SOS! Ensuring safety and security in an expanding system of systems landscape

TNO Publiek › TNO 2023 R11859
28 September 2023

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2023 R11859 – 28 September 2023

SOS! Ensuring safety and security in an expanding system of systems landscape

Author(s)	Sezen Acur, Teun Hendriks, Yoram Meijaard, Carolien van der Vliet-Hameeteman
Classification report	TNO Publiek
Number of copies	TNO Publiek
Report text	TNO Publiek
	TNO Publiek
Number of pages	30 (excl. front and back cover)
Number of appendices	0
Project name	INTERSECT
Project number	060.37563

This publication is part of the project INTERSECT (with project number NWA.1160.18.301) of the research programme Dutch Research Agenda which is (partly) financed by the Dutch Research Council (NWO).

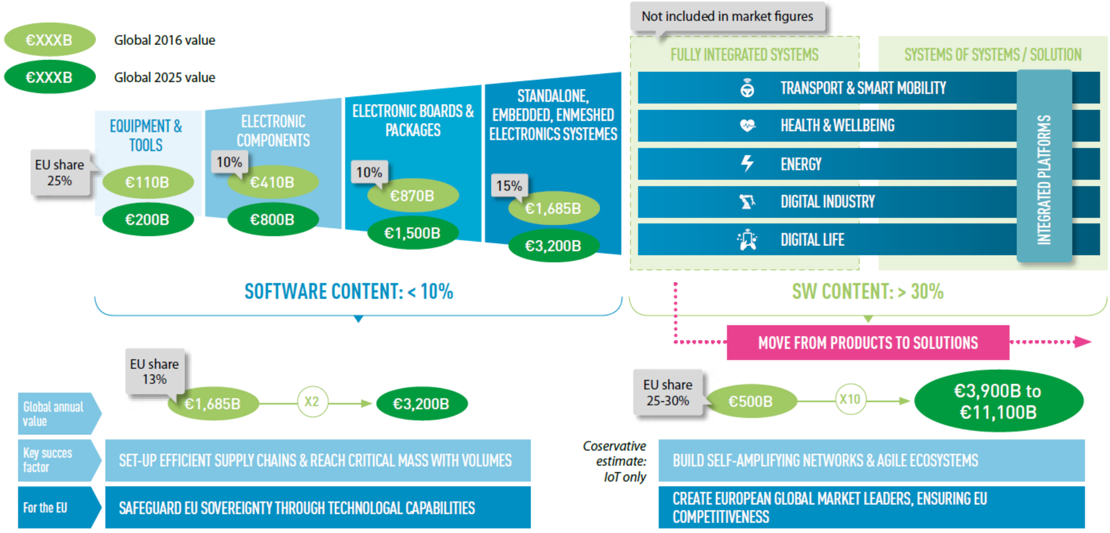
Contents

1 Introduction

1.1 Digitalization increases complexity of systems and drives solution eco-systems

Today's high-tech systems have become very complex. Much of their added value derives from high level software (SW) on top of the mechatronic control of the hardware. This phenomenon is called digitalization and can be observed in many industry sectors. For example, in the automotive industry, for the actual functioning of the components, there is dependence on the SW that provides functionality. This is also applied to semi-conductor suppliers combining SW and HW to create desirable behaviors of the system. Thus, the suppliers increasingly provide SW with their integrated circuits (IC). Next generation vehicles will be 'software-defined' [1]: SW will control the interaction of (most) subsystems, for example to provide a smooth ('magic-carpet') ride to the driver by camera recognition of speed bumps, and then pro-actively adjusting the suspension to compensate appropriately. Digitalization thus can provide very compelling benefits, yet trustworthiness to society must remain assured [2].

Next to trend of digitalization, increasingly systems are deployed in system of systems (SoS) constellations. Smart phones and their app eco-system is perhaps the most well widespread SoS example: smart phones have data incoming from various sub-systems. Combined, the phone provides certain functions such as interacting with an app to check the security cameras at home or stop the rinsing cycle of the washing machine. High tech-systems now see the same trend towards SoS and eco-systems. Also, these, complex, systems integrate components from many suppliers, who in turn work with third parties (sub-suppliers). In fact, the biggest growth for the industry value chain occurs in integrated solutions, with value-add increasingly moving from single products to solution ecosystems, this value created in large part through significant SW content. These trends are quantified in a 2019 report commissioned by ARTEMIS [3] indicating that "[t]he market related to stage 5 ([distributed] solutions and ecosystems) is expected to grow tenfold over the [period 2016-2025], reaching between 3.9 and 11.1 terra Euro according to McKinsey" – see Figure 1Figure 1.


€XXXB Global 2016 value
€XXXB Global 2025 value
Not included in market figures
EQUIPMENT & TOOLS
EU share 25%
€110B
€200B
ELECTRONIC COMPONENTS
10%
€410B
€800B
ELECTRONIC BOARDS & PACKAGES
10%
€870B
€1,500B
STANDALONE, EMBEDDED, ENMESHED ELECTRONICS SYSTEMES
15%
€1,685B
€3,200B
FULLY INTEGRATED SYSTEMS
SYSTEMS OF SYSTEMS / SOLUTION
TRANSPORT & SMART MOBILITY
HEALTH & WELLBEING
ENERGY
DIGITAL INDUSTRY
DIGITAL LIFE
INTEGRATED PLATFORMS
SOFTWARE CONTENT: < 10%
SW CONTENT: > 30%
MOVE FROM PRODUCTS TO SOLUTIONS
EU share 13%
€1,685B
X2
€3,200B
EU share 25-30%
€500B
X10
€3,900B to €11,100B
Global annual value
Key succes factor
For the EU
Coservative estimate: IoT only
SET-UP EFFICIENT SUPPLY CHAINS & REACH CRITICAL MASS WITH VOLUMES
SAFEGUARD EU SOVEREIGNTY THROUGH TECHNOLOGAL CAPABILITIES
BUILD SELF-AMPLIFYING NETWORKS & AGILE ECOSYSTEMS
CREATE EUROPEAN GLOBAL MARKET LEADERS, ENSURING EU COMPETITIVENESS

Note: rounded figures. (1): 2025 estimate value potential for the Internet of Things, not the full potential for ECS end-applications.
Source: Decision, IDC, MGI, Advancy research & analysis

Figure 4: *Global and European value chain 2016-2025*

Figure 1: Trends in the Global and EU value chain including a move from products to solutions.

The primary added value of these distributed solutions is achieved through cooperation between heterogeneous systems to solve more complex problems by exploiting the set of multi-technology, multi-brand and even multi-domain functionalities generated by the cooperation. The system of systems solution emerges from the composition/integration of multiple systems to perform a task or reach an objective that none of the constituent systems can perform or reach on their own [3].

On the flip side however, managing increased complexity and correct functioning of intelligent interaction with changing environment now overwhelms the classical system Verification and Validation (V&V) approach of coping with component failures and correcting all SW bugs. For example, in autonomous vehicles, complete testing at system level is simply infeasible [4]. Two of the reasons mentioned are firstly that the combinations of adverse events and driving conditions that could occur are simply too numerous to enumerate to derive a complete set of requirements and test cases. Secondly, with intelligence based on stochastic (AI-based) technologies, small changes in initial conditions could potentially lead to diverging system behaviors. This means that every system-level test could potentially result in a different outcome despite attempts to exercise nominally identical test cases.

In summary, these trends towards increasing systems intelligence and SoS have significant impact on Cyber-Physical Systems development. We examine this in the next section.

1.2 Impact on systems development

Following market and business trends, systems development today has shifted from the traditional waterfall methodology to evolutionary, agile development methods, as exemplified by the Scaled Agile Framework [5]. Table 1 shows, for a number of system development characteristics, the change in way-of-working. Such changes can be witnessed in, amongst others, the high-tech equipment, and automotive industries.

Table 1: Changing characteristics in systems and systems of systems developments.

	From	To
Scoping	Fit-for-purpose	Future-proof
Performance	Efficient	Scalable
Safety	Managed Risk	Operational Design Domain (ODD) based
Security	Protected	Resilient
Innovation pace	Slow, yearly	Rapid, matter of weeks

With respect to system scope, traditionally scoping was done to achieve fit-for-purpose to satisfy requirements for an individual system or system product line. These days, scoping is forward looking to ensure that next system generations can be created as an incremental evolution of the last system generation. System performance changes from efficient to be scalable, both in (low-end versus high-end) variants of systems as in system-cloud solutions to cater for various numbers of cloud-connected systems. For complex systems, safety moves from managing component and SW risks only towards releasing functionality for use within a restricted operational design domain, e.g., for autonomous vehicles, releasing functionality only for use on highways in dry conditions. Security moves from protection against loss of assets only towards operational resilience, to safeguard business continuity. This all must be made fitting within a much more rapid innovation pace.

Systems are becoming more SW intensive, with the biggest growth occurring in the distributed solutions, from products to solution ecosystems. Managing increased complexity and ensuring desired behavior in interaction with typically dynamic environments now overwhelms the classical V&V approach of coping with component failures and correcting all SW bugs. In response, systems development processes are changing towards evolutionary, agile, scalable, resilient process that provides for a higher innovation pace.

Next, we focus more specifically on the system development characteristics of security and safety.

Security is imperative for systems to achieve and maintain confidentiality, integrity, and availability of information and related (cyber-physical) systems. For example, to protect personal information and intellectual property (PI, IP). With highly complex, highly SW and data intensive systems, security vulnerabilities must be expected, even with due diligence and significant security measures taken.

Safety is important for many systems. For many systems, if safety is compromised, then it can lead to loss of life, injury, or disruptions of critical services. With highly complex, highly SW and data intensive systems, system behavior occurs in interaction with specifics of the context/environment. With highly variable (SoS) contexts or complex environments, exhaustive specification and testing is not feasible due to system and environment complexity, e.g., as mentioned before for autonomous vehicles [4]. Undesired interactions of system functionality for a specific (out of many) environments or contexts then could give rise to safety hazards.

Security and safety have become interlinked. In 2015, white-hat hackers (security researchers) demonstrated that they remotely could take over control of a Jeep Cherokee via its internet connected entertainment system [6]. They even were able to kill its engine remotely while the Jeep was driving on the highway. This hack exposed the risk for security hacks to severely compromise a vehicle's safety. Safety and security are also sometimes conflicting. Patching security vulnerabilities may need rapid updates, but safety considerations may need thorough evaluation e.g., partly repeating clinical trials for medical equipment to ensure no harm will be caused by an update.

With increasing complexity and increasing system intelligence, security and safety has become an ongoing concern, also beyond design and development, i.e., during system operational phase. It is not feasible anymore to resolve all issues during design. Hence, impact of emerging security vulnerabilities and safety issues in system operation must be minimized, until incremental system updates can resolve the root cause.

Safety and security need Systems Engineering (SE) focus. Maintaining safety and security of system of systems in such an expanding landscape is difficult to achieve. It requires full lifecycle consideration. The practice of delegating safety and security to experts as a 'specialty engineering' design task after the system has been conceptualized is not effective anymore [7]. Adapting a system design after the fact for safety and security takes significant time, energy, and efforts. This effect is amplified in a system of systems context. Therefore, the safety and security are best considered already in the early phase of system development, i.e., before a design is fixed. This means that safety and security become integral Systems Engineering (SE) topics.
How safety and security can be embedded integrally into a systems life cycle requires changes to existing methodologies so safety and security can be reflected in the SE process [8]. Next sections will provide further details on Systems Engineering as a discipline, and how systems of systems are conceived from the principles of systems engineering, as a prelude to highlight the safety and security challenges for Systems Engineering.

1.3 Systems Engineering (SE)

Systems Engineering (SE) [9] is an interdisciplinary field focusing on creating a system that fulfills a purpose or need. In an SE lifecycle, the system shall go through the steps of design, integration, validation & verification, and future management including support and retirement of the system. In a changing system of systems landscape, the SE process can create complex systems with due diligence, given that SE's intradisciplinary approach considers the ecosystem of the aforementioned complex systems.

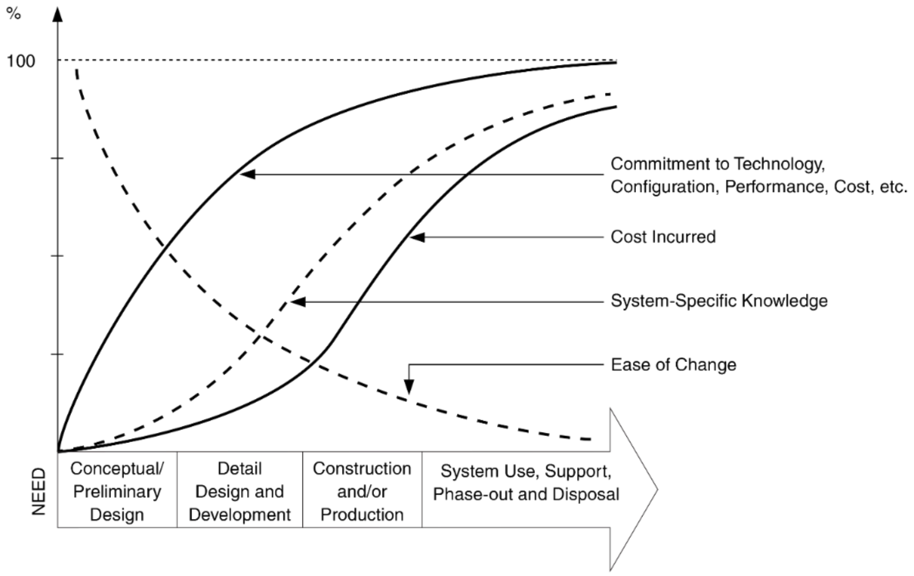


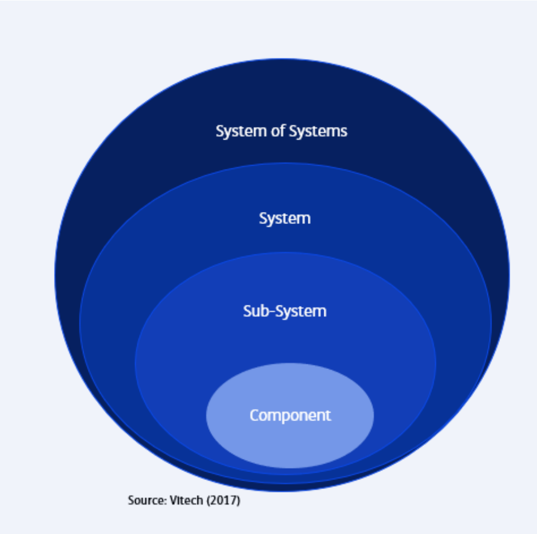
Figure 2: Lifecycle commitment, system-specific knowledge, and incurred costs ([10])

Systems Engineering as a discipline is geared to manage the gap between the fast ramp up of lifecycle commitment versus the slow build-up of system-specific knowledge (see Figure 2). Managing this gap in the Systems Development Lifecycle, and ensuring effective collaboration of the various disciplines (e.g., HW, SW, Electronics, Physics, Data Science, Mechatronics, ..., as applicable) are the key contributions of SE. Some of key deliverables of SE are System Requirements, System Architecture and System Design, V&V plans, Risk Management plans, and Operational & Maintenance Manuals as Lifecycle Support Plans. In these key deliverables, Safety and Security in an increasing system of systems context need to be reflected.

Systems become increasingly connected and used in so-called system of systems constellations. One example of an SoS is a (smart) city mobility system. This SoS comprises of e.g., public transportation networks, ridesharing and private vehicles, scooters and bikes, smart parking, traffic management systems, electric vehicle charging infrastructure, etc. All these systems are interacting and together provide urban transportation and mobility.
Not all SoS are the same in terms of systems development challenges. In the next section, we refer to distinguishing characteristics of SoS, and an SoS typology from literature to clarify SE challenges in system of systems development and operation.

1.4 The landscape of system of systems

The landscape of system of systems is diverse and composes of various aspects such scale, geographic distribution, and complexity [11]. Systems Engineers need to consider the type and characteristics of the encompassing system of system in order to provide for a fitting system. From components to sub-systems, to systems, these all need to provide the right functionality and behavior in the context of the encompassing system of system (see Figure 3).



Source: Vitech (2017)

Figure 3 – Increasing scope from components to System of systems.

Distributed Energy Resource (DER) systems are a second good example of a contemporary system of systems, see Figure 4. DER systems use renewable energy sources (such as wind or solar) to generate 10 Megawatts or less energy. These systems are decentralized, modular and flexible. Management, monitor or control of DER systems is done via public or private networks. As such, they are susceptible to cyberattacks. For example, attacks might impact the stability of the grid by compromising sensor data as to whether there is a surplus or deficit of energy. This may lead to power shortages on the areas served via this system [12]. Depending on the level of openness of such a DER system and SE choices made, the effort required to ensure safety and security of the system might be more or less.

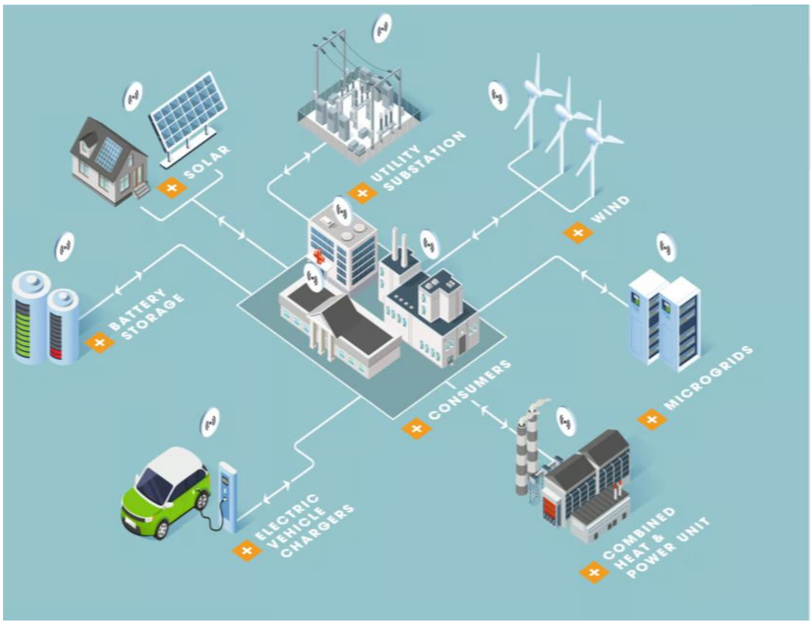


Figure 4: Example of a Distributed Energy System [12]

Knowing the characteristics and types of system of systems can help understand what level of control and management an entity might want to have in order to keep the system safe and secure. Here we follow [11] to explain the various characteristics of system of systems and a categorization of types of SoS. In this reference, various characteristics of system of systems are distinguished as follows:

- Operational Independence
  The components within a SoS are expected to independently function in case such SoS is disassembled. Typically, these components existed prior to becoming a part of SoS and therefore when separated, they can support a new capability.
- Managerial Independence
  The component systems are managed partially rather than entirely for their purposes. That way, even though they can collaborate with other SoS components, they are capable of operating independently.
- Geographic Distribution
  The component systems are geographically dispersed in a large area; therefore, the collaborating systems can only exchange information and knowledge with each other.
- Evolutionary development
  An SoS never fully develops, and it can be under constant change over time as it “evolves”. Additions, modifications, and removal may be experienced within an SoS.
- Emergent Behavior
  Emergence is a byproduct of the global system’s behavior. By having systems working together, an emergent behavior is achieved which individual systems alone could not achieve. This is an objective of SoS as in component systems are expected to work together and achieve such characteristics.

How a SoS is governed, how it evolves, how emergent behavior is controlled or merely occurring may all influences the of constituent systems, and the necessary measures to ensure safety and security of these constituent systems as of the overall SoS.

Based on above SoS characteristics, [11] discerns the following types of system of systems as listed in Table 2:

Table 2: Types of System of systems

Types	Definition
Directed	These are the SoS that are engineered, centrally managed, and meant to fulfill specific purposes. This type of system of systems can also have new purposes that systems owners may want to address.
Acknowledged	There are recognized objectives, a manager, and resources for the acknowledged SoS. On contrary, the systems have independent ownership, objectives, development, and sustainment methods. Once cooperative agreements between the SoS and the system, only then changes in the system are reflected. (i.e., Military joint systems capability. Navy, versus Airforce, versus Army)
Collaborative	The components interact in order to fulfill agreed central objectives yet in the central management, there is no coercive power to run the system. Therefore, these interactions are considered voluntarily. (i.e., V2V in vehicles. Agreements are made in Car to Car Communications Consortium (C2CC).
Virtual	There is neither a central management authority nor an agreed central objective; therefore, virtual SoS emerges from component interactions. Invisible, self-organizing mechanisms maintain virtual SoS. (i.e., decentralized solar energy generation (rooftop etc.)

The nature of SoS creates significant difficulties to ensure correct, safe, and secure, behavior at (constituent) system level [13]. From Table 2, one can infer that, once in SoS central ownership or central management are no longer in place, it becomes harder to achieve, prove, and maintain safety and security of the constituent systems, while operating in an SoS context.

In traditional systems engineering, proof is created through verification and validation approaches. Verification approaches, when applied to the SoS, have problems creating agreement on the standard against which to verify. Conflicting goals, lack of an SoS authority, evolutionary growth, and changes in other systems, or changes in usage of other systems in the SoS context may impact the safety and security of your organization's system [13]. Such changes are not necessarily announced or known in advance of occurrence. Furthermore, a system buyer could decide to deploy your organization's system in other SoS constellations than originally anticipated at design time and tested for in V&V activities. Thus, when a system is deployed in looser SoS contexts, some means of adaptivity and some measure of robustness (resilience) towards changing contexts are needed.

The landscape of system of systems varies from centrally directed SoS to completely ad-hoc, i.e., virtual SoS. More loosely governed / coordinated SoS constellations allow for greater flexibility of usage, yet may result in more complex and interdependent interaction of constituent systems. This makes it harder to ensure safety and security of constituent systems. Overall SoS usage, behavior, and interaction between constituent systems may not necessarily known at design time. Thus, some measure of robustness (resilience) towards changing usage contexts and some means of fielded system adaptivity are needed, to minimize impact of disruptions and ensure business or mission continuity.

The system of systems landscape introduces a next level of complexity. Is there a way to handle the level of complexity and ensure safety and security for systems (especially within system of systems)? More specifically, is there an agreed template or guideline all built systems should comply to? The next section discusses standards and regulations regarding safety and security and associated challenges.

2 Safety and security standards in SoS context

2.1 Introduction

There is an overwhelming body of work being done on standardization and regulation for safety and security. Several standards bodies (e.g., ISO, IEC, NIST) cover safety and security in their work, and further standardization efforts are ongoing. The large body of standards, and the required interpretation to apply them to specific products and development process, presents a significant challenge to the developing organization. In this section, we provide a brief overview of relevant safety and security standards, as regulations for the EU.

2.2 Overview of safety standards

The most commonly known safety standards are of International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Each of them promotes rules, standards, and processes, that are essential to ensure the safety of passengers as well as the driver. Objectives are to prevent system failures, which could lead to injuries and accidents, but also prevent reasonably foreseeable misuse, etc. Especially IEC 61508 [14] is considered to be the foundational safety standard that can be applied to various industry sectors.
A variety of government or private entities established standards for safety, and they are sector specific. For instance, in transportation industry, the safety standards and policies are divided into road, maritime, rail and air. Aside from that, there are also automotive standards which comprises of both technical and non-technical necessities. ISO 26262 [15] and ISO/PAS 21448 [16] are examples.

2.3 Overview of security standards

Similar to safety, a set of security standards are established in order to provide system security within a variety of sectors such as IEC 62443 [17]. ISO/IEC 27000 series [18] provide best practice recommendations for information security including but not limited to privacy, IT, and cybersecurity issues. IEC 61508 [14] covers the interdependencies of safety and security, and new hardware, software, and system development paradigms (object-oriented and model-based design, test and simulation, agile development, cognitive decision, safety of the intended functionality). IEC 61508 comprises of three parts; 1 and 2 being SW and HW while the last part is on SW only containing the mandatory requirements. In IEC 61508 edition 2010, impact of security threats on safety and maintenance of a safety manual became a requirement to consider.

NIST also provides an extensive library of security standards. The NIST SP 800 [19] are commonly popular for the US Defense choice while the NIST Cyber Security Framework (CSF) [20] is specifically for cybersecurity. Furthermore, NIST’s 1800 series [21] is a publication of cybersecurity standards and frameworks intended for real-world technologies which have complex modular background or specific capabilities.

Depending on the context, safety might be more established than security. For instance, in the automotive industry, the first version of the safety standard ISO 26262 stems from 2011. In contrast, the security standard ISO 21434 [22], which covers automotive cybersecurity and compliance, was first published in 2021.

2.4 Regulations

In the European Union, the Network and Information Systems Directive is recently updated, now known as NIS2 [23]. Furthermore, a Cyber Resilience Act is in a proposal stage for negotiation. EU member states need to create national laws for the NIS2 Directive, and when adopted, also for the Cyber Resilience Act. Unfortunately for industries, member states have considerable freedom how to write their national laws, making product compliance on EU level far trivial for industries. Beyond the EU, industries then must comply also with e.g., relevant UK and US law regarding cybersecurity. The automotive industry needs to comply with UN regulations UNR 155 [24] for Cyber Security and UNR 156 [25] for Software Updates.

2.5 Challenges with safety and security standards in SoS context

In general, standardization bodies and standards are slow-moving, consensus-based, while technology and the threat landscape are fast-moving. Given the current complexity of standards, standards cannot provide recipes and checklists for safeguarding. Instead, many standards provide processes to be followed for arriving at safe and secure systems instead, with leave room for interpretation.

In summary, standards compliance only is not sufficient for adequate security and safeguard against adverse impact on safety. In several regions of the world, notably the EU, new regulations are also introduced. The EU directives need to be implemented into national law for each EU member. This brings the concern that countries create slightly different national regulations of e.g., the EU NIS2 Directive, causing effective compliance across the many countries to be difficult.

Safety and security standards are established to provide protection at a certain level for systems. Standards ensure accountability and form the basis for acceptable processes and technical protocols to arrange for safety and security of systems and services. Given the current system complexity, including dynamic environment and uncertainties in SoS contexts, there is no guarantee for certainty via safety and security standards. Indeed, standards alone are not in the position to provide guarantees for safety and security in a system. Furthermore, as standards are slow-moving, while technology and the threat landscape are fast-moving, standards compliance by itself is not sufficient to ensure adequate security and safety.

Safety and security standards do help to provide accountability and do provide best practices and processes for organizations to work towards ensuring safety and security of their products. However, given increasing systems complexity and varying system and SoS contexts, safety and security standards are not in a position to provide recipes or nor guarantees that a system during its lifetime will remain safe and secure using measures installed and verified during development.

Instead, safety and security have become lifecycle concerns: they must be addressed during the whole lifetime of a systems, significantly also during system operation. The next section will highlight two reasons for this: the role of inherent uncertainty within system of systems, and the impact of potential changes in the socio-technical context of systems, i.e., system stakeholders or owners.

3 Safety and security are lifecycle concerns for system of systems

Safety and security are emergent properties of a system. There is no one method to 'provide safety and security', rather, safety and security of a system emerges from numerous decisions made by during the design and development of the system. No standards nor proprietary methodology can guarantee these properties 'by-design'. This does not absolve developing organizations from addressing safety and security thoroughly during system development, on the contrary. However, work is not done once a system is released to the field.

Safety and security have become lifecycle concerns: they must be addressed during the whole lifetime of a systems, significantly also during system operation. In this section, we highlight two key reasons for this, the increasing level of uncertainty over the lifecycle, and the impact of changes in the socio-technical context of systems.

3.1 The level of uncertainty over the lifecycle of SoS is increasing

Given varying or evolving contexts and environments, ensuring safety and security within system of systems is difficult. Not everything can be anticipated, the complexity and uncertainty may cause unavoidable gaps of knowledge or ignorance to surface towards safety and security on a person's or an entity's view. In particular, security vulnerabilities and day-0 exploits are bound to surface from time to time in today's SW intensive systems. Hence safety and security must be managed over the lifecycle to address such gaps of knowledge surfacing over time and impacting system operation.

Along with complexity and human behavior comes ignorance, uncertainty, and risk affecting system functionality. According to [26], successfully creating, operating, and maintaining engineering systems requires addressing such levels of uncertainty with respect to the stakeholders. If the stakeholders align and agree on a solution collectively, then the level of diversity is considered commensurate. If the stakeholders do not align and there is no collective solution, it is considered incommensurate. Depending on the level of 'unknown-ness' (shown in the chart under level of uncertainty) and if the stakeholders are aligned or not, the solution to a problem may range from applying a precautionary principle to risk management and decision analysis.

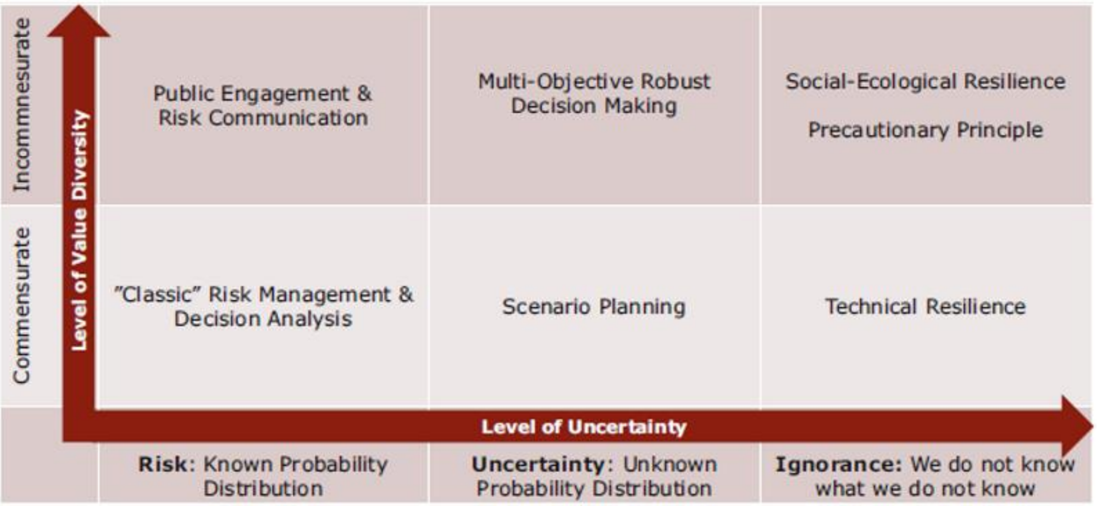

Incommensurate
Commensurate
Level of Value Diversity
Public Engagement & Risk Communication
Multi-Objective Robust Decision Making
Social-Ecological Resilience
Precautionary Principle
"Classic" Risk Management & Decision Analysis
Scenario Planning
Technical Resilience
Level of Uncertainty
Risk: Known Probability Distribution
Uncertainty: Unknown Probability Distribution
Ignorance: We do not know what we do not know

Figure 5: Managing risk, uncertainty, and ignorance in engineering systems design [26]

The following are the three types of possible situations with levels of 'unknown-ness', which could jeopardize the proper functioning of a system:

- Risk: Possible outcomes and probabilities are known [27]
- Uncertainty: Possible outcomes with unknown probabilities [27]
- Ignorance: Unknown outcomes with unknown probabilities [28]

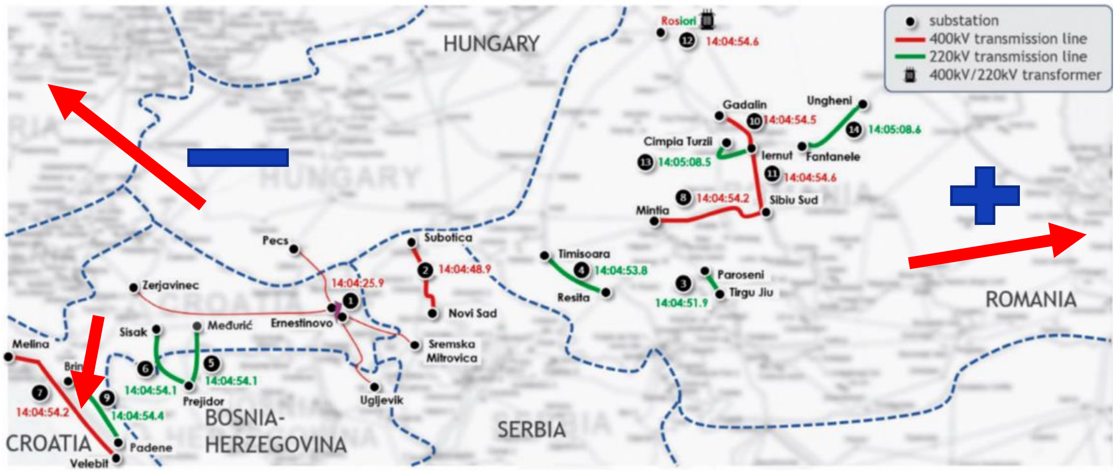


Figure 6: Map view of the 8 January power supply failure incident [29]

To illustrate these concepts, we look at a power grid incident that occurred a few years ago. On 8 January 2021, a power supply failure in between Croatia and Serbia caused splitting of the continental synchronous area in Europe as multiple transmission network elements has tripped. This caused a ripple effect and resulted in power deficiency in the north-west area of Europe and surplus in the south-east area which further disrupted the frequency in both regions for approximately one hour [30]. After one hour, the transmission system operators from Slovenia ensured that the power was restored to normal operation; however, locally managing electricity flow in short notice required larger local flexibility resources, which was not available at the time [31]. The probability and outcome here were unknown, showing an example of ignorance. Furthermore, as north-west area was impacted by the frequency deviation, electricity services in France and Italy was disconnected as some received less than the frequency threshold of 50 Hz. The providers came up with a solution but did not know how long that would have helped as they were resolving the deficit issue, leads to the aspect of uncertainty. The disruption and a lack of operating reserves in the Northern European region nearly caused a blackout which is considered to be a high-level risk. In the European report, in order to avoid further incidents, the recommendation has been that “power operations become resilient to cope with unexpected disturbances and faults to guarantee unchanged high security of supply of European customers”. [30]

Modern system of systems are large and complex, which means they have potential weaknesses and possible residual flaws. Unavoidable gaps w.r.t. knowledge in safety and security are to be expected within such complex systems. This increases chances of encountering situations in operation where uncertainty, ignorance and risks could affect system operation. Collective stakeholders agreements of on a solution approach is important to determine what steps to take in case of unexpected incidents or events, in order to be resilient, provide for business continuity and rapid incident recovery.

3.2 Uncertainty may be caused by context changes during the SoS lifecycle

Another rationale to manage safety and security over the entire SoS lifecycle is the unpredictable nature of the context of the SoS. The context of an SoS includes the involved stakeholders in the SoS, which may be *direct owners of systems* or *suppliers of components/subsystems*. This organizational context of a SoS yields requirements and objectives for the safety and security of the entire SoS. For example, these requirements can take the form of contractual agreements regarding safety levels, agreed-upon functionally of the SoS, or shared liability for security.

A change in context includes changes in ownership of any of the stakeholders involved in the SoS, whether that is the primary owner or any party within the supply chain. Changes in ownership can occur, for example, by mergers or acquisitions. Moreover, during the SoS lifecycle it may be that new stakeholders emerge and conversely, that previously important stakeholders no longer play a role. A typical example of a newly emerging stakeholder are government regulators that need to enact a new piece of legislature. These context changes are hard, if not impossible, to predict and are therefore another source of uncertainty.

The effect of contextual changes on the safety and security of an SoS can be illustrated by considering the supply chain. A supply chain is a network of collaborating parties. The collaboration is possible due to shared objectives. The result of these objectives are agreements between the different parties to deliver goods/services of an agreed upon quality and quantity. When a single party changes their objectives, this can lead to malfunctioning of the supply chain. A change in ownership is a typical trigger to changes in objectives. Note that this may be due to entirely legitimate reasons. For example, after an acquisition of a security vendor, the parent company changes the objectives of the daughter company to align better with the objectives of the parent company. By doing so, they no longer deliver a product that was critical for the security of the resulting SoS.

Note that context changes can occur at any phase of the SoS lifecycle. In other words, the requirements that follow from the context of the SoS are not fixed for the duration of the SoS lifecycle. When the SoS enters a new phase in its lifecycle, changes in context are more likely to occur. Schematically this is depicted in Figure 7 where the transition between lifecycle phases may trigger context changes.

For system engineers, this means that at some point they need to deal with changes in context. These changes may change or introduce entirely new objectives for the SoS. As such, the possibility of these changes should be considered in the systems architecture. Resiliency measures aimed at reduced impact from contextual changes are key to ensure safety and security.

Contextual changes over the lifecycle of SoS, in terms of ownership and (supply chain) stakeholders, may impact security and safety of the SoS, even if the SoS itself did not change. Accommodating changing stakeholders, usage or context may require consideration in the architecture of the SoS and/or modification of the SoS during its operational lifetime.

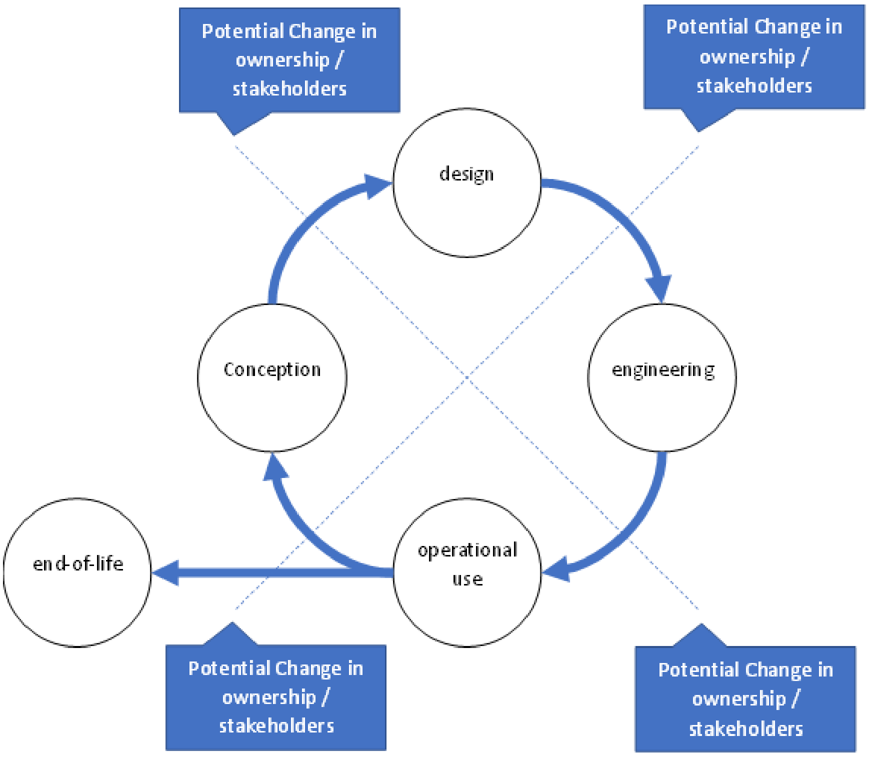

Potential Change in ownership / stakeholders
Potential Change in ownership / stakeholders
design
Conception
engineering
end-of-life
operational use
Potential Change in ownership / stakeholders
Potential Change in ownership / stakeholders

Figure 7: Changing phases in a SoS lifecycle can trigger changes in context of the SoS, particularly with respect to the ownership of the SoS and its relevant (supply chain) stakeholders.

Within the systems engineering (SE) community, new ways are looked for to integrate safety and security with the principles of SE and adapt SE methodologies accordingly. Next sections elaborate on how safety and security could integrate in SE, and first steps towards SE instilling resilience in sytems to support business continuity and rapid incident recovery.

4 The Future of SE calls for SE to integrate safety and security

In the traditional systems engineering process, safety and security are ‘bolted on’ after the system architecture and decomposition are determined and delegated to specialty engineering disciplines [32]. As the problem analysis in that paper bears out, ‘bolting-on’ safety and security as specialty-engineering after the fact is not effective anymore. This sentiment is echoed in the INCOSE Vision 2035, [33], in which Systems Engineering is expected to incorporate safety and security in the SE system development life cycle. Simultaneously, INCOSE is undertaking a number of Future of Systems Engineering (FuSE) investigations to create roadmaps. INCOSE’s FuSE security initiative [32]and associated project charter call for expertise in safety and security to be integrated in the SE team.

INCOSE’s FuSE Security initiative has formulated six SE objectives and eleven foundational concepts for integrating security in SE (see Figure 9). In development of future systems, security is expected to be is embedded in systems engineering, and security agility is practiced both with respect to enabling rapid systems innovation (architectural agility) as rapid adaptation of fielded systems (operational agility).

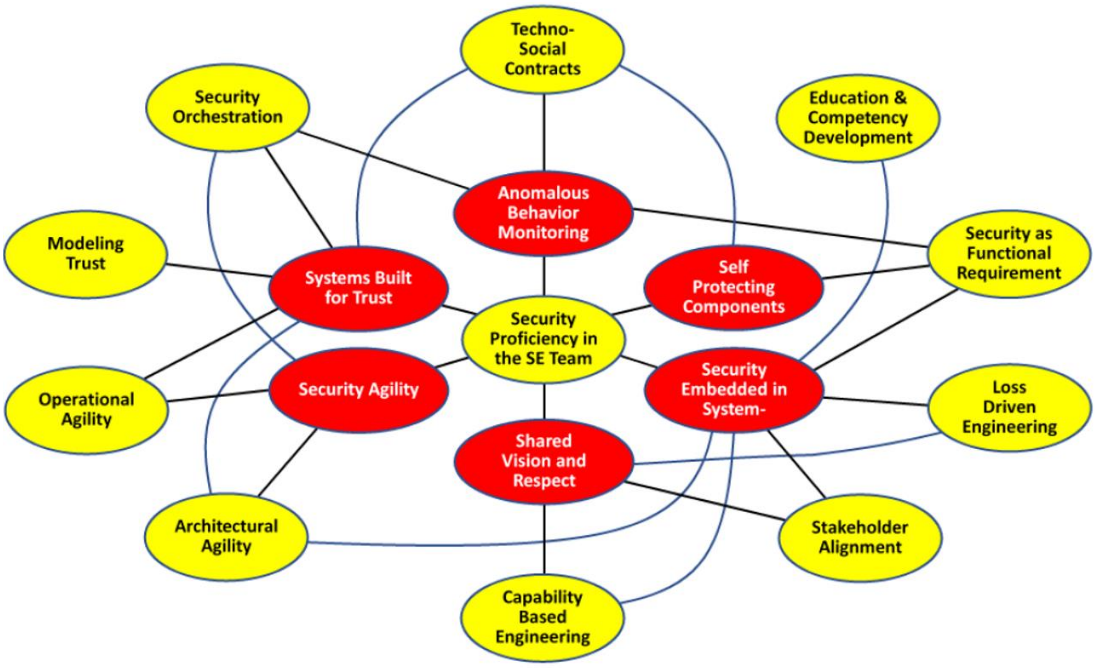

Techno-Social Contracts
Security Orchestration
Education & Competency Development
Anomalous Behavior Monitoring
Modeling Trust
Systems Built for Trust
Self Protecting Components
Security as Functional Requirement
Security Proficiency in the SE Team
Operational Agility
Security Agility
Security Embedded in System-
Loss Driven Engineering
Shared Vision and Respect
Architectural Agility
Stakeholder Alignment
Capability Based Engineering

Figure 8: FuSE Synergistic Linkage Between SE foundation concepts and SE security objectives (concepts in yellow and objectives in red ovals) [32]

These concepts and roadmap aim to tackle current SE problems with security. For instance, security agility today is insufficient: the response capability to respond to emerging security threats and events is not able to respond to threats in a timely fashion, and not capable to keep up with the evolving threat landscape, in both knowledge and response capabilities. Part of this problem is that the systems engineering level, insufficient knowledge of system security engineering is available, also to communicate across knowledge and expertise boundaries.

SE needs to move security and resilience analyses to much earlier development phases. Traditional vulnerability assessments and risk/consequence models for security, safety, and related ‘ilities occur too late in the SE process. Thus, SE should embrace a harmonized loss-driven engineering approach [34]: “loss” provides a more consistent metric than traditional risk/vulnerability metrics focused on design only. Then SE will be able to perform top-down security considerations starting with desired results/value rather than selecting / applying available solutions, in order to achieve better alignment across solutions, and enabling better security orchestration during systems operation. Stakeholder alignment is key for the success of these activities.

SE should be able routinely evaluate and incorporate requirements to enhance systems and information security and resiliency to security threats early in the SE process. Furthermore, SE should be able to manage and update incident response capabilities over the full system life cycle, not only “by-design”.

Integrating safety and security in systems engineering has definite benefits for the system and its development by considering threats early and focusing on desired results and synergy of solutions. Yet, SE also needs to consider the impact of the unexpected incidents and how to cope with dynamic environment, uncertainty and resulting risks to the system. For this SE needs to be able to develop a resilient system and support this resilience throughout the entire system life cycle. The next section looks at two initiatives to strengthen resilience in SE.

5 How can SE ensure resilient safety and security over the full lifecycle?

So, Systems Engineering needs to adopt a proactive approach to help identify and address potential security vulnerabilities and safety issues from the early stages of design all the way to system retirement. Disruptions to system operation are a realistic as a scenario, and when occurring, need to be to be responded to in a timely fashion.
Business continuity in face of security or safety disruptions requires systems to be *resilient*, i.e., possess the ability to prepare for, and adapt to, changing conditions and withstand and recover rapidly from disruptions. Such resilience includes the ability to anticipate, withstand and recover from deliberate attacks, accidents, and also naturally occurring threats or incidents. [35]In complex SoS manifesting an unavoidable lack of knowledge at design time, and hidden weaknesses and vulnerabilities, resilience has thus become a key ‘ility.

Resilience, the capability to withstand and recover from disruptions, expands the scope of safety and security. Security engineering is primarily concerned with the protection of assets and is primarily oriented to the concept of asset loss. Resiliency engineering is rather oriented toward capabilities and harms to systems. System resilience focuses on capabilities that support missions or business functions and aim to minimize the effects of adversarial actions on systems, and impact on their capabilities and system usage behavior. Even when the misuse is non-disruptive to the system of interest, it could reduce confidence in system capabilities, and alter system usage behavior to affect external systems, possibly resulting in cascading failures in other parts of the SoS.

So, how to achieve systems resilience, especially against cyber- threats? Recent work is addressing this question. In the following sections we present two significant solution directions, the first work establishing resilience engineering and listing foundational principles, and the second proposing how to integrate resilience into the SE workflow.

5.1 Foundational principles for systems resilience

Systems resilience has a strong relation with business / mission continuity. A key challenge for achieving resilience is how to distribute the relevant functionality, redundancy, and monitoring over the constituent systems and within the system of interest. The National Institute of Standards (NIST) is investigating cyber resiliency and cyber resilience engineering, which intends to architect, design, develop, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources [35].
NIST provides the following foundational principles of engineering for system resilience [35]:

- **Focus on the mission or business functions.** Systems resilience needs a focus on capabilities supporting organizational missions or business functions in order to maximize the ability of organizations to complete critical or essential missions or business functions despite an adversarial presence in their systems and infrastructure threatening mission-critical systems and system components.
- **Assume a changing environment.** Both the operational as threat environment will have ongoing and episodic changes in the system users; also, adversaries learn from experience: usage scenarios as motives may change hence over time.
- **Focus on the effects of the disruptions and threats.** System resiliency analysis focuses on the effects that disruptions or threats can have on the system of interest and, thereby, on the missions or business functions, organization, or external stakeholders.
- **Assume adversaries will compromise or breach the system or organization and may maintain a prolonged presence in that system or organization.** Modern systems are large and complex entities, and adversaries will always be able to find and exploit weaknesses and flaws in the systems, in the environments of operation (e.g., social engineering), and supply chains.

The organizational and SE risk management strategy should reflect these principles to drive resilience goals and objectives, and from thereon perform appropriate selection and prioritization of resilience design principles and techniques to apply into a system. NIST provides foundational principles and a first reasoning framework to select resilience solutions in [35]. MITRE provides a web-based 'CREF navigator' [36]codifying this NIST framework in an easy-accessible web page.

SE should incorporate resilience thinking/engineering, to drive system capabilities that support mission or business functions, yet also minimize the effects of incidents and adversarial actions on systems, as impact on their capabilities and system usage behavior.

Systems resilience is an important capability for SE to strive for in relation to safety and security. Nonetheless, also for resilience no absolute guarantees cannot be given. Thus, the efficacy and adequacy of proposed resilience solutions to support business continuity needs assessment. Trade-offs must be decided upon across contradictory, competing, and conflicting needs and constraints including risk, cost, time, and effort. Such assessment and decision making should be integral part the SE workflow. The next section shows a promising SE method how to do this.

5.2 Integrating resilience into the SE workflow

Integrating resilience into the SE workflow requires a collaboration of systems engineering, safety and security, operations, and system test (as part of SE). Work by the Systems Engineering Research Center (SERC) has created a methodology called Cyber Security Requirements Methodology (CSRM) [37] to incorporate resilience for security. This methodology bears promise to be extended with resilience for safety, in particular for safety-of-the-intended-functionality.

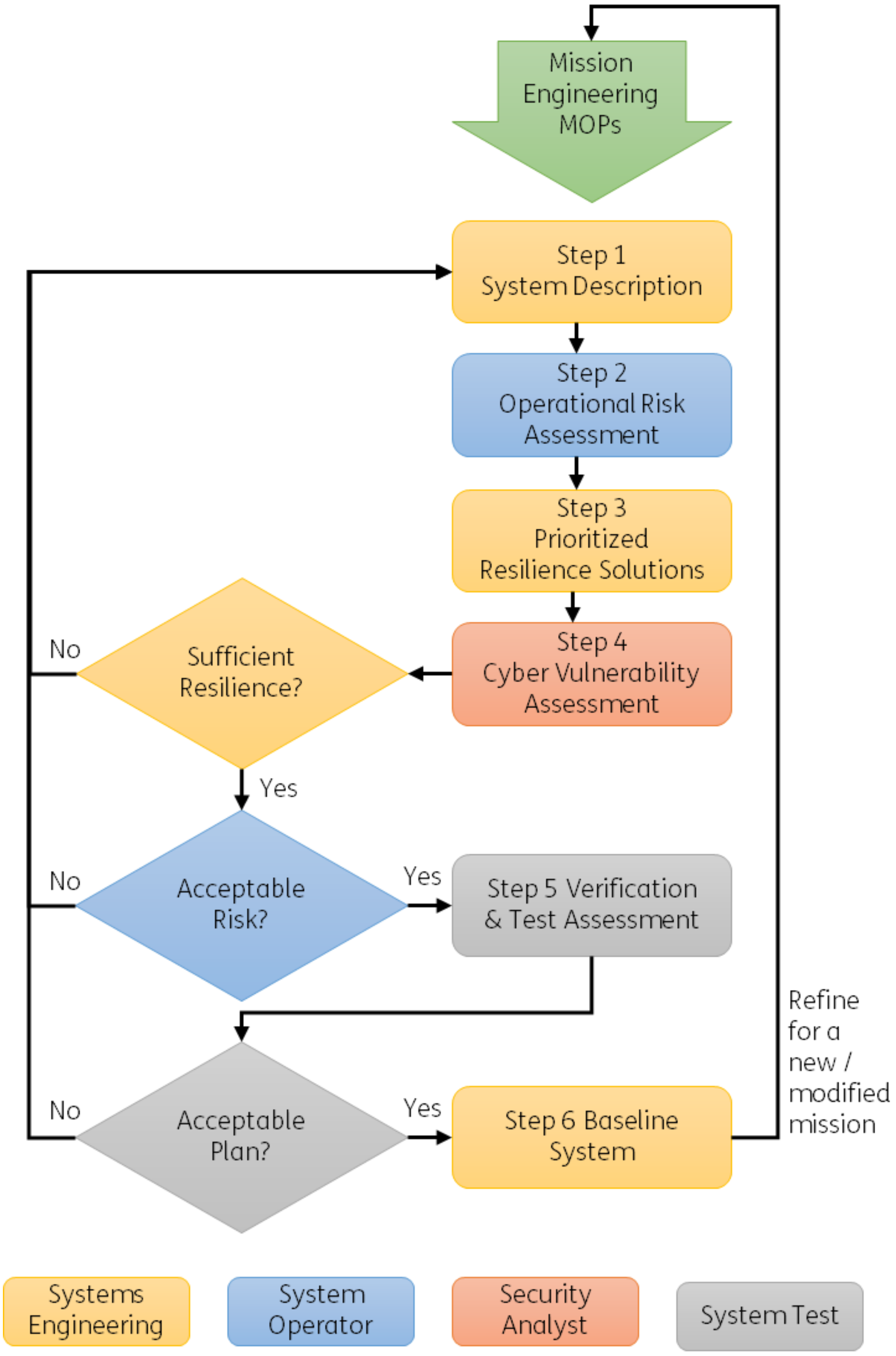

Mission Engineering MOPs
Step 1 System Description
Step 2 Operational Risk Assessment
Step 3 Prioritized Resilience Solutions
Step 4 Cyber Vulnerability Assessment
Sufficient Resilience?
No
Yes
Acceptable Risk?
No
Yes
Step 5 Verification & Test Assessment
Acceptable Plan?
No
Yes
Step 6 Baseline System
Refine for a new / modified mission
Systems Engineering
System Operator
Security Analyst
System Test

Figure 9: CSRM workflow with relevant experts in the process [37]

CSRM seeks to support and enhance current techniques used for the preliminary design of CPS with a minimally intrusive process for also addressing system cybersecurity (and potentially SOTIF) requirements. Due to the nature of the available means to improve system cybersecurity—defense, resilience, and enhanced development and design practices—it is desirable to identify such requirements as early as possible and before significant design and architecture choices are finalized.

CSRM identifies potential resiliency solutions based on the mission and system descriptions; inputs from stakeholders such as system operators, owners, and cyber-security experts (and potentially SOTIF experts); and the judgment of the systems engineering team. This end-to-end SE methodology models loss scenarios, hazards, threat activities, resilience requirements, system resilience modes of operation, control-driven representations of security requirements, and test and evaluation activities.

The SE workflow of the CSRM methodology is shown in Figure 9. Four teams participate in this workflow: system engineers, system operators, security experts, and system test personnel. These trams are responsible for the relevant steps as colored it the workflow. This workflow iterates until all teams are satisfied with the system and the solutions. Overall, the resilient system becomes the new baseline system after the review of engineers. The early phase interdisciplinary collaboration and assessment as proposed by CSRM is a key benefit: cyber-resilient induced change is easier to accommodate, and less cost already committed (see section 1.3).

> CSRM provides SE with a methodology to addresses interdisciplinary collaboration needed to improve and increase resilience in early on in systems design. Collective agreement between experts indicate that the system has been reviewed for functionality against safety and security concerns. Therefore, system design can resume as a baseline also for later changes when fielded to adapt to changes in environment when safety and security incidents would occur.

6 Conclusion

6.1 Summary

Security and safety are emergent properties of a system and are interlinked: security breaches may cause safety incidents. No system can provide absolute security and safety due to limits of human certainty, the uncertainty that exists in the lifecycle of every system, and constraints such as cost, schedule, performance, feasibility, and practicality [38] . As such, systems engineers must make trade-offs across contradictory, competing, and conflicting needs and constraints to provide adequate levels of safety and security, whilst keeping the system operational.

The system of systems landscape is changing, which makes it more difficult to ensure safety and security. Systems are increasingly complex, software intensive, and deployed in distributed system of systems and solution ecosystems. Systems still need to be correct and display safe behavior, even when interacting with this dynamic environment. Proving these properties now overwhelms the established Verify & Validate approach used by system engineers to cope with component failures and software bugs.

Safety and security standards are established to provide guidelines for the protection of systems. Standards are the basis for acceptable processes and technical protocols to arrange for safety and security of systems and services. However, compliance to a standard does not provide guarantees nor certainty with respect to safety and security of a system.

In fact, today's large and complex system of systems invariably have potential weaknesses and possible residual flaws. Unavoidable gaps w.r.t. knowledge in safety and security are to be expected within such complex systems. It can be expected that during operation situations will be encountered where such lack of knowledge is at the root of incorrect or unsafe system operation. In case of such events, upfront and collective stakeholders agreements are then important to determine what steps to take in order to achieve rapid incident recovery, provide business continuity and remain resilient.

Consequently, systems engineering should embed safety and security in its SE process over the full system lifecycle. SE should be able evaluate and incorporate requirements to enhance safety and security early in the SE process. Furthermore, SE should be able to manage and update incident response and recovery capabilities over the full system lifecycle to make the system capable to anticipate and withstand attempts to disruption.

This position paper advocates for SE to incorporate resilience thinking/engineering in its SE process, to drive system capabilities that support mission or business functions, yet also minimize the effects of incidents and adversarial actions on systems, as impact on their capabilities and system usage behavior. Collaboration of systems engineering, safety and security, and operations is now crucial for creation and operation of complex, yet resilient, systems and SoS which fulfill the needs of society, and are trustworthy for society.

Two initiatives to do so are described in this paper. Firstly, *Cyber Resilience Engineering* [35] which defines foundational principles and a reasoning framework for systems to improve their capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises. Secondly, the *CSRM* [37] risk-based methodology for SE to address cyber security during the early design phase of cyber-physical system, in collaboration with system owners and experts from a wide range of domains, included security, operations, and system test. CSRM addresses the necessary interdisciplinary collaboration needed to assess and increase resilience in systems.

6.2 Next steps and call for action

The collaboration of systems engineering, safety and security is crucial for creation and operation of resilient systems and SoS which fulfill the needs of society and are trustworthy for society. SE should ensure that effects of incidents and adversarial actions on systems are minimized, and disruptions in operation quickly responded to, and recovered from.

Collaboration of systems engineering with safety and security, but also operations is called for to instill adequate resilience in systems. Foundational principles are identified, and an overall methodology now suggested. However, practical guidelines are missing.

Next steps now are to investigate how to make cyber-resilience practical. How to assess threats, how to enable orchestrated response and recovery. When are counter measures adequate? How to give guidance to various disciplines and how to maintain and update know-how on the threat and vulnerability landscape and adapt resiliency strategies accordingly.

To the reader of this paper: if you are interested to improve the business continuity prospects of your system and improving its resilience, please contact TNO for further information. With your system and problem as practical case study, we at TNO can investigate the necessary steps, practicalities, and guidelines of how achieve adequate resilience supporting needed business continuity and trustworthiness of your system to its stakeholders and society at large.

Within the INTERSCT project, TNO is working on Cyber Resilience (Systems) Engineering.

The authors of this position paper invite you to cooperate with TNO on improving the business continuity prospects of your system and strengthening its resilience.

Acknowledgments

The authors wish to thank Andre Smulders for his significant contributions to this paper.

7 References

[1] A. Zhou, R. Liu, G. Lu, Y. Zhou, T. Wang and W. Liu, "Software-Defined Vehicles - A Forthcoming Industrial Revolution," 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/consumer-business/deloitte-cn-cb-software-defines-vehicles-en-210225.pdf. [Accessed 15 August 2023].

[2] P. Neumann, "How Might We Increase System Trustworthiness?," *Communications of the ACM,* vol. 62, no. 10, pp. 23-25, 2019.

[3] ARTEMIS IA, "Embedded Systems: Trends and Challenges," 2019. [Online]. Available: https://artemis-ia.eu/news/embedded-intelligence-trends-challenges-book-release.html.

[4] P. Koopman and M. Wagner, "Challenges in autonomous vehicle testing and validation," *SAE International Journal of Transportation Safety,* vol. 4, no. 1, pp. 15-24, 2016.

[5] SAFe, "Scaled Agile Framework," 20 August 2023. [Online]. Available: https://scaledagileframework.com/.

[6] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway - With Me in It," 21 July 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[7] J. Brtis and M. McEvilley, "Unifying Loss-Driven Systems Engineering Activities," *INSIGHT,* vol. 23, no. 4, pp. 9-13, 2020.

[8] TNO ESI, "System security: challenges and opportunities in creating secure high tech systems," 2021. [Online]. Available: https://esi.nl/research/output/leaflets.

[9] R. Haberfellner, O. de Weck, E. Fricke and S. Vössner, Systems Engineering, Cham: Springer International Publishing, 2019.

[10] B. Blanchard and Fabrycky, Systems Engineering and Analysis, 5th ed., Upper Saddle River, NJ: Pearson Education, Inc., 2011.

[11] J. S. Dahmann, "Systems of systems characterization and types," *Systems of Systems Engineering for NATO Defence Applications (STO-EN-SCI-276),* pp. 1-14, 2015.

[12] Stantec, "Powering communities through the energy transition," 2023. [Online]. Available: https://www.stantec.com/en/markets/energy/grid-modernization/distributed-energy-resources.

[13] E. Honour, "Verification and Validation Issues in Systems of Systems," *arXiv preprint arXiv:1311.3626,* 2013.

[14] IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission (IEC), 2010.

[15] ISO 26262, "Road vehicles — Functional safety," International Organization for Standardization (ISO), 2018.

[16] ISO/PAS 21448, "Road vehicles — Safety of the intended functionality," International Organization for Standardization (ISO), 2022.

[17] IEC 62443, "Industrial communication networks-network and system security," International Electrotechnical Commission (IEC), 2013-2018.

[18] ISO/IEC 27000, "Information technology — Security techniques — Information security management systems — Overview and vocabulary," ISO and IEC, 2018.

[19] NIST SP 800 Series, "Computer Security Resource Center - SP 800 Series," 13 June 2023. [Online]. Available: https://csrc.nist.gov/publications/sp800.

[20] NIST CSF, "CYBERSECURITY FRAMEWORK," 13 June 2023. [Online]. Available: https://www.nist.gov/cyberframework.

[21] NIST SP1800 series, "NIST Computer Security Resource Center - SP1800 series," 14 June 2023. [Online]. Available: https://csrc.nist.gov/publications/sp1800.

[22] ISO 21434, "Road vehicles — Cybersecurity engineering," International Organization for Standardization (ISO), 2021.

[23] Directive (EU) 2022/2555, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E," 14 December 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[24] UN R155, "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," United Nations ECE, 2021.

[25] UN R156, "Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system," United Nations ECE, 2021.

[26] J. Oehmen and J. Kwakkel, "Risk, Uncertainty, and Ignorance in Engineering Systems Design," in *Handbook of engineering systems design*, Cham, Springer International Publishing, 2021, pp. 1-31.

[27] F. H. Knight, Risk, Uncertainty, and Profit, Boston: Houghton Mifflin, 1921.

[28] M. Smithson, Ignorance and uncertainty: Emerging paradigms, New York: Springer-Verlag Publishing, 1989.

[29] Modernpowersystems, "The 8 January system separation," 25 February 2021. [Online]. Available: https://www.modernpowersystems.com/features/featurethe-8-january-system-separation-8550370/.

[30] ENTSO-E, "ICS Investigation Expert Panel," 15 July 2021. [Online]. Available: https://eepublicdownloads.azureedge.net/clean-documents/SOC%20documents/SOC%20Reports/entso-e_CESysSep_Final_Report_210715.pdf.

[31] G. Novak, "LinkedIN," 23 March 2021. [Online]. Available: https://www.linkedin.com/pulse/day-europes-power-grid-almost-faced-massiveblackout-gregor-novak.

[32] R. Dove, K. Willett, T. McDermott, H. Dunlap, D. P. MacNamara and C. Ocker, "Security in the Future of Systems Engineering (FuSE), a Roadmap of Foundation Concepts," in *INCOSE International Symposium*, Honolulu, HI, 2021.

[33] INCOSE, "SE Vision 2035," 2023. [Online]. Available: https://www.incose.org/2023_redesign/publications/se-vision-2035.

[34] INCOSE, "Loss-Driven Systems Engineering," *INSIGHT,* vol. 23, no. 4, pp. 1-33, 2020.

[35] NIST SP 800-160 vol. 2, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," National Institute of Standards and Technology, Gaithersburg, MD, 2021.

[36] MITRE, "CREF navigator," 2023. [Online]. Available: https://crefnavigator.mitre.org/inspector.

[37] T. Sherburne, M. M. Clifford, B. M. Horowitz and P. A. Beling, "The Cyber Security Requirements Methodology and Meta-Model for Design of Cyber-Resilience," in *Systems Engineering for the Digital Age: Practitioner Perspectives*, Hoboken, NJ, John Wiley & Sons, Inc., 2023, pp. 539-554.

[38] NIST SP 800-160 vol. 1, "Engineering Trustworthy Secure Systems," National Institute of Standards and Technology, Gaithersburg, MD, 2022.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life