Engineering Technology Open Access Journal

Juniper Publishers key to the Researchers

Short Communication
Volume 3 Issue 5 - February 2021
DOI: 10.19080/ETOAJ.2021.03.555622

Eng Technol Open Acc

Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice

Chaminda Hewage*

Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom

Submission: February 05, 2021; **Published:** February 17, 2021

***Corresponding author:** Chaminda Hewage, Cardiff School of Technologies, Cardiff Metropolitan University, UK

Abstract

The emergence of Industry 4.0, Industry IoT (IIoT), Internet of Everything (IoE), Internet of Medical Things (IoMT) and Cyber Physical Systems (CPS) have created a paradigm shift in the way we design, develop, operate and manage engineering systems. At present, most of the legacy and modern engineering systems/applications are connected via Internet or private networks to provide an efficient service as well as to manage the system productively (e.g., automation). Even though, these interconnected systems pave the way for more technological and business opportunities, these also introduce additional risks to the system and outcome. For instance, unauthorised access to a CPS could end up in a disaster and malicious access to a SMART home application could have an adverse impact on the individuals at home. Prior to the wider deployment of internet, everyone was concerned about the health and safety of the system or its output. With the network (both Internet and internal networks) being the primary command and control channel or the mechanism for automation, the importance of integrating cyber security with health and safety practices has become a priority. In response, it is understood and agreed in general that having good cyber security always help to achieve better health and safety from engineering systems. This article elaborates on the challenges, opportunities and strategies to integrate cyber security and safety in engineering best practices.

Keywords: Cyber security and safety; Security by design; Security by default; Secure systems; Industry Control Systems (ICS); Cyber Physical Systems (CPS); IIoT

Introduction

In traditional engineering practice, cyber security and safety do not go hand in hand in an organization's general operation and management. Often both of these aspects are two different functionalities within an organization and managed by two separate departments. Safety standards in engineering such as IEC 61508 [1] and RTCA DO-356A/EUROCAE ED-202A [2] highlight the importance of addressing cyber security concerns to achieve better system safety. However, current safety and cyber security standards do not provide detail guidelines on how they can work together. It is important to integrate these two practices due to the increased use of digital technologies to manage safety systems (e.g., Industry Control Systems (ICS), Industry IoT).

The consequences of cyber-attacks are two fold;

a) Cyber attack may not intend to attack the safety system (e.g., data theft).

b) The main purpose of the attack could be to compromise the safety system.

The later is the main target by Nation state actors, who can device a complex attack towards safety systems. The impact could be either the system itself being compromised (e.g., Cooling system of a Turbine) or the productivity of the Engineering system being compromised (e.g., Low electricity generation). Figure 1 demonstrates the usage and aims of cyber security and safety in systems engineering. In order to achieve optimum outcomes from a system, these two disciplines need to be jointly designed and work together.

If safety related Operation Technology (OT) is not secured, the system cannot be categorized as safe. Therefore, joint approach is required to tackle the cyber security and safety risks together as discussed in [3]. The IET and NCSC have recently published a code of practice for engineering practitioners about how these distinguished functional units within an organization can work towards lowering the risks created by lack of cyber security and safety measures [4]. Another code of practice by IET guides cyber security practice in building industry in [5]. The National

Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience [6] in US highlights how government and private sector organizations should work together to manage risks and achieve security and resilience outcomes for critical infrastructure. Under this initiative, the 2015 Sector-Specific plans have established goals and priorities for the sector that address their current risk environment, such as the nexus between cyber and physical security. Currently this covers 16 critical infrastructure sectors including energy, water and wastewater, nuclear reactors, dams' sector, etc. [7]. Similar code of practices or best practice guidelines are in need to elaborate how organizations can jointly minimize cyber security and safety risks of modern engineering systems.

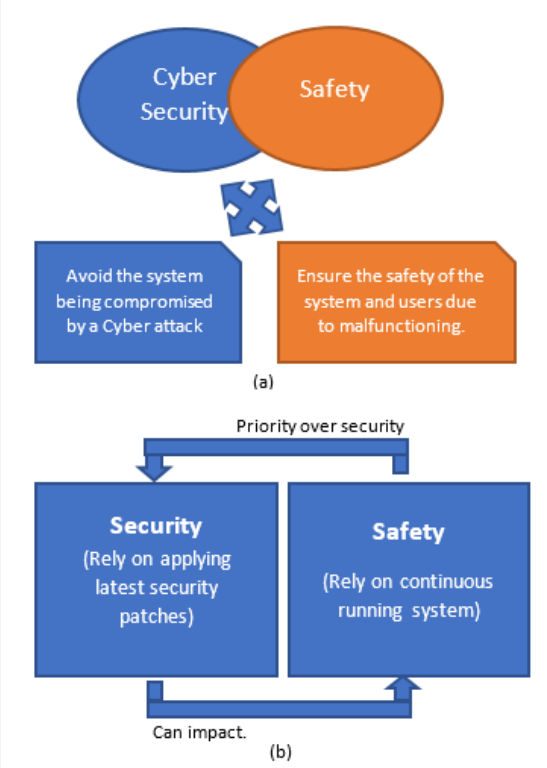

Figure 1: Safe and secure system a) Requirements b) Conflicting requirements.

Looking back at recent incidents, for instance recent death of a hospital patient in Germany, caused by a Ransomware attack [8], we can conclude that future health and safety of our services and products, no doubt depends on how successful we are in managing cyber security risks. Moreover, in case of any Cyber Physical System (CPS), where the system is interacting with the physical world, it is essential to integrate cyber security with health and safety. These emerging requirements necessitate the importance of cyber security in enabling health and safety. These objectives can be achieved by following security by design and security by practice principles for both physical and virtualised systems. In addition, best practice guidelines would help in bridging security, health and safety together in wider engineering practice. Rest of the article discusses challenges, best practice guidelines, potential design principles which could be deployed to overcome the challenges identified.

Recent Attacks on Safety Critical Systems

Below list highlights recent high profile cyber security attacks that affected the safety of the system itself and health and safety of the system users. The attacks targeting health systems could have adverse impact on patients' health and safety. A significant increase of Ransomware attacks targeting healthcare systems and facilities was observed recently. These attacks often manage to disrupt their normal operation, causing discomfort to patients, which could have catastrophic outcome for patient's safety. This is more apparent during COVID-19 pandemic where cyber criminals targeted Coronavirus vaccine research facilities and global vaccine supply 'cold chain'. These efforts could end up compromising the health and safety of the products (in this case vaccine) and services offered by different health sectors.

a) Ransoware attack in a German hospital which indirectly linked to death of a patient [9].

How to cite this article: Chaminda H. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. Eng Technol Open Acc. 2021; 3(5): 555622. DOI: 10.19080/ETOAJ.2021.03.555622.

b) WannaCry Ransomware attack which affected health services across UK [10].

c) Demonstration of Automotive systems (including breaking and steering) hacking [11].

d) HatMan malware targeting industrial Safety Instrumented System (SIS) [12].

e) EKANS ransomware which has the ability to target Industry Control Systems (ICS) [13].

f) The National Cyber Security Centre (NCSC) accused a group called APT29 - also known as "the Dukes" or "Cozy Bear" - for the attacks on coronavirus research facilities [14].

g) The international COVID vaccine supply 'cold chain' has been targeted by cyber-espionage [15].

Challenges for Integrating Cyber Security and Safety

Safety and cyber security practices have been evolved as individual disciplines for many years. Therefore, it is important to understand the fundamental similarities and differences in each of these practices. Some of the main challenges for integrating safety and cyber security practices are listed below.

a. Conflict between risk acceptance criteria in safety and security.

b. Conflicting objectives and understandings of safety and security tradeoffs.

c. Different engineering perspectives (Security and Safety engineers).

d. Quantitative vs qualitative risk assessment.

i. safety: based on well-established safety margin calculations, often quantitative).

ii. Cyber security: Mostly based on the likelihood (qualitative approaches) due to the unpredictable nature of security threats/attacks.

e. Identification of system boundary (e.g., Engineering systems that are connected via digital technologies (e.g., Internet) are boundless and can be reachable from anywhere.

f. Dynamic and static nature of cyber security and safety respectively.

g. Different maintenance goals (Cyber security: 'fix immediately' vs Safety: 'fix after careful consideration').

h. Different risk control philosophy (e.g., enabling Defense in Depth (DiD)).

According to the challenges discussed above, the main challenge for integration is how the risks are identified, evaluated, mitigated and managed. If we can find a common approach for risk management, it would be effortless for practitioners to minimize the impact of risks introduced by cyber security and safety. Organizational practices such as coopetition would also pave the way for better management of cyber security and safety where both functions are handled by different departments of the organization.

A combination of management principles (e.g., accountability), governance (e.g., policies), culture (open/learn culture), Competence (e.g., Code of practice for competence for safety-related systems practitioner or Code of practice for cyber security and safety), supply chain and technical principles are proposed in IET code of practice for cyber security and safety [4]. These principles immensely help organizations to achieve shared goals with respect to cyber security and safety. In addition to these emerging code of practices for cyber security and safety, following best practices and secure design principles for system development are proposed by the author of this article to facilitate this integration. The below sections elaborate on the proposed strategies which can be deployed by organizations to jointly address cyber security and safety.

Best Practice Guidelines for Cyber Security and Safety

It is a widespread practice in businesses to follow best practice guidelines to achieve service and product quality, health and safety excellence. The best practice guidelines in safety and cyber security would immensely help organizations to secure systems while adhering to safe operating parameters. Currently, there are number of international standards targeting specific business functions (often operates within their own silos e.g., ISO 27001:2013 Information security). However, not many codes of practices or standards are available at present to guide organizations through combined cyber security and safety practices to achieve better results. The underpinning Plan, Do, Check and Adjust (PDCA) life cycle of these international standards (e.g., ISO standards), provide an opportunity for businesses to achieve joint objectives while specialized in each particular discipline. For example, most of the organizations thrive to obtain ISO9001:2015 Quality Management Standard [16], ISO27001: Information Security Management Standard [17], ISO45001: Health and Safety Management Standard [18] and SIO14001: Environmental Management System [19] certifications to improve their business productivity and also to comply with industry wide best practice. The requirements of these standards have several common aspects which can be jointly implemented. For example, detailed mapping between some of these ISO standards requirements are presented in [20]. There is an apparent trend in the industry that these best practice standards are increasingly handled by a single unit of the organization (e.g., Quality secretariate) and provide consistent guidelines to the whole organization from a central location. For example, these organizations keep a shared risk register with general risks and function specific risks. These practices help the organizations to integrate risk management in both cyber security and safety even though there are fundamental

How to cite this article: Chaminda H. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. Eng Technol Open Acc. 2021; 3(5): 555622. DOI: 10.19080/ETOAJ.2021.03.555622.

differences as discussed under challenges for integration in this article.

This consistent approach is also facilitated by the best practice standards such as ISO 31000: Risk management [21] and ISO 22301 - Business continuity [22] where organization can approach the risk management and business continuity measures in more holistic way than targeting them under different functions withing the same organization. Furthermore, it can be observed that specific industries are also coming up with their own standards to provide better safety and cyber security for their systems. For example, recent TISAX: Trusted Information Security Assessment eXchange standard provides required cyber security best practice guidelines (securing the supply chain) for Automotive industry [23]. This is very important for Automotive systems since compromised cyber security system could have an adverse impact on its safety. With the emergence of driverless cars, it is crucial for these cars to operate within safety guidelines while talking to nearby cars (e.g., vehicle to vehicle communication) and responding to sensor readings in real-time.

Adhering to best practice guidelines also help organizations to demonstrate the compliance to regulations and laws (e.g., ISO27001 -> GDPR). For instance, EU Network & Information Systems Regulations (NIS Regulations) provides legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services). This was introduced as critical enablers of our societies and economies are increasingly underpinned by the internet and private networks and information systems. Hence it is important to ensure a high common level of network and information security (NIS). According to this directive transport, energy, water, health, and digital infrastructure services are categorized as essential services due to the importance of these services to its citizens. In order to make sure that these services offer assured safety, operators need to integrate good cyber security practices with current health and safety of their product or service offerings.

Cyber Security and Safety by Design (CSSD)

Secure design principles, secure architectures and best practice guidelines will help organizations to design systems that are secure and safe. Addressing safety and cyber security concerns at the design phase is the key to success. Security or safety shouldn't be an afterthought. Hence addressing cyber security and safety of the system from its inception, will provide a better framework to address security and safety concerns and minimize the impact from associated risks. Integrating safety and security at the final phase of the system development will be costly and may not be able to address all the concerns due to fundamental flaws of the design. The NCSC defines five cyber security design principles to manage risks which ranges from threat modelling to addressing availability, scalability, redundancy, recoverability etc. [24]. One of the key secure design principles is making the disruption impossible. For instance, avoid Denial of Service (DoS) attacks where service and application are unable to serve its purpose because of a security incident. For instance, if a hospital is affected by a ransomware attack how the services can be run while investigating the incident. Disaster recovery plans, business continuity plans would help in these situations to maintain the required health and safety offering. According to this guide, addressing supply chain security is also paramount to achieve better security and safety.

Additional care should also be in place if the whole or part of the system uses any virtualization solutions. Most of the current systems either use public or private cloud solutions due to operational and scalability support. These virtualization solutions could introduce additional privacy and security risks into the system. Hence, it is necessary to address all security risks associated with these virtualized instances to operate a secure and safe system.

The integrated cyber security and safety is essential in managing crisis situations like COVID-19 pandemic. It is well documented that COVID-19 unleashed a wave of cyber-attacks which affected both communities who are subjected to lockdown restrictions as well as organizations who deliver essential services [25-28]. In crisis situations like COVID-19, safety critical systems provide the much-needed support for general public. Hence it is important to protect the digital technologies to provide safe services to customers. For instance, a number of important activities such as vaccine research, development and distribution networks came under attack during the pandemic. Hence having jointly optimized cyber security and safety systems would be well placed to deliver the required services within safety margins of Operation Technology (OT).

Conclusion

Increasingly, many safety critical systems are connected via either private or public networks. Cyber-attack on the digital infrastructure could have an adverse impact on the output of the safety critical system. Therefore, it is necessary to jointly address cyber security and safety concerns from the design stage of the system to the operation and maintenance. This will provide the optimum operational parameters for safety critical applications. Even though, there are best practice guidelines to address cyber security and safety on its own, currently there is lack of guidelines on how these can be jointly addressed. Therefore, further research and policy development is necessary to overcome the challenges of combining cyber security and safety practices as discussed in this paper.

References

1. International Electrotechnical Commission (2010) IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.

How to cite this article: Chaminda H. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. Eng Technol Open Acc. 2021; 3(5): 555622. DOI: 10.19080/ETOAJ.2021.03.555622.

2. RTCA DO-356A/EUROCAE ED-202A (2018) Airworthiness Security Methods and Considerations.
3. Riel A, Kreiner C, Macher G, Messnarz R (2017) Integrated design for tackling safety and security challenges of smart products and digital manufacturing. CIRP Annals 66(1): 177-180.
4. IET and NCSC (2020) Code of Practice: Cyber Security and Safety : IET.
5. IET (2014) Code of Practice for Cyber Security in the Built Environment : IET Standards.
6. Homeland Security (2015) 2015 Sector-Specific Plans.
7. Homeland Security (2013) NIIP 2013: Partnering for Critical Infrastructure Security and Resilience.
8. Fox News (2021) Ransomware attack results in death at German hospital.
9. Forbes (2020) Cyberattack on a Hospital Leads to the First Ransomware-Linked Death.
10. BBC (2017) Ransomware cyber-attack: Who has been hardest hit?
11. Miller C (2019) Lessons learned from hacking a car. IEEE Design & Test 36(6): 7-9.
12. CERT.be (2020) TRISIS/HitMan Malware.
13. Fortinet (2020) EKANS Ransomware Targeting OT ICS Systems.
14. Foreign & Commonwealth Office (2020) UK condemns Russian Intelligence Services over vaccine cyber attacks.
15. Financial Times (2020) Covid vaccine supply chain targeted by hackers, say security experts.
16. ISO standards (2015) ISO 9001:2015 Quality Management Standard.
17. ISO standards (2013) ISO/IEC 27001:2013 Information Security Management Standard
18. ISO standards (2018) ISO 45001:2018 Occupational Health and Safety
19. ISO standards (2015) ISO 14001:2015 Environmental Management Standard
20. Integrated-standards.com (2018) Mapping ISO 9001, ISO 14001 and ISO45001.
21. ISO standards (2018) ISO 31000:2018 Risk Management.
22. ISO standards (2019) ISO 22301:2019 Business Continuity Management.
23. ENX Association (2021) TISAX.
24. NCSC (2020) Secure design principles.
25. Hewage C (2020) Coronavirus pandemic has unleashed a wave of cyber-attacks – here's how to protect yourself. The Conversation, 31: 03.
26. Nawaf L, Hewage C, Carroll F (2021) Minimization of Cyber Security Threats Caused by COVID19 Pandemic. 6th International Congress on Information and Communication Technology (6th Proceedings by Springer- ICICT 2021). London UK.
27. Bentotahewa V, Hewage C, Williams J (2021) Security and privacy issues associated with Coronavirus diagnosis and prognosis. EAI International Conference on AI-assisted Solutions for COVID-19 and Biomedical Applications in Smart-Cities. Online Conference.
28. Alkhalil Z, Hewage C, Nawaff L, Khan I (2021) Phishing Attacks: Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science 3(6): 1-40.

DOI: 10.19080/ETOAJ.2021.03.555622

How to cite this article: Chaminda H. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. Eng Technol Open Acc. 2021; 3(5): 555622. DOI: 10.19080/ETOAJ.2021.03.555622.