Operational Security Modeling and Analysis for IACS

Yuan Gao[1], Ines Ben Zid[2], Xinxin Lou[3],Mithil Parekh[4]

Abstract: Security Certifications based on international standards, like ISO 27000 and IEC 62443 series, are strongly favored by industrial manufactures and (critical) facility owners. However, comparing to mature safety certification procedures, there is only a small portion of security certifications available on the market for the booming Industry 4.0 solutions and IoT/IIoT products. The major challenge is how to define a practical working scope, which is compatible with frequent system updates as well as creations of new systems by coupling supplier services. Meanwhile, the potential security impacts should be quantitatively predictable since some of them are tolerable, which are different from most of safety constraints. Thus, in this paper, we proposed an operational security model, which intends to support monitoring and analysis on a dynamically running system. It was extended from the 3-domains security model we proposed in previous work by introducing run-time perspectives and procedures. In addition, cooperating with the security in design concept, the proposed operational procedures were developed following the guidance of the security standard series IEC 62443. For addressing the external threats, Open Source Intelligence (OSINT) were involved to query whether some confidential information, like user-credentials and system vulnerabilities are already collected and publicly known to adversaries. The introduction of OSINT can support more transparent risk assessment approaches. As the conclusion, with the operational security model, we proposed a hybrid approach which consists of security certifications and continuous monitoring/consulting to solve the current challenge.

Keywords: Security Model; Operational Security Model; Security Operation; Continuous Monitoring; OSINT; Functional Safety; IEC 62443; Industry 4.0; IoT; IIoT

1 Introduction

Successful independent testing, which is guided by international/domestic standards, proves confidence to the market in the form of certification. Among numerous kinds of certifications, safety is one of the most important and mature categories due to the first priority of preventing human and environment away from injuries and hazards. Meanwhile, there are also security certifications based on international standards, like ISO 27000 [II11] and IEC 62443 series [IE15], which are strongly favored by industrial manufactures and regulators. However, comparing to the market booming of Industry 4.0 as well as IoT (Internet of Things) and IIOT (Industrial Internet of Things) products, there are little security certifications available on the market. In other words, the valuable

[1] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätplatz 2, 39106 Magdeburg, yuan.gao@ovgu.de
[2] Bielefeld University, ines.ben.zid1@gmail.com
[3] Bielefeld University, xlou@techfak.uni-bielefeld.de
[4] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätplatz 2, 39106 Magdeburg, mithil.parekh@ovgu.de

doi:10.18420/inf2019_ws31

experience of providing safety certifications cannot be directly reused or easily adapted for fulfilling the requirements of security certifications.

The major challenge is how to define the certificating scope, which is compatible with frequent system updates. Figure 1 depicts a variant of the NIST enterprise architecture [FG89] according to the Industry 4.0 requirements described in [Rü15]. For serving different business architectures (BA) and associated information architectures (IA), various applications can be developed on the information system architecture layer for providing services to their upper layers. Accordingly, the industry 4.0 service requirements are dispatched to and fulfilled by (multiple) industry facilities, like factories, their hardware, software and logistic connections etc., plus Internet to forge a virtual factory.

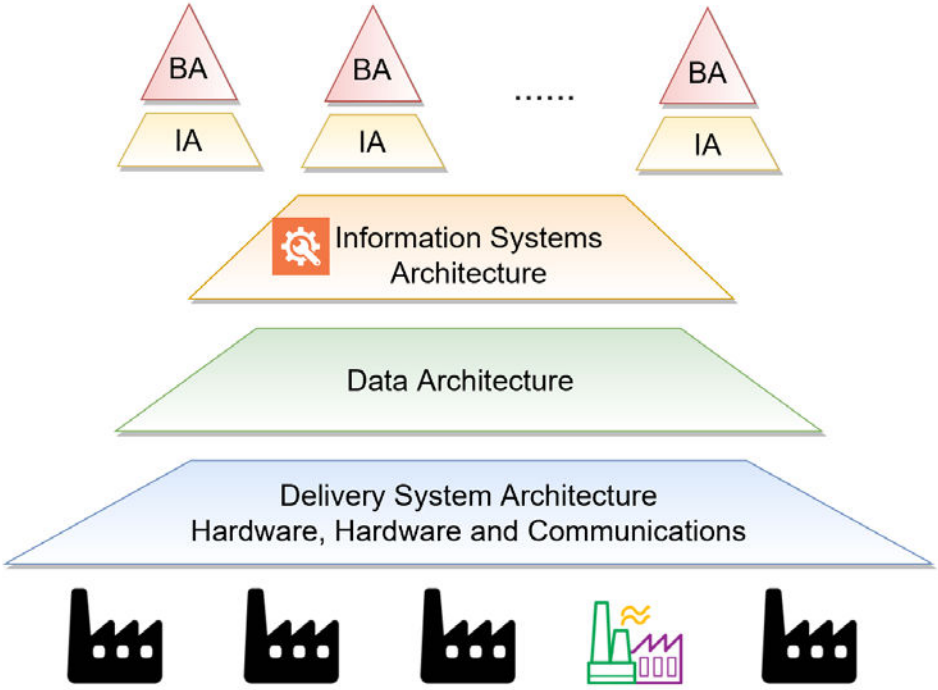

Figure 1: Enterprise Architecture Model in I4.0, adapted from [FG89].

Not like the safety certification towards a stable system, there will be numerous virtual factories are created and decoupled every day. Thus, certificating an unstable system is in principle impossible. In other words, a new security analysis framework is needed, which is not only used only one single time to certificate a system but will be used within the full life-cycle of the system to indicate its security gesture in a regular manner. In this paper, we extended the 3-domains security model [Ga17] to handle the operational security perspectives, like continuous monitoring and system updates described above.

This rest of this paper is organized as followed. In Section 2 we discuss related works that provide foundations and hits for the proposed model. Section 3 focuses on the differences between safety and security. Then we propose the operational security model in Section 4 as well as put into the context of the security standard series IEC62443. Finally, the conclusion is summarized in Section 5 together with discussion regarding future works.

2 Related Work

Fault tree analysis (FTA) is widely used in safety analysis [Er99]. Pietre-Cambacedes et al. also applied this analysis method to security scenarios [PB10]. In his later work [KBP12], FTA was further extended with boolean logic driven markov process (BDMP) for providing a formal expression. However, safety and security were not distinguished within the context of FTA. This paper extended our previous work about the 3-domains security model.

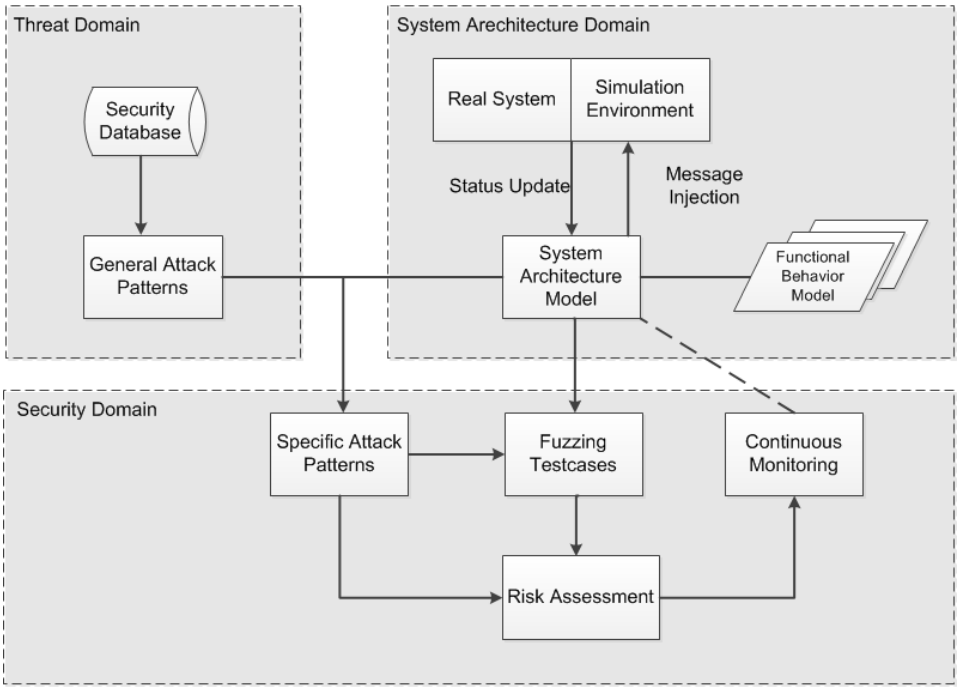

Figure 2: 3-Domains security model.

As shown in Figure 2, the in [Ga17] proposed security model consists of three domains: System Architecture Domain, Threat Domain and Security Domain. Firstly, a system architecture model is created to model security relevant perspectives of the target IACS.

In the threat domain, relevant publicly known vulnerabilities and exploits against the target IACS are collected. Considering the large amount of the known threats, they can be previously categorized and iteratively taken into account according to time/budget constraints. Next step in the security domain, security experts will work on these inputs to assess the cyberattack risks as well as perform security testing. This work can be done in several iterations to address enough details in the system architecture model and increase the coverage of the considered known threats (vulnerabilities and attack patterns). Known vulnerabilities and relevant attack vectors will be under continuous monitoring on a running system. In this paper, the major extension is to allow the system architecture updating and to trigger a rebuild of the security domain afterward. Meanwhile, we will discuss how to enhance the continuous monitoring to realize system architecture changes and to perform security scans based known vulnerabilities and exploits.

Open Source Intelligence (OSINT) can bring more information to the threat domain. There are many open source and commercial tools are ready to use, e.g. SpiderFoot, Nmap and Shodan. On one side, these tools help penetration tester to scan a system with known vulnerabilities and exploits. On the other side, they are utilized by hackers to automate their attacks.

3 Safety vs. Security

Safety Analysis and security analysis share some common concepts while are different from each other. Firstly, they are connected, a violation of security might cause severe impact on safety. Secondly, ideally both of their risks should be minimized. However, they play different roles in industrial environment. Safety is the most important feature of industrial production. It protects human and environment away from injury and hazard. Comparing to this, security covers a wider spectrum to protect the target organization from losses. In other words, safety is a “Must” prerequisite while security includes both “Must” and optional protection goals. They can be vary in different scenarios. For example, in a manufacturing factory, safety has the highest priority while security plays an important role too. However, in the office IT domain, safety takes only a very small portion and security is more focused in this case.

Thus, the certification process requires the safety of system must be provable and fail-save. This means even in an extreme situation, the system itself or associated safety critical system will detect the danger and prevent it automatically. For example, in a critical infrastructure, the internal pressure of a container must be monitored and kept under a safety threshold [Ga17]. No matter the reason, when the pressure inside the container reaches the pre-defined threshold, an alarm will be triggered, and its associated valve will be automatically opened. The safety process is prior to the daily normal operations of the critical infrastructure [IE11]. It is clear that breaking the daily operation will raise the cost while it is still far less than the possible (severe) safety impact. Comparing

to this, the constraints on security are more flexible and complex. There are several reasons regarding this difference:

- **Delayed Impact:** Security impact may happen later than a security breach.
- **Different Scales:** Some of them are tolerable while others are not.
- **Complex Dependencies:** Compromised system can infect others through network.

The first reason is due to that fact the security breaches are normally conducted intentionally. Thus, the consequence might happen quite later after the first security breach, which is different from the safety impact turns to be measurable soon. Considering the Advanced Threat Persistent (APT) [Th10], the real security impact will be triggered even after years or be secretly abandoned. In the latter case, the breach might be even not observable. Secondly, security impacts may vary, and it is possible to mitigate them during run-time. For example, when abnormal access to automation computer is observed, the incidents response team (IRT) can react to this attack by enable white-listing firewall rules. In this situation, shut down the factory or stop operation is not the best choice anymore. Interrupting daily operation is the easiest solution while not the optical one. A run-time attack and defense can happen between attackers and the cybersecurity team of the victim organization. At last, the assumption in security analysis is quite different from the safety world. In safety analysis, damage or hazard are considered independent from each other [PB10], which means redundant systems can increase the system reliability on safety aspects. However, in a security attack, a hijacked system will turn to be the launchpad of the adversaries. In the
following Section 4, these 3 major differences will be addressed by the proposed operational security model.

4 Operational Security Model

For addressing those challenges mentioned above, two extensions of the 3-domains model are proposed in this paper. The first extension is to allow update on the system architecture model. Once the architecture model is updated, security analysis and relevant risk assessment can be rebuilt according to protection rules. Protection rules are a set of rules need to be checked to fulfill the baseline of security requirements. It is clear, for example, a reorganized assembly line can be very complex and will cost hundreds to thousands of man-months to perform a new risk assessment. Here we proposed several methods to ease the re-assessment of the updated system.

The second extension is to allow continuous monitoring to scan the system. However, performing scan might interrupt the normal operation, which is not acceptable in most

scenarios. One solution is to perform only passive scan and collect data for an off-line analysis on a simulation environment (Figure 2). Another solution relies on the real system to notify its changes to the simulation environment. Then all scans are performed

on the simulation environment instead of the production system. The latter solution is more compatible to frequent updated systems, like in different Industry 4.0 scenarios.

4.1 Running Example

In the following Table 1, two simplified industry 4.0 examples are described. In the left column, the first example shows an end user can design a table and issue the production request to the furniture factory A. While in the right column, the second example is regarding the design and production of a kitchen. In this case, two factories: the same furniture factory A and the electricity devices factory B are involved. According to Figure 1, the whole process of these two examples are roughly divided into three layers. They are business architecture and information architecture (BA/IA), information system architecture (ISA), and data architecture as well as delivery system architecture (DA/DSA).

	Production Table	**Production Kitchen**	
BA/IA	Input of user specifications, e.g. dimensions		
ISA	Production Target and Program		
DA/DSA	Furniture Factory A	Furniture Factory A	E-Device Factory B

Table 1: Two examples of Industry 4.0 productions.

	Risk	**Layers(s)**	**Impact**	**Likelihood**
1	Leak of user's data like room dimensions	BA/IA	middle	middle
2	Production dispatch is delayed	ISA and DA/DSA	low	high
3	Safety production issue	All layers	high	low

Table 2: Risk assessment table part of the two examples.

Table 2 lists three risks relevant for these two examples. The first risk is regarding of the data protection of the user data because the design input might include some sensitive information from the user, like the room size and shape. This risk might exist in the BA/IA layer, where the user privacy data is leaked due to e.g. transmission without data encryption. The second risk is about delaying the production. A denial of service (DoS) attack can happen on the ISA layer or on the communication between ISA layer and the DA/DSA layer. As a result, the user's production request cannot be distributed to the

target factory in time. Thus, the production is delayed. Risk with number 3 is the most complex one. The attack can pretend to be a normal user and inject crafted design input into the system. Without knowledge of the malicious data, the ISA layer translate them into control program and dispatch the fake program to the target factory. At the end, the vulnerable production machine, like a robot arm might cause physical damage due to the fake program. This attack goes across all three layers in Table 1.

4.2 Modeling Aspects

If we compare the two examples, table production and kitchen production, there is no

significant difference regarding the risk 1 and risk 2. One prerequisite is that factory A

and factory B passed the same security examination. Meanwhile, the services on all other layers are shared by the two example services. In other words, under these circumstances, if the table production service is considered secure enough, the kitchen production service can be considered secure too. The reason is due to now the security targets are switched from a system, which consists of individual components to a layered service chain. When each component (no matter in which layer) is secured plus connection between layers are secured, operations between two adjacent layers are considered secure. By categorizing industry 4.0 services into different layers and specifying security requirements for each layer, we can ease the security analysis of an industry 4.0 service, which is constructed during the operation time. For adapting the security requirements of industry 4.0, the system architecture model illustrated in Figure 2 was extended with the new layer perspective.

However, risk 3, which goes across all the 3 layers, does not fit in this method. We can assume that, in the table production service, input validation are deployed thus no malicious code can be generated and dispatched to factory A. Even in this case, the adversary has the chance to craft some inputs for finally injecting generated malicious code into a vulnerable system of factory B. Though we can argue one reason is due to factory B contains vulnerable systems, and it cannot be avoided. For mitigating those risks as similar as risk 3, the extension of layer perspective is not enough. A security breach over 3 or even more layers can be addressed by real-time monitoring on different layers. In other words, the crafting malicious input attack cannot be discovered or analyzed before it happens. However, it is possible to detect it and mitigate it during its fly. For example, in the BA/IA layer, the compromising a user might be detected. Or in the information system layer, the generated code can be reported by code reviewing supported by AI technology. It is also possible to notice the existing vulnerable system in the factory by querying security databases regularly. Especially the OSINT discussed in Section 4.5 can help to detect the compromising of user and existing vulnerabilities more efficiently.

To summarize, we extend the 3-domains security model in two points:

- **Layer Perspective:** System architecture model was further enhanced by the layer perspective. Security analysis can be conducted based on combined services from different layers. The analysis focusses on security requirements within a layer as well as communications between layers.
- **Continuous Monitoring:** For addressing complex security breaches, continuous monitoring on daily operations can be deployed to discover abnormal behaviors in different layers.

In addition, monitoring performed on target system can be further enhanced by OSINT technology, which evaluates actual threats from time to time. The evaluated threats contain two parts: The first part involves information known to adversaries, such as domains, emails, hosts and software information i.e. It describes how much information regarding the target is already collected thus can be associated to a certain threat level. The second part contains known vulnerabilities existing in system. Then these weak points must be continuously monitored to prevent exploits from adversaries.

4.3 Mapping to IEC 62443

The proposed operational security model followed the international standard series IEC 62443.

In the proposed layer perspective, security analysis focusses on components within a layer and communication between layers. The concepts here used is same as the zone and conduit concept defined in IEC 62443-3-2 [IE15].

An IACS can be divided into several security zones while assets within the same zone share a common security level. A conduit represents a controlled communication channel between zones. Communication between zones are only allowed through conduits. Similar to this, in our model, we focused on layers (zones) and communication between layers (conduits). One different, in industry 4.0, there is no specific constraints on communication between layers. Thus, the situation can turn to be more complex. In this paper, only controlled communication between adjacent layers are considered. Communication over several layers can be monitored for discovering abnormal behaviors.

In addition, the international security standard IEC 62443-3-3 focuses different security-relevant system requirements (SRs) on the system level [IE13]. The standard describes continuous monitoring as the SR 6.2. Monitoring mechanisms and systems can be deployed in IACS without interrupting its normal operations. Furthermore, security information and event management (SIEM) can support the continuous monitoring by correlating distributed operation logs. SIEM can also support IRT for monitoring and taking quick reaction to on-going security attacks [GX16].

4.4 Safety vs. Security

As discussed in Section 3, we have different assumptions in safety and security analysis. Both analyses can be performed with FTA. However, in safety analysis, segregated systems are considered independent from each other. This means, the probability of all of them fail are the product of individual failure rates. Compared to this, in security analysis, system dependencies must be taken into account. For example, one compromised component will increase the risk of all components within the same network. They might be either directly attacked from the compromised component or affected by suffering a shortage of bandwidth or other resources. It is meaningful to perform security FTA together with the proposed 3-domains model with operational features. On one side, the system architecture model plus different model perspectives provide a clear presentation of system dependencies. On the other side, the operational features can help to determine risks on run-time. Especially it is meaningful for IRT to guess which component the next victim could be and quickly deploy preventive security controls in place.

4.5 Open Source Intelligence (OSINT)

OSINT is a rapid developing technology for both penetration testers and adversaries. Sensitive security information like user, email, geo-location and web domain info i.e. are harvested and stored by hacker communities. OSINT contains public information about a single person, a running IoT product or an industrial facility. Vulnerability databases, like CAPEC [Ba08], CVE [MG02] and TARA [Wy12], stores general vulnerabilities, which are exploitable for a series or a group of devices. Vice versa, OSINT sources stores specific information, like the serial number, software version and listening ports of a running product and possible exploits in some cases. Thus, from the attacker's point of view, it combines the threat domain and system architecture domain to form specific attack patterns as in Figure 2. Similarly, it can also help penetration testers and facility owners to identify vulnerability instances in their system and take essential mitigation. OSINT information focus on component level and can support the continuous monitoring.

Regarding our running example discussed in Section 4.1, OSINT tools can help to discover whether an active user is probably already compromised by adversaries. In this case, the service provider has enough budget, it might even notify the real user security risk (e.g. the user email is already compromised in a hacker database) before real security breach happens. Meanwhile, scanning of system in the delivery system architecture layer regularly can help the owner to discover and patch known vulnerabilities as early as possible.

5 Conclusion and Future Work

In this paper, we discussed the actual challenges regarding the booming of industry 4.0 solutions and IoT/IIoT products. For solving the problems, we extended our 3-domains security model with layer perspective and continuous monitoring. Compared to safety analysis, both new features are needed for handling security analysis in flexible way.

In the future, the layered model of industry 4.0 scenarios will be further refined. A full supply chain including logistics will be modeled and analyzed using the operational model proposed in this paper. It can be expected that for handling the complex industry 4.0 examples, the model will be further improved. In addition, the resource problem in industry 4.0 should be addressed. Until now we assume that there are always enough factories for taking the service requests from users. That is partially true since in general there is overcapacity in industrial production. However, there are still bottlenecks should be examined for avoiding or reducing service interruptions.

References

[Ba08] Barnum, S.: Common attack pattern enumeration and classification (capec) schema description, 2008.

[Er99] Ericson, Clifton A: Fault tree analysis. System Safety Conference, Orlando, Florida 1/, pp. 1–9, 1999.

[FG89] Fong, Elizabeth N; Goldfine, Alan H: Information management directions: the integration challenge. NIST Special publication 500/, p. 167, 1989.

[Ga17] Gao,Yuan; Fischer, Robert; Seibt, Simon; Parekh, Mithil; Li, Jianghai: Integrated Secuirty Framework: Towards a Holistic Approach for Analysis, Simulation and Management of System Security Features. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Chemnitz/, 2017.

[GX16] Gao, Yuan; Xie, Xin: SIEM Framework for Policybased Monitoring of SCADA Systems. Lecture Notes in Informatics (LNI), INFORMATIK 2016, Klagefurt: Workshop New Security Standards for Industrial Automation and Control Systems (IACS/SCADA)/, 2016.

[IE11] IEC: 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, 2011.

[IE13] IEC: 62443 Security for Industrial automation and control systems, Part 3-3: System Security Requirements and Security Levels, 2013.

[IE15] IEC: 62443 Security for Industrial automation and control systems, Part 3-2: Security risk assessment and system design, 2015.

[II11] ISO; IEC: 27005 Information technology, Security techniques, Information security risk management, 2011.

[KBP12] Kriaa, Siwar; Bouissou, Marc; Piètre-Cambacédès, Ludovic: Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments. 2012.

[MG02] Mell, Peter; Grance, Tim: Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme, 2002.

[PB10 Piètre-Cambacédès, Ludovic; Bouissou, Marc: Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). 2010 IEEE International Conference on Systems, Man and Cybernetics/, pp. 2852–2861, 2010.

[Rü15 Rüßmann, Michael; Lorenz, Markus; Gerbert, Philipp;Waldner, Manuela; Justus, Jan; Engel, Pascal; Harnisch, Michael: Industry 4.0: The future of productivity and growth in manufacturing industries. Boston Consulting Group 9/, 2015.

[Th10] Thomas M Chen: Stuxnet, the real start of cyber warfare?[Editor's Note]. IEEE Network 24/6, pp. 2–3, 2010.

[Wy12] Wynn, J.; Whitmore, J.; Upton, G.; Spriggs, L.; McKinnon, D.; McInnes, R.; Graubart R; Clausen, L.: Threat Assessment and Remediation Analysis Methodology Description, https://www.mitre.org/publications/technicalpapers/threat-assessment--remediation-analysis-tara, [Online; accessed 17-May-2019], 2012.