Research Article

Identify Components to Manage Security Requirements in RAMI 4.0: An Explanatory Case Study on Industrial Architecture

Muhammad Amman Zaheer^{*}, Malik Nauman, Rizwan Bin Faiz

Department of Computing, Riphah International University, Islamabad, Pakistan

ABSTRACT

The evolution of smart technologies in the manufacturing industry has a strong impact on industrial processes. Though the term "Industry 4.0" has popularized enough to become a buzzword, it brings serious security concerns from the stakeholders. Reference Architecture for Modeling Industry 4.0 and 4.0 (RAMI 4.0) is a widely adopted standard for Industry 4.0 and Smart Factories. This paper proposes an extension of architecture to overcome security challenges. We elaborate industry model "RAMI 4.0" with system description and its security related information among IT components. Our recommended architecture addresses deep understanding of RAMI 4.0 layers with security modeling. Our proposed approach in the form of case study

Keywords: Security; Cyber physical systems; Industry 4.0; Reference architecture; Rami 4.0; Internet of things; Information security

INTRODUCTION

MIndustry 4.0 promises to revolutionize the industrial processes forever with a deep impact on society. In the last decade, the smart manufacturing processes have helped to envisage the notion of smart factories [1]. 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. The concept refers to equipment's, suppliers, factories, production lines, products and customers being linked through Internet technologies. The fundamental purpose of Industry 4.0 components is to cooperate and collaborate between technical objects, which mean they have to be virtually connected for bridging of digital and physical environments. 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 system that associate people, products and smart devices, and moreover the closely related big data, Artificial Intelligence, new digital value added services, and business processes [2]. 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 IT domain and all the 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. Cyber Physical Systems are replacing PLC system, typically communicating over industrial networks usually connected to the Internet [1].

and define its structure for Industry 4.0 specifically related to the logistics industry. The paper discusses the security layers introduced in RAMI 4.0 at two levels

- Layer wise basic view
- Section wise advanced view

These architecture layers are not yet standardized; others are split into several (sub) layers. Our contribution in this paper is to analyze the security components using in layered and section approach, and discuss the possibilities to apply it on highly structured on logistics environment.

METHODOLOGY

Reference architecture

Reference architecture comprises of functions list and some denotation of their API's, user interfaces and actions. It provides IT services catalog for a specific domain. It can be expressed as a different level of abstraction. It defined a complete set of procedure and method to execute the task. It improves system quality; minimize budget and timely completion of the project. Normally, 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 project life cycle. It facilitates in the implementation of software architecture that consist of multidimensional categorization it is also recognized as a framework or model.

In this paper, our focus is to identify the usage of security components

Correspondence to: Muhammad Amman Zaheer, Department of Computing, Riphah International University, Islamabad, Pakistan, E-mail: ammanzaheer@gmail.com

Received: 03-Feb-2022, Manuscript No. AAE-22-48372; Editor assigned: 10-Feb-2022, PreQC No. AAE-22-48372 (PQ), Reviewed: 24-Feb-2022; QC No. AAE-22-48372, Revised: 03-Mar-2022, Manuscript No. AAE-22-48372 (R); Published: 10-Mar-2022, DOI: 10.35248/2167-7670.1000186.

Citation: Zaheer MA, Nauman M, Faiz RB (2022) Identify Components to Manage Security Requirements in RAMI 4.0: An Explanatory Case Study on Industrial Architecture. Adv Automob Eng. 11:186.

Copyright: © 2022 Zaheer MA, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Zaheer MA, et al.

OPEN OACCESS Freely available online

Reference architecture model industry 4.0

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 [2]. Figure 1 generally illustrates the structure of the RAMI 4.0 model. A model has three axes follow as:

- Architecture layers.
- Process life cycle value stream.
- Hierarchy levels.



The third foundation of 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. Stages are as follow:

1-Type

- Development
- Maintenance

2-Instance

- Production
- Services

The second 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 the product usage. 1st axis layer also referred to as architecture layer, which 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:

- 1. Business layer.
- 2. Functional layer.
- 3. Information layer.
- 4. Communication layer.
- 5. Integration layer.
- 6. Asset layer.

With the mapping of all three axes the RAMI 4.0 model establishes an entire linking of components or section elements.

Industrial internet reference architecture

Industrial Internet Consortium (IIC) proposed a standardized open architecture designed for industrial manufacture systems. IIRA is not a standard, but basically it is a technological guideline that acts as an architectural pattern and methodology in order to facilitate Industrial Internet of Things (IIoT) system which derive their own systems based on an ordinary framework and model [1]. Main concerns identified by the IIC are classified into four viewpoints are:

- Business
- Usage
- Functional
- Implementation

Thus, IIC founds security analysis across all checkpoints precisely at initial level, which is difficult to encapsulate it [1]. Interoperability among IIRA and RAMI has been demonstrated in the last technical report. Bridging of elements between the IIRA 3-tier viewpoints as well as with its related IT segments re found coupled with the RAMI 4.0 [1].

IOT-A reference architecture

In the view of required smart things for an IOT-A to connect, there lies a prerequisite encompassing its general guided structure for communication between entities and related services across different platforms[3]. A common observation is to achieve IOT-A objective based on two steps, primarily is to establishing a common understanding of the IoT domain and secondly is to developing a technical system ability on a definite standards and set rules along with proper guidelines which finally derives a solid system of an architectural model [3]. An architecture reference model can be visualized as following perspective:

- Domain model
- Information model
- Functional model
- Communication model

Moreover, IOT-A architecture comprises of following parts: Sensors to get signals in the form of data, gateway to monitor data processing and filtering of same by holding centralize data management, System Applications to control commands, Data analytic for manual data processing to measure business values.

In short, IOT-A platform provides better flexibility and scalability, core architecture comprises of infrastructure, platform, software and storage, monitoring, preprocessing, and security layers between the physical and transport layers. The described four perspectives are the foundation stone of an IOT-A which enables it to interact with all related models.

Comparative study

Framework comparison study gives us the following results as shown in Table 1.

Table 1: Framework comparison (Model comparison) study.

Layers	RAMI 4.0	IIRA	IOT-A
Asset	С	Х	X domain model
Integration	С	Х	Х
Communication	С	С	X Part of function view
Information	С	С	С
Functional	С	С	С
Business	С	С	Х
Life cycle-value stream	С	Х	Х
Hierarchy level	С	Х	Х
Security	?	Х	X Part of function view

Brief perspective about logistics

Since earlier times, the word logistics is termed mainly for a military supply lines till 1898. Logistics management is the become 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 [4]. Hence, our focus in this thesis is to manage logistic work process and its function as an integrated environment as seen in Figure 2. Moreover, logistics activities link with the customer, procurement, manufacturing process, and product assembly.



Smart logistics: Advanced logistics embraces intelligent services due to availability of related smart products. Smart logistic is gained from a technology approach and thereby to change from intelligent services to smart logistic. Having the right product by timely determine at the right place and its right condition are the general requisites of logistics. But because of 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 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 show in Figure 3 [4]. Modern technologies have abilities to show 24/7 availability, maintenance efficiency and affordability for generation of data through network communication [5]. 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.

Era of logistics 4.0: 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 in the Figure 4 and Tables 2-5 [5] how industrial logistics has transformed into today's real logistics with its futuristic development stream.

Concept of logistics 4.0: Advancement of Technology has driven a dramatic increase in industrial productivity since the last dawn of smart industry. The first automated industry has found in the era of the 1970s. During last decades the best practices in industrial technological progress were only incremental, especially inflect with the breakthroughs that transformed IT, Mobile, Communications an e-commerce. Now our generation is in the midst of the fourth wave of technological advancement: the rise of new digital industrial technology known as industry 4.0 transformations that are being proceeding [5]. Over the last few years, the fourth industrial revolution has attracted remarkable attentions throughout the world. Today we are facing a

OPEN OACCESS Freely available online

new paradigm called industry 4.0, which in the first glimpse seemed to be a rebirth of the old CIM idea. A multilink environment that uses to communicate between machines, components, and people now known as smart technology. Artificial Intelligence has not only reduced manpower but it is also found cost effective in autonomous vehicles movement. Nowadays, Manageable goods are being transported around the globe in way i.e advancement in logistics technology [6].

There will be various ways to explain the business process and work flow of RAMI 4.0 layers. The structure of 3D based model has been depicted in tabular form. Therefore, the mapping process of layers and description of components deals with the alteration of system definition into a layered model according to standardized rules set by RAMI 4.0. Therefore, it is concluded that define model is still under development process that bound system to reveal complete information. The RAMI 4.0 model is divided into six vertical layers out of which, we have proposed three for mapping each component. Moreover, an important factor i.e security axis which is a limitation in this structure. We have transformed the security layer into two ways:

- General view of security components
- Detail view of security components

The first level generally categorizes the top issues like business risk generally it highlights the main issues of the system model that should be at its peak level of risk. Fundamental issues of security directly effect on the business model, to prioritizing your risk we have to be categorized into a section or at a level as seen in Table 2 while advance level showed at deep monitoring of security aspects. Actions are divided into classes and classes further transform into subclasses. Detail section and subsections of security flaws are called advance view. Components connect with one or more security aspects depend on the requirement and identified spaces that should be addressed in this description model. During system analyzing we performed security checkpoints that jointly refer to security related observation and information.

System description

By the reference to Logistics industry, the Asset Layer is a part of RAMI 4.0 layer. It portrays the physical entity which transforms digital into the real world. Basically, it is divided into two sections one is component and other one is an administrator shell. Components are tangible items that linked with the integration and administration of shell. Shell has the ability to manage those components in virtual representation form i.e data cables, Prime Mover, machines, documents and software applications as illustrated in Table 2 Layer further map with 2nd axis product life cycle and 3rd axis hierarchical view. The Communication Layer has standardized practices between the integration and information layers. It describes the principle linkages of the network environment. IOT System integration is involved in such a process that communicates in a uniform data format through defined standards. The main purpose of this layer is to transmit and receive data using specified and verified protocols as illustrated in Table 3.

The Information Layer is a vital layer among all as it holds data in a structured way. The fundamental principle of this layer is to give business information about the total no. of booking and delivered orders, they carried all information of the system and its users as seen in Table 4. It carries information about all fueling plants, consuming and materials that are manufactured in the industry. In short, the system has the ability to get connected directly with their customer and keeps their feedback. Information might be in the form of S/W application or databases, facts, and figures.



Figure 4: Entity frame logistics security.

Table 2: Mapping with asset layer.

Asset layer					
Telephone, Fax, Consumers, Suppliers, Service providers	Customer feedback, Connected apps	Promotions	Automated notification	Connected world	
Erp systems, Softwares web administrators, 3 rd party tools	Manage documents, Data storage	Product life cycle	News and updates	Enterprise	
Manufacturing components, Spare parts, Data centers	Product life span	Assemble parts	-	Work center	
System control apps, Switch, Hubs	Tools monitoring, Technical support	Production plan	Improve performance	Stations	
Users, System alse's routers, Biometrics	Test commands	Advance control	-	Control devices	
ATG, RFID readers, Wifi	Repair tool, Temp analysis, Detecting components	-	Sensors	Field devices	
Prime mover, Maps, Documents, Fuel pumps, Tags, Motors, Trackers	Revised design, Add feature	New series	S/W updates	Product	

Table 3: Mapping with communication layer.

Communication layer					
IP,LAN,WAN, Antenna	Connection	Services	Measure performance	Connected world	
HTTP/FTP data request/Response, GSM Mode, 3G	Maintenance cycle	Data view	Service usage	Enterprise	
Gateway	Security checks	Remote view	Bandwidth improve	Work center	
SDLC Communication	-		-	Stations	
Transmitter/Receiver	Cell/Battery	BLE,HTTP,TCP/IP	Instruction manual	Control devices	
Sensor Values	Maintenance, New sensor	-	-	Field devices	
	-		-	Product	

Table 4: Mapping with information layer.

Information layer					
Tot sales, Online orders, Lire Tacking Facility, Supplier data, Location	Re assessment	New technology	Instruction manual	Connected world	
Dashboard, Enterprise Applications, Purchase/Order Info, Freight, Services System	Bill of material	-	Customer feedback	Enterprise	
Events, Notification, Reports, Status	Working plan	Notification types	Updates	Work center	
Simulation, Components Info, Data and Files	Production concept		Instruction	Stations	
System info, Puts detail		-	Life cycle	Control devices	
Temperature, Readings, Scanning		-	-	Field devices	
Logistics Vehicles, Fuel, Pumps	Packaging, loading, unloading	Serial number	Life cycle	Product	

As a described framework, RAMI 4.0 is lacking security issues in the Logistics industry. Security is a vital element for business stability. This layer is responsible for the monitoring system, securing data,

authentication users and prevents intruders as highlighted in Table 5 leverage over failure and improves quality.

Table 5: Additional axis security checkpoints mapping with Asset Layer.

Predict	Prevent	Detect		Respond
	Asset layer merge security			
Telephone, Fax, Law enforcement, Consumers, Suppliers, Service providers, Emergency services	Customer feedback, Connected apps	Promotions	Automated notification	Connected world
ERP systems, Softwares Web Administrators, 3 rd party secure tools, Firewalls	Manage documents, Data storage	Product life cycle	News and updates	Enterprise
Manufacturing components, Spare parts, Data center, NVR	Product life span, System alert	Assemble parts		Work center
System Control Apps, Switch, Hubs, DVR	Tools monitoring, Technical Suppost	Production Plan	Improve Performance	Stations
Users, System Algo's. Routers, Biometrics	Test commands	Advance control	-	Control devices
ATG, RFID readers, WHEEL Fiber Opties, CCTV Sensors	Repair tool, Temp analysis, Detecting components	-	Sensors	Field devices
Prime mover, maps, Fibre Optics, documents, fuel pumps, Tags, Motors, Security Certificates, Trackers, Antivirus, Surveillance,	Revised design, Add feature	New senies	S/W Updates	Product

RESULTS AND DISCUSSION

This study is an in depth study that has been performed in the IT Department of a public sector organization. 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, identified objects that are being used in the system. Secondly, physical things which are being integrating with digital worlds through communication protocols [7]. Next step, generate real time information about machines, motors, devices, and other physical objects, It also updates sensor based information through IOT. The last step is to revise system behavior and improves its features, the additional security layer is required as. With this layer, the system is monitoring and controlling environment by sending alerts, system recovery during cyber-attacks, securing products and items, and other alternates. Such realtime monitoring information connected to law enforcement agencies for instance if, any vehicle lifted or misplaced then real time tracking screen also available for the police force presented security workflow [8].

Intelligent integrated RFID system implemented to control intranet and extranet logistics process such as tracking objects and inventory management. Moreover, the system is highly secured in generating real time information and communication.

System architecture level 1

As per indication of logistics industry Asset Layer identifies physical components. Enlisted Components in asset layer has prominent role in its working model. Assets are anything relevant to physical thing, entity, item or any rigid object. We can classify items of asset layer into the following mechanism see such as devices, machines, documents, software applications, spare parts, system users, customers, suppliers, distributors, service providers or any other physical objects [9]. With respect to logistics industry our main objective is to control and manage the flow of system. A key of this case study is to follow real time data information pertaining to security alerts. Each item or component has been identified as per system working model.

System architecture level 2

Primarily, joint layer is used to connect the physical things into digital (real world). It is the real Communication Layer which provides standardized communication between assets integration with the information layer. According to scenario, the role of communication is to transmit and receive data using the standardized protocol as shown in. It may be defined as per ISO and IEC for the industrial system. ISA committee has identified not only roles in any industry but they have a proper definition of how object connect and share information under the given standards [10]. Different communication protocols are TCP/IP, HTTP/FTP protocols, transmission through LAN or WAN, GSM Antenna, RFID protocols, and communicates through BLE (Bluetooth Low Energy) or Wi-Fi devices.

System architecture level 3

Next layer of RAMI 4.0 is Information Layer carries data info in an ordered way. Basic responsibility is to cater information about connected things. For instance, a total number of sales purchase orders info, suppliers and locations info. It is based on real time tracking info. It holds information on all coupled motor, machines, products, materials and all other things that are used in this environment. Each component transmits information through standardized communication protocol that is manufactured in an industry [9]. It

OPEN ORCESS Freely available online

also helps in providing system, machines and motors status for their life period that are used to assemble products. Real time information from customers assists to keeps their feedback and continuous improvement. Information is not only software based, i.e., but it might also be in the form of application or data facts, figures, and files.

System architecture level 4

Another challenge in RAMI 4.0 is to need an additional layer or security checks to improved system flaw, to protect the system from vulnerabilities, for emergency cases gets immediate security alerts or other various factors. In this case study, product lifecycle maintenance needs to cover additional precautionary processes, belongs to 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 [10]. There is the demand of alternate scenario if given mechanism failed to do. Thus, the security layer covers the above implementation.

In a general survey, we come to know that security risks and threats that the information assets are facing challenges more serious. Main issues of IS are to understand the existent vulnerabilities and threats during data generating process using assets. Moreover, we evaluate the results by conducting a different interview of industry experts regarding security challenges that industries are facing nowadays. We extended our research by comparison of Logistics companies and get their experts to view, they claimed that average is 30 percent of their total budget in 2010 on information security, up from 20 percent in 2006, and many of them will continue to increase information security spending.

CONCLUSION

In this paper, we have presented system description and its real time problem of reaching that should control based security standard risks to an acceptable level. We have performed a mapping study in the field of logistics by adding of security requirements; it improves the RAMI 4.0 model. In addition, security factors need to improve in the above model there is additional axis required that cover all security aspects in this framework. We categorized security checks into base view for general perspective at a basic level, then advance view for detail analyzing of security factors. Further, work is requisite to merge advance security components by analyzing deeper modes. In fact, there are two aspects still need to consider. Primarily, underlying the methods for the technical system to upgrade security standard in CPPS 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

- SMa Z, Hudic A, Shaaban A, Plosz S. Security viewpoint in a reference architecture model for cyber-physical production systems. In2017 IEEE European symposium on security and privacy workshops (EuroS and PW). 2017;pp. 153-159.
- Flatt H, Schriegel S, Jasperneite J, Trsek H, Adamczyk H. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). 2016;pp. 1-4.
- De Loof J, Sap CM, Meissner S, Nettsträter A, Cea AO, Sap MT, et al. Internet of Things-Architecture IoT-A Deliverable D1. 5-Final architectural reference model for the IoT v3. 0. IoT-A. 2013:1499.

Zaheer MA, et al.

OPEN OACCESS Freely available online

- 4. Pisching MA, Junqueira F, Miyagi PE. Service composition in the cloud-based manufacturing focused on the industry 4.0. In Doctoral Conference on Computing, Electrical and Industrial Systems. 2015;450:pp. 65-72.
- Grangel-González I, Halilaj L, Coskun G, Auer S, Collarana D, Hoffmeister M. Towards a semantic administrative shell for industry 4.0 components. In2016 IEEE Tenth International Conference on Semantic Computing (ICSC). 2016;pp. 230-237.
- Sadeghi AR, Wachsmann C, Waidner M. Security and privacy challenges in industrial internet of things. In2015 52nd ACM/ EDAC/IEEE Design Automation Conference (DAC). 2015;pp. 1-6.
- Varga P, Plosz S, Soos G, Hegedus C. Security threats and issues in automation IoT. In2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). 2017;pp. 1-6.
- 8. Ungurean I, Gaitan NC, Gaitan VG. An IoT architecture for things from industrial environment. In2014 10th International Conference on Communications (COMM). 2014;pp. 1-4.
- 9. Domingo Galindo L. The challenges of logistics 4.0 for the supply chain management and the information technology. Master's thesis, NTNU.
- 10. Zaheer MA. Rami 4.0 (Part 3): Smart Electronic Industry 4.0 Hierarchy Level. Dzone/IoT Zone. 2017.