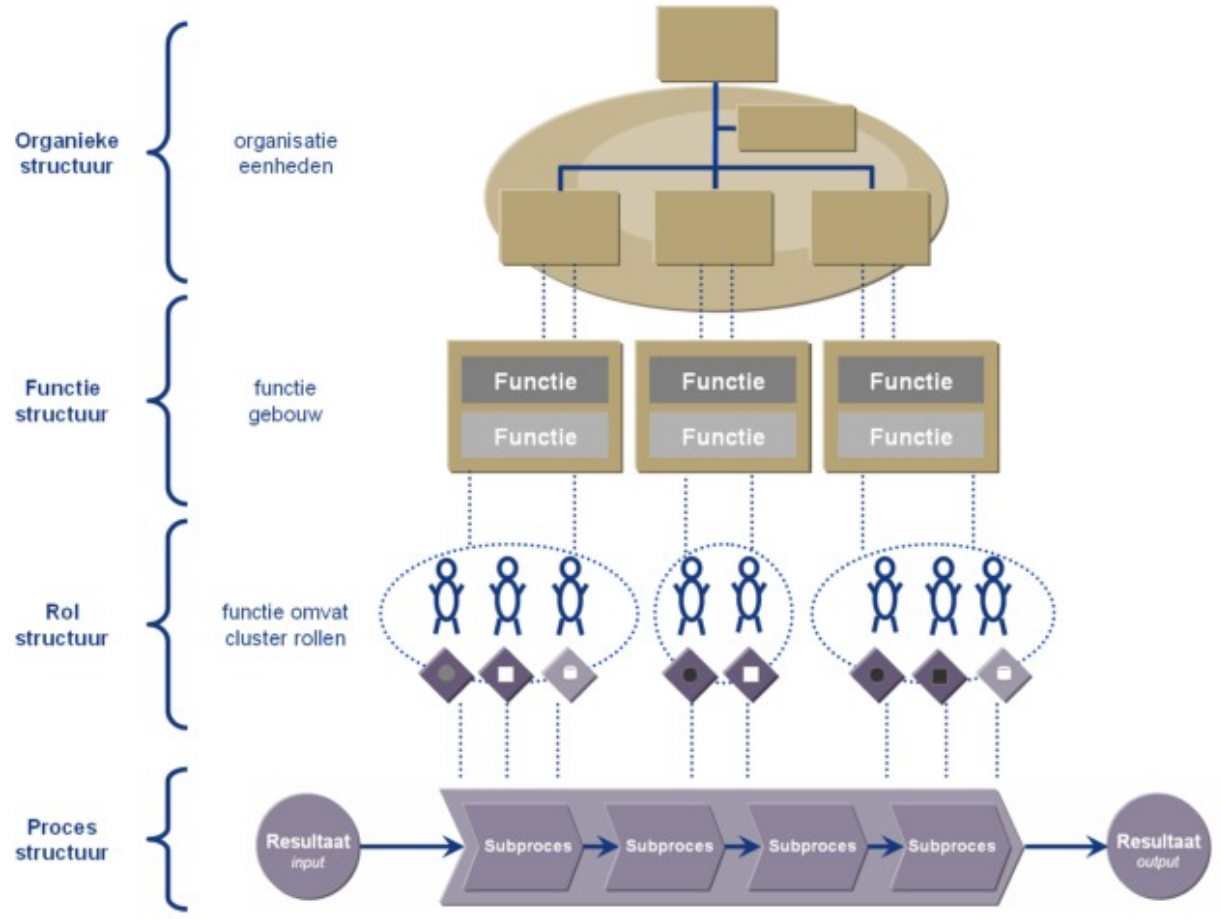

Figure 18: Integration of hierarchical and process roles. Obtained from [43].

APPENDIX E: TERMS AND DEFINITIONS

ABBREVIATION	TERM	DEFINITION / REMARKS	SOURCE
	Actuator	“Device that can change a property of a physical entity in response to an input.”	[57]
	Agile	“Agile is a time boxed, iterative approach to software delivery that builds software incrementally from the start of the project, instead of trying to deliver it all at once near the end.”	[52]
	Attacker	“Person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources.”	[57]
	Authentication	“Provision of assurance that a claimed characteristic of an entity is correct.”	[57]
	Autorization	“Granting of rights, which includes the granting of access based on access rights.”	[57]
	Availability	“Property of being accessible and usable upon demand by an authorized users.”	[57]
	Bimodel IT	“Concept which refers to having two operating modes of IT.”	[35]
CSO	Chief Security Officer	An organisation’s most senior person who is accountable for security as a whole.	
	Cloud Services	“Services related to cloud computing where cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.”	[15]
	confidentiality	“Property that information is not made available or disclosed to unauthorized individuals.”	[57]
COBIT	Control Objectives for information and related Technology	Framework to govern information systems.	
CPS	Cyber Physical System	“Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components.”	[12]
	Cyber-Security	“Preservation of confidentiality, integrity and availability of information in the Cyberspace”. In turn “the Cyberspace” (is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.”	[51]
DoS	Denial of service	“Prevention of authorized access to resources or the delaying of time - critical operations.”	[57]
	DevOps	“DevOps is the practice of operations and development engineers participating together in the entire service lifecycle, from design through the development process to production support.”	[50]
	End point	“Component that has computational capabilities and network connectivity.”	[57]

ABBREVIATION	TERM	DEFINITION / REMARKS	SOURCE
ERP	Enterprise Resource Planning	Information technology aimed at supporting planning and logistics of an organizations.	
GDPR	General Data Protection Regulation	Regulation aimed at protection of persons in terms of data processing (also see privacy).	
GRC	Governance, risk and compliance	Strategy for managing an organisation's governance, risk and compliance.	
HIPAA	Health Insurance Portability and Accountability Act	Regulation aimed at protecting sensitive patient data.	
IAM	Identity and acces management	Process and policies involved in managing the lifecycle and value, type and optional metadata of roles and access privileges of individual network users.	
IIOT	Industrial Internet of Things	"System that connects and integrates industrial control systems with enterprise systems, business processes and analytics note 1: industrial control systems contain sensors and actuators. note 2: typically, these are large and complicated system."	[57]
ISACA	Information Systems Audit and Control Association	"Association which promotes the practise of controlling and auditing of information systems."	[27]
IT	Information Technology	"Equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which — 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.'	[15]
ITIL	Information Technology Infrastructure Library	Best-practise for managing information services.	
	integrity	"Property of accuracy and completeness."	[57]
IEC	International Electrotechnical Commisiion	Commission for electrotechnical standards.	

ABBREVIATION	TERM	DEFINITION / REMARKS	SOURCE
IOT	Internet of Things	“Internet of Things envisions a self configuring, adaptive, complex network that interconnects ’things’ to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing’s identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.”	[55]
IP	Internet Protocol	Protocol to sent data from one endpoint to another through the internet.	
MRI	Magnetic resonance Imaging	“MRI is a non-invasive imaging technology that produces three dimensional detailed anatomical images without the use of damaging radiation. It is often used for disease detection, diagnosis, and treatment monitoring. It is based on sophisticated technology that excites and detects the change in the direction of the rotational axis of protons found in the water that makes up living tissues.”	[59]
MITM	Man in the Middle	“Procedure where an attacker makes independent connections with a victim and relays messages and thereby controls the entire conversation.”	[20]
MES	Manufacturing Execution System	Information technology aimed at managing operations at plant level.	
	non repudiation	“Ability to prove the occurrence of a claimed event or action and its originating entities.”	[57]
	Operating Model	A Target Operating model is a simplified description of interrelated elements of an organisation, such as, but not limited to: technology, processes and people, that are important for executing the strategy, to successfully deliver the organisations value proposition’.	
OT	Operational Technology	“Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.”	[57]
POS	Point of Sale	“A retail point of sale system typically includes a cash register (which in recent times comprises a computer, monitor, cash drawer, receipt printer, customer display and a barcode scanner) and the majority of retail POS systems also include a debit/credit card reader.”	[60]
	Privacy	“Right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.”	[57]
	Privacy	“Right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.”	[57]

ABBREVIATION	TERM	DEFINITION / REMARKS	SOURCE
POLISM	Process, organisation, locations, information, suppliers and management system	Elements that constitute a target operating model.	
PLC	Programmable Logic Controller	“Electronic device designed for control of the logical sequence of events.”	[57]
	Ransomware	“A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.”	[55]
	Reliability	“Ability of a system or component to perform its required functions under stated conditions for a specified period of time.”	[57]
	Resilience	“Ability of a system or component to maintain an acceptable level of service in the face of disruption.”	[57]
	Safety	“The condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.”	[57]
SoX	Sarbanes-Oxley	“Regulation aimed at protecting the general public and shareholders from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of corporate disclosures.”	[54]
	Security	“Property of being protected from unintended or unauthorized access, change or destruction ensuring availability, integrity and confidentiality.”	[57]
	Sensor	“Device that observes properties of the physical world and converts them into a digital form.”	[57]
SOC2	Service Organisation Controls	Compliance requirements aimed at minimising the risk and exposure to data.	
	Stuxnet	“Family of cleverly written malware worms that primarily target SCADA (Supervisory Control and Data Acquistition) control systems for large infrastructures such as industrial power plants.”	[61]
SCADA	Supervisory Control and Data Acquisition	“A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (delays, data integrity, etc.) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.”	[57]
SOS	System of Systems	See cyber-physical systems (CPS).	
TOGAF	The Open Architecture Framework	“Open framework for managing enterprise architectures.”	[58]

ABBREVIATION	TERM	DEFINITION / REMARKS	SOURCE
	Wanna-cry	“A strain of ransomware worm that emerged on May 12, 2017, and quickly spread to infect over 200,000 systems in more than 150 countries.”	[61]

*** END OF DOCUMENT ***