



Research Article

Industrial Challenges of Security Threats upon Security Related IOT Components in RAMI 4.0

Muhammad Amman Zaheer*, Rizwan Bin Faiz, Syed Hasnain Abbas

Abstract

Intensification in security threats has upraised the concern to design secure architecture that mitigates security threats in smart industries. Since there is no empirical evidence in literature which identifies security threats mitigation upon security related IoT components in all three dimensions of Reference Architecture Model for Industry RAMI 4.0 due to why architecture becomes vulnerable to security threats e.g., authentication, authorization etc. Therefore, mitigation of security threats at the architecture level in IoT related security components remains an ongoing challenge for smart industries in general and specific to Cyber Physical System (CPS). This paper secure CPS by mapping security threats upon security component(s) in IoT application(s) in all three dimensions of RAMI 4.0, which is proposed by the German electrical industry based on DIN SPEC 91345. Since the objective of current research is industrial evaluation of security threats in CPS upon security-related IoT components in all three dimensions of RAMI 4.0, we therefore firstly map IoT related security components at all three dimensions of RAMI i.e., architecture layers, process layers and hierarchy levels and then model authorization and authentication threats upon IoT related security components at architecture, process and hierarchy layers.

Keywords

Internet of Things (IoT), International Society of Automation (ISA), Industry 4.0 (I4.0), Cyber Physical System (CPS), Reference Architecture Model Industry 4.0 (RAMI 4.0).

Introduction

Advancements in technologies and application will automatically increase the productivity of industry [1, 2, 3]. Industry does not appreciate the complex characteristics of industry 4.0 due to which they are uncertain of what it presents them [4]. Industry 4.0 promises to revolutionize the industrial processes forever with a deep impact on society. In the last decade, smart manufacturing processes have helped to envisage the notion of smart factories Error! Reference source not found. Industry 4.0 is now generally referred to the conceptual model, and it supports the acceptance of automation, artificial intelligence, robotic technology in Manufacturing, and producing through the connected environment with the usage of CPS 0. The Germany notion of “Industrie 4.0” is recalled as “Industrie du Futur”

in France, “Intelligent Manufacturing” in China, and “Advance industrial automation” by some others 0. It is also considered as a new industrial age [5, 6]. Industry 4.0 is now also considered very useful in this “COVID 19” as it use wireless connectivity [7]. Because of all these advantages companies need to move from traditional technology to industry 4.0 [8]. The concept refers to equipment, suppliers, factories, production lines, products, and customers being linked through Internet technologies. The fundamental purpose of Industry 4.0 is to facilitate cooperation and collaboration between technical objects, which means they have to be virtually represented and connected for bridging of digital and physical environments. It facilitates real-time virtual representation to connect physical devices and machines 0. In essence, it is all about automation and increasing the level of productivity using smart manufacturing methodologies. Industry 4.0 (I4.0) describes the digitization of systems that associate people, products, and smart devices, and moreover, the closely related big data, Artificial Intelligence, new digital value-added services, and business processes 0. It connects and merges production with information and communications technology. I4.0 links customer data with machine data, and machines communicate with machines. It is also referred to as the Integrated Internet, Smart Industry, and advance Manufacturing. The convergence of the IT domain and all the previously mentioned technologies (IOTs, Big Data, Cloud Services, etc) with additional accelerators such as advanced robotics and AI/cognitive has made the realization of this notion possible 0. Cyber-Physical Systems are replacing PLC systems 0, typically communicating over industrial Networks, usually connected to the Internet 0. Thus, emerging of technology set to level the battlefield in terms of security components, data loss prevention, and cloud computing.

The paper discusses the 3D working model of RAMI 4.0 and highlights security issues during IoT components integration and communication. Initially, research showed the principle of reference architecture along with the business process and function, types of security components within Industry 4.0 explained in a case study (Section 2 & 3). Moreover, we implemented an illustrative case study for a better understanding of scenarios. We concluded our 3D model structure with the help of diagrams and descriptions based on recommendations and future vision (Section 3). Finally, we validated our approach from industry experts in the form of interviews and an online survey (Section 4).

Industrial Reference Architecture RAMI 4.0

RAMI 4.0 was proposed for the development of industrial manufacturing system [9]. The main aim of RAMI 4.0 was to develop a common understating of industry 4.0 [10]. RAMI 4.0 establish a connection between assets and information with the combination of IoT components thus, the process helps in the understanding of lifecycle from developing to the production stage, ultimately all layers and process link to hierarchy levels at specified sections based on RAMI 4.0 standards” demonstrating 3D RAMI structure as shown in Figure 1.

Reference architecture comprises of functions list and some denotation of their APIs, user interfaces, and actions. It provides

*Corresponding author: Muhammad Amman Zaheer, Department of Computing, Riphah International University, Islamabad, Pakistan, Tel: +923455228031, E-mail: ammanzaheer@gmail.com

Received: September 16, 2021 Accepted: September 30, 2021 Published: October 07, 2021

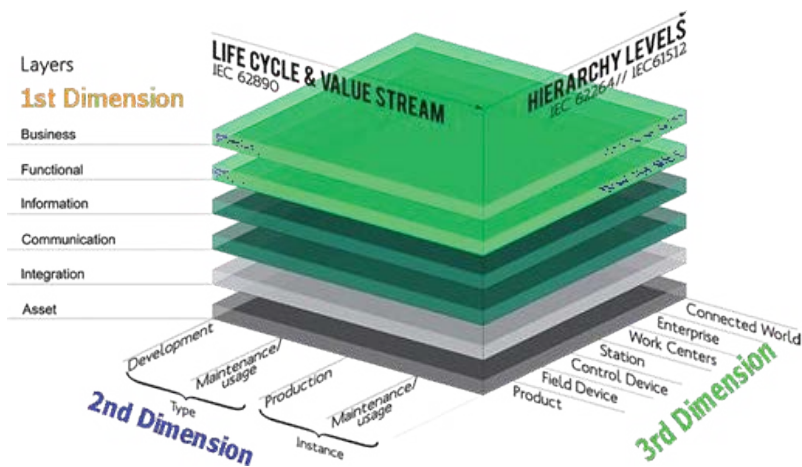


Figure 1: RAMI 4.0 Model Views 0.

IT services catalog for a specific domain. It can be expressed as a different level of abstraction. It defined a complete set of procedures and method to execute the task. It improves system quality; minimizes budget, and timely completion of the project.

Normally, the best practices of reference architecture in a standardized form are to implement its structure. It is a designed pattern that depicts mutual logical interaction and relationships of its components. Reference architecture also plays a vital role in the development of the project life cycle. It facilitates the implementation of software architecture that consists of multi-dimensional categorization; it is also recognized as a framework or model.

Industry architecture RAMI 4.0 comprises of a three-dimensional structure which incorporates the crucial phases of Industry 4.0. Multifaceted relationships, along with wrecking projected phases into minor and manageable parts Error! Reference source not found.

Figure 2 generally illustrates the structure of the RAMI 4.0 model. A model has three axis [11] follow as:

Architecture Layers

Process Life Cycle - Value Stream

Hierarchy Levels.

1st axis layer, also referred to as the architecture layer, is again categorized into six layers in the form of grids, and it also depicts the IT components in an organized manner.

Generally, layers are connected from the bottom to top sequence, as shown below:

Business Layer: Planned business strategy and business goal

Functional Layer: It is responsible for production rules, action, and processing and system controls.

Information Layer: Present live information in the form of data fact and figure 3.

Communication Layer: Mode of transmission and receiving data through communication protocols

Integration Layer: Interaction of physical components with system and machines

Asset Layer: Describe physical components and their behavior.

The 2nd dimension of RAMI 4.0 is a Life Cycle and Value Stream that comprised of the IEC 62890, which means its life cycle from core development progress to the maintenance of product usage 0.

Type: The type of product emerges in several phases during the development process. Following stages are:

- Development
- Maintenance

Instance: It is finalized with the release of a special product version. It consists of:

- Production
- Services.

The third foundation of the RAMI 4.0 model is hierarchy levels are based on IEC 62264, which reflect the diverse functionality launching from the product up to the connected world 0. Stages are as follow:

Product: It defined as a physical entity like a machine, motor, or equipment that has the ability to perform the task.

Field Devices: It is used for detect and identifies components information.

Control Devices: Manage system IO commands

Stations: Basically, these are operators who performed real-time operations.

Work Centers: A central hub for data managing and storing for system production.

Enterprise: Usually defined as ERP applications and business management suites and system software Connected World: End users are real time connected with manufacturing product for their reviews and information. With the mapping of all three axis the RAMI 4.0 model establishes an entire linking of components or section elements 0.

Related Work

It is evident from the current literature that smart industries across the globe are facing security threats due to their vulnerabilities in the

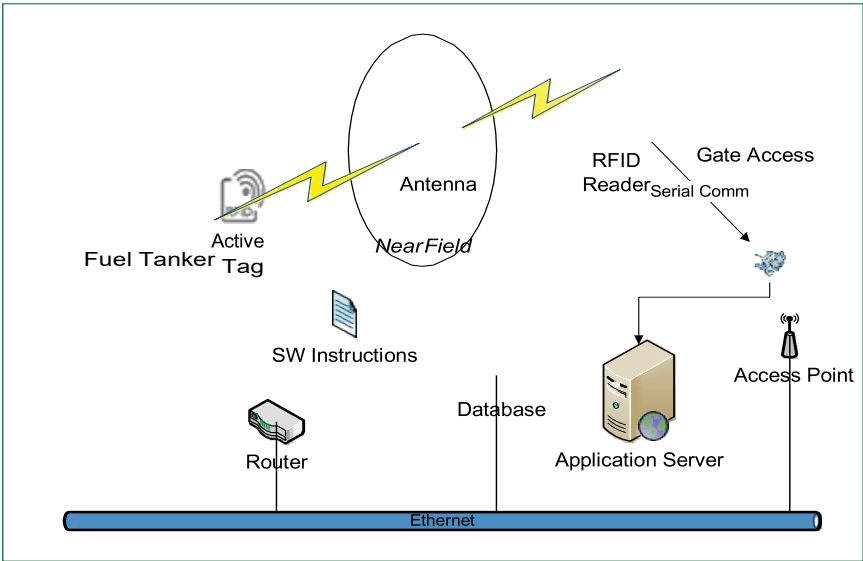


Figure 2: Mapping of Security components upon architecture layers.

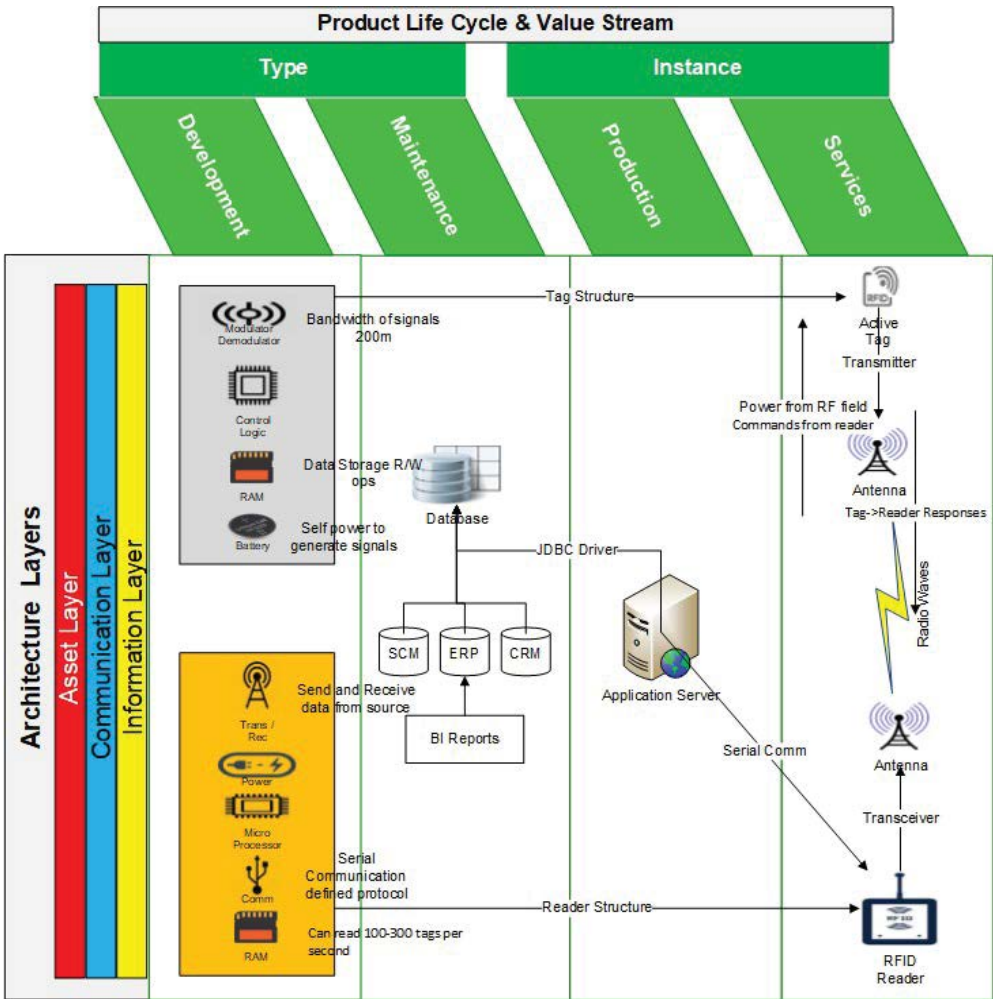


Figure 3: To identify security components at architecture layers & process life cycle (2D View).

industrial reference architecture. Therefore, it is a need for current time to mitigate security threats in general, especially in industry 4.0. Industry 4.0 is modern technology with a massive complexity in its structure. Even though there exist various industrial architectures e.g., Arrowhead, IIRA, IoT-A and RAMI 4.0 to reduce security threats in smart industries. Reference source not found. but since security-related components of CPS are not being mapped upon IoT applications through industrial reference architecture that is “RAMI 4.0” at three dimensions, hence they remain vulnerable to security threats. Therefore, security threat mitigation at the architectural level in IoT related security components remains an ongoing challenge for smart industries in general and RAMI 4.0 in particular. Ref. 0 introduces the security layer as a fourth dimension, above all three dimensions, in RAMI 4.0 to interconnect ICT components which are based upon security viewpoints. They mapped simulated network related components from asset layer upon hierarchical layer. They demonstrated components through Business Process Model Notation under the specific guidelines of industrial standards.












Ref. 0 identifies security-related threats and mitigating them in cloud-based monitoring services through industrial standard i.e., VDI/VDE guidelines. The research study described the mapping components followed by; Profinet, RFID, TCP/IP communication, Cloud Monitoring Services and Machine Learning (ML), and data

monitoring services on all three dimensions of RAMI 4.0. They proposed a process model on how to monitor identified components to confront industrial threats and vulnerabilities with suitable countermeasures.

A security-related framework for industrial IoT applications was introduced to expose security attacks DoS in IoT components that directly affected on production system. They proposed a case study of the smart automobile industry in which they identified the following components; for tracking of products, suppliers, smart devices (smart phones and wearable’s), SW apps, and network equipment Table 1. Their suggested approach reduces the risk of DoS attack at the communication layer in CPS. Their integrated framework facilitated in utilizing max resources-maintained product quality, and controlled CPS system security.

Ref. 0 Merged two layers architecture, and process life cycle. Identify the mapping of components that interlink chain of commands from process to product development. Further they highlighted that security checks need to be improved in RAMI 4.0. Besides, it also identifies the gap between interactions of humans at various levels i.e., managers, engineers, technicians, clerks, and operators interact with Cyber Physical System (CPS). However, current research does not show how IT-related components are mapped upon the process layer of RAMI 4.0.

Table 1: Components Identification and Description

Items	Descriptions	Icons
Boom Barrier	Gate access	
RFID	IoT services security components.	
Prime Mover	Loading material and vehicle	
Active tags	Signal detection	
DB	Database for data storage DB security services	
Router	For data communication	
App Server	System Application access point	
SW App & Manual	SW control and usage Application Security	
Access Point		
Communication	Serial & Ethernet Proxy Authentication and Security Certificate	
RFID Antenna	Information transmission and detection process	

Research Motivation

Although it is evident from the literature reviewed in this section that security threats have been identified and mapped over IoT components in one dimension of RAMI 4.0. However, there is no evidence of authorization and authentication threat identification and their corresponding mitigation upon security-related IoT components in all three dimensions of RAMI 4.0, which makes our architecture vulnerable to security threats e.g., authentication, authorization etc. Therefore, there is a need to mitigate security threats at architecture level in IoT related security components has been an ongoing challenge for smart industries.

Research Goal

A critical review of the above literature reveals that it is a need to model authentication and authorization threats upon security-related IoT components in RAMI 4.0. The above goal can further be divided into below-mentioned objectives:

- RO1: To identify security components in all three dimensions i.e., architecture layers, process life cycle, and hierarchy levels of RAMI 4.0.
- RO2: To map security components in all three dimensions i.e., architecture layers, process layers, and hierarchy levels of RAMI 4.0.
- RO3: An evaluation of authorization and authentication threats mitigation upon IoT related security components in all three dimensions i.e., architecture, process, and hierarchy layers of RAMI 4.0 through industrial case study i.e., CPS.

To achieve the above three objectives, we can progress to improve security in the industrial model. The conceptual model has been presented in the form of a case study. In the below sections, we demonstrated our approach in the form of text and diagrams.

Case Study

Since earlier times, the word logistics is termed mainly for military supply lines till 1898. Logistics management becomes the part of supply chain management which entails planning, controlling and transportation of goods. As of now, it involves the integration of information, transportation, inventory, warehousing, and material packing. Hence, our focus in this research is to manage logistic work process and its function as an integrated environment, as seen in Figure 4. Moreover, logistics activities interconnect with the customer, procurement, manufacturing process, and product assembly.

The evolution of industrial production can be divided into three main periods. These evaluations were an abrupt change and sometimes just served as an improvement in the art of work. To simplify all editions of the industry and its logistics requirements, (1.0, 2.0, 3.0, and 4.0 editions) were designed. It can be seen below how industrial logistics has transformed into today's real logistics with its futuristic development stream.

Advanced logistics embraces intelligent services due to the availability of related smart products. Smart logistics is gained from a technology approach and thereby to change from intelligent services to smart logistics. Having the right product by timely determine at the right place, and its right condition are the general requisites of logistics. But because of the dynamic change in the logistic environment, these requirements seem to be difficult to be fulfilled. Smart logistics is the

shift from traditional supply chains to open the supply network. The technology-driven approach that is used to define smart products and smart services is utilized and extended to defined smart logistics for you, as shown in Figure 5.

Modern technologies have abilities to show 24/7 availability, maintenance efficiency, and affordability for generation of data through network communication. Connected factories are mainly focused on the implementation of high-tech methodologies. Real-time data facilitates monitoring on ongoing activities and at once decision-making process. Cyber Physical Systems (CPS) is the combination of physical as well as computing process [12]. The CPS is based on physical hardware, software, human resources and business services. Automation process facilitates operators and workers to directly interact within system architecture.

This section is scrutinizing the case study that has been performed in the IT department of a public service sector organization. The case study illustrated as captured information of vehicle movement from one place to another. It carried fuel tanks with an active RFID module attached to it [13,14]. The boom barriers authenticate registered vehicles. Further, RFID track information of transport in and out. With this information it assists different type of users like stakeholders can calculate their revenue, security agencies can monitor in real-time location, customers receive their order in a connected environment. An advanced scenario is described, and the environment facilities are used in order to perform a simulation of a real factory with smart devices to the automated system. Initially, identify objects that are being used in the system. The next step is to integrate physical things with digital worlds through communication protocols. It generates real-time information about machines, motors, devices, and other physical objects [15]. It also updates sensor-based information through IoT. During production stage, maintenance needs precautionary processes like system protection, safety, data shield, tragedy alerts, and other advanced security equipment required to install. Real-time monitoring is the basic need for emergency services to take appropriate action in case of big loss or failure[16].

The last step is to revise system behavior and improves its features by the recommendation of threat mitigations and additional precautionary measures in the above process [17-19].

Discussion

Our proposed approach is validated by a focused group of ten industry experts who had 7-18 years of experience from Germany, Austria, USA, China, Poland, Russia, Italy and Estonia. They were currently working in the roles such as: Industrial Automation Technology, Industry 4.0 sales experts in Enterprise Consultants International, Quality Assurance Manager in M&S field at NATO STO CMRE smart industry, Business advisory Digital Platform IoT Solutions.

We critically evaluated our research through semi structured interviews. We then based upon their feedback updated our approach, shown in Figure 6 and 7, which was then validated by each one of them.

Conclusion

Critical review literature reveals that there is no evidence of authorization and authentication threat identification and their corresponding mitigation upon security-related IoT components in all three dimensions of RAMI 4.0, due to which architecture becomes

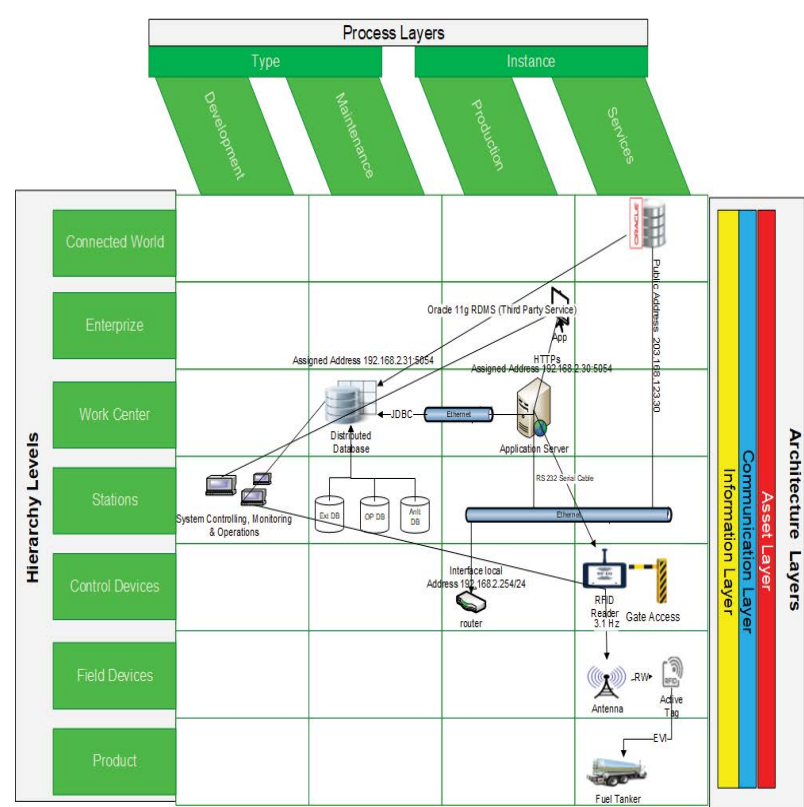


Figure 4: Identify security components at architecture layers, process life cycle & Hierarchy Levels (3D View).

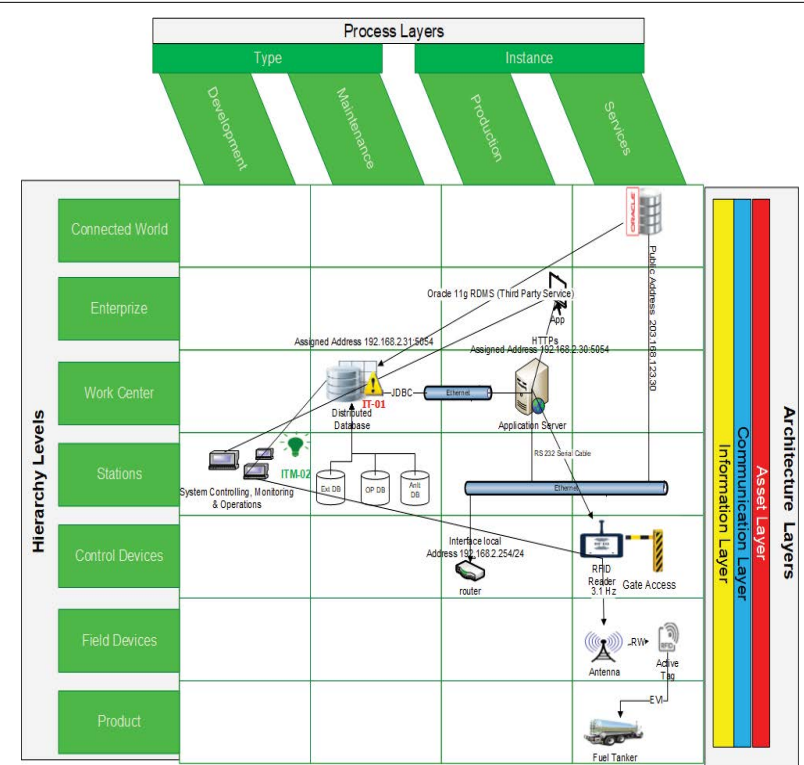


Figure 5: Threats upon IoT related Security Components in architecture, process and hierarchy layers.

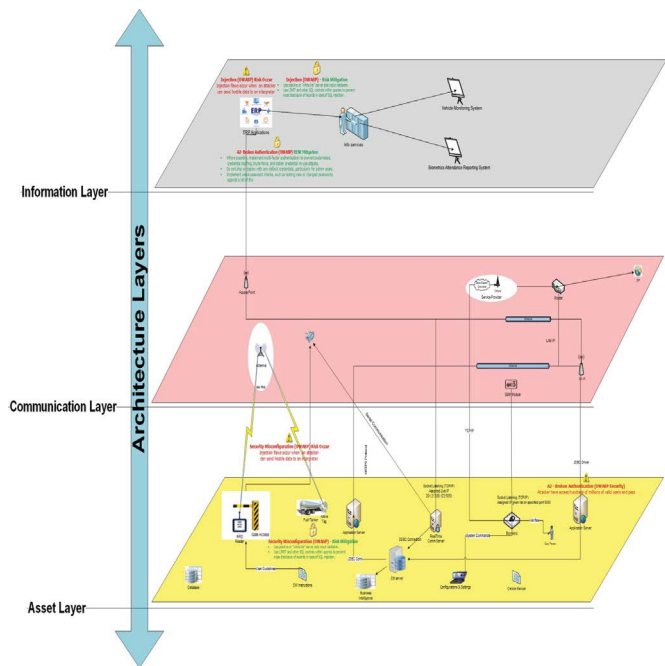


Figure 6: Authorization and authentication threat mapping upon IoT related security components in 3D architecture view.

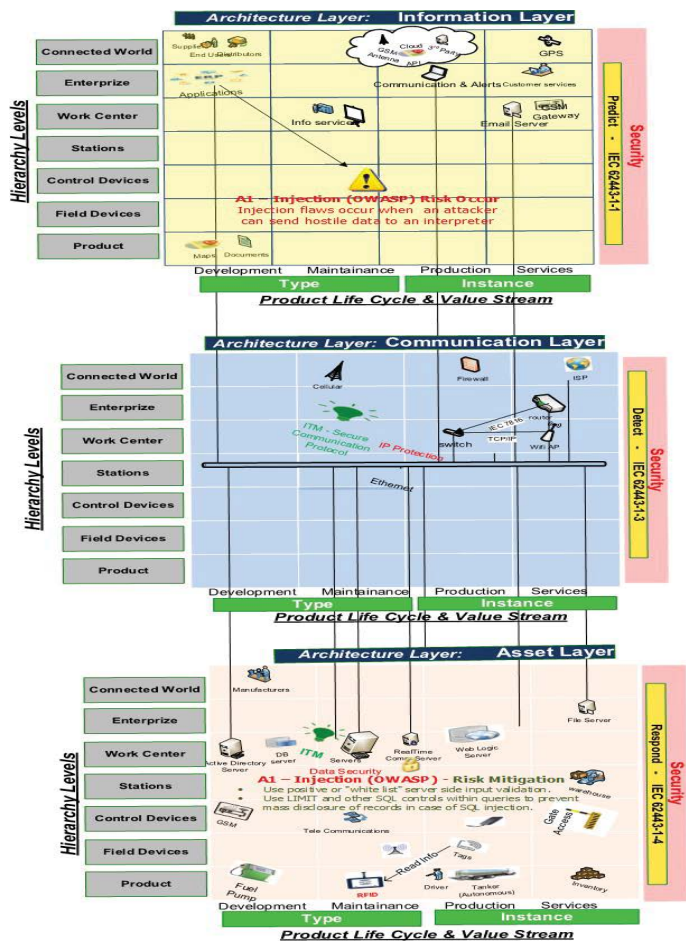


Figure 7: Authorization and authentication threat mapping upon IoT related security components in architecture, process & hierarchy levels.

vulnerable to authentication, authorization threats. Thus, there is a need to mitigate security threats at architecture level in IoT related security components has been an ongoing challenge for smart industries.

Current research mitigates security threats upon security related IoT components in RAMI which is reference architecture for Industry 4.0. The first contribution of this research is that it identifies security components in all three dimensions i.e., architecture layers, process life cycle, and hierarchy levels of RAMI 4.0. Secondly mapping security components in all three dimensions i.e., architecture layers, process layers, and hierarchy levels of RAMI 4.0. It then evaluates authorization and authentication threats mitigation upon IoT related security components in all three dimensions i.e., architecture, process, and hierarchy layers of RAMI 4.0 through industrial case study i.e., CPS.

Our future work is requisite to merge advanced security components by analyzing deeper modes. In fact, there are two aspects that still need to consider. Primarily, underlying the methods for the technical system to upgrade security standard in CPS for identification of security components and mapping structure. On the other hand, a framework tool is required to validate our approach in a productive environment.

References

1. Vaidya S, Ambad P, Bhosle S (2018) Industry 4.0 – A Glimpse *Procedia Manufacturing*. 20: 233-238.
2. Li Da Xu, Eric L, Xu, Ling Li (2018) Industry 4.0: state of the art and future trends. *Int J Res*, 56(8).
3. Bibby L, Dehe B (2018) Defining and assessing industry 4.0 maturity levels – case of the defence sector. *Production Planning & Control The Management of Operations*, 29(12).
4. Dalenogarea LS, Beniteza G B, Ayala NF, Frank AG (2018) The expected contribution of Industry 4.0 technologies for industrial performance. *Int J Production Eco*. 204: 383-394.
5. Javaid M, Haleema A, Vaishyab R, Bahic S, Sumand R, et al, (2020) Industry 4.0 technologies and their applications in fighting COVID-19 pandemic. *Diabetes Metab Syndr*, 14(4): 419-422.
6. Gokalp E, Şener U, Erhan Eren P (2012) Development of an Assessment Model for Industry 4.0: Industry 4.0-MM. *Software Process Improvement and Capability Determination*, 128-142.
7. Sadeghi AR, Wachsmann C, Waidner M (2015) Security and privacy challenges in industrial Internet of Things. in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA.1-6
8. Flatt H, Schriegel S, Jasperneite J, Trsek H, Adamczyk H, et al. (2016) Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany. 1-4.
9. Manogaran G, Thota C, Lopez D, Sundarasekar R (2017) Big Data Security Intelligence for Healthcare Industry 4.0. In *Cybersecurity for Industry 4.0*, 103-126.
10. Ungurean I, Gaitan NC, Gaitan VG (2014) An IoT architecture for things from industrial environment. In 2014 10th International Conference on Communications (COMM), Bucharest, Romania, 1-4.
11. De Melo PFS, Eduardo Paciência G (2019) Controller Interface for Industry 4.0 based on RAMI 4.0 and OPC UA. *Workshop on Metrology for Industry 4.0 and IoT*, IEEE.
12. Kannengiesser U, Müller H (2018) Industry 4.0 Standardisation: Where Does S-BPM Fit?, *ICPS proceedings*, ACM.
13. Kannengiesser U, Müller H (2018) Towards viewpoint-oriented engineering for Industry 4.0: A standards-based approach. *Industrial Cyber-Physical Systems (ICPS)*, ACM.
14. Zaheer MA (2017) RAMI 4.0 (Part 1): Smart Electronic Industry 4.0 Architecture Layers - DZone IoT. *dzone.com*.
15. Kobara K (2016) Cyber Physical Security for Industrial Control Systems and IoT. *Ieice Transactions on Information and Systems*, 99(4): 787-795.
16. Sharpe R, Van Lopik K, Neal A, Goodall P, Conway PP (2019) An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components. *Computers in Industry* 108: 37-44.
17. Xu T, Wendt JB, Potkonjak M (2014) Security of IoT systems: Design challenges and opportunities. In 2014 IEEE/ACM International Conference on Computer-Aided Design 417-423.
18. Stock T, Seliger G (2016) Opportunities of sustainable manufacturing in industry 4.0. *Procedia CIRP* 40: 536-541.
19. Bourke R, Mentis M (2014) An assessment framework for inclusive education. Integrating assessment approaches. *Assesment in Education*, 21(4): 384-397.

Author Affiliation

[Top](#)

Department of Computing, Riphah International University, Islamabad, Pakistan.