POLITECNICO
DI TORINO

A Master's Thesis on

Safety 4.0 Technologies

Asif Ali

A Thesis submitted for the fulfillment for the

Master of Science Programme In

Automotive Engineering at Politecnico di Torino, Italy

Author

Asif Ali

Matricola: S229978

Ms. Automotive Engineering

DIMEAS (Department of Mechanical and Aerospace Engineering)

Supervisor

Micaela Demichela

DISAT (Department of Applied Science & Technology)

Abstract

The technological evolution brings the Industrial shifts. The new technologies such as cyber physical system, Internet of things, human machine collaboration, additive manufacturing and artificial intelligence bring the fourth industrial revolution called industry 4.0. With this new Industrial transformation some of these new technologies will be adopted in the manufacturing environment and consequently new methods of safety will be required.

Some of the technologies was already in use before the industry 4.0, therefore we follow an approach that it will be more useful to renovate the existing safety procedure and methods. Thus all the actions required to renovate safety is explained in detail. Industrial Safety is wide topic and it’s difficult to explain as a whole. Therefore, we will explain the safety of technologies that will make industry 4.0.

Industry 4.0 manufacturing systems are highly interconnected structures that include a large number of people, IT devices, automation components and machines. There is exchange of documents and information among the devices of the technological system. In order to provide interactions between these highly interconnected, open and heterogeneous components, a high degree of confidentiality, integrity and availability is required. In addition to safety, industry 4.0 required a whole range of fresh security aspects which is explained quite comprehensively in this thesis.

Table of Contents

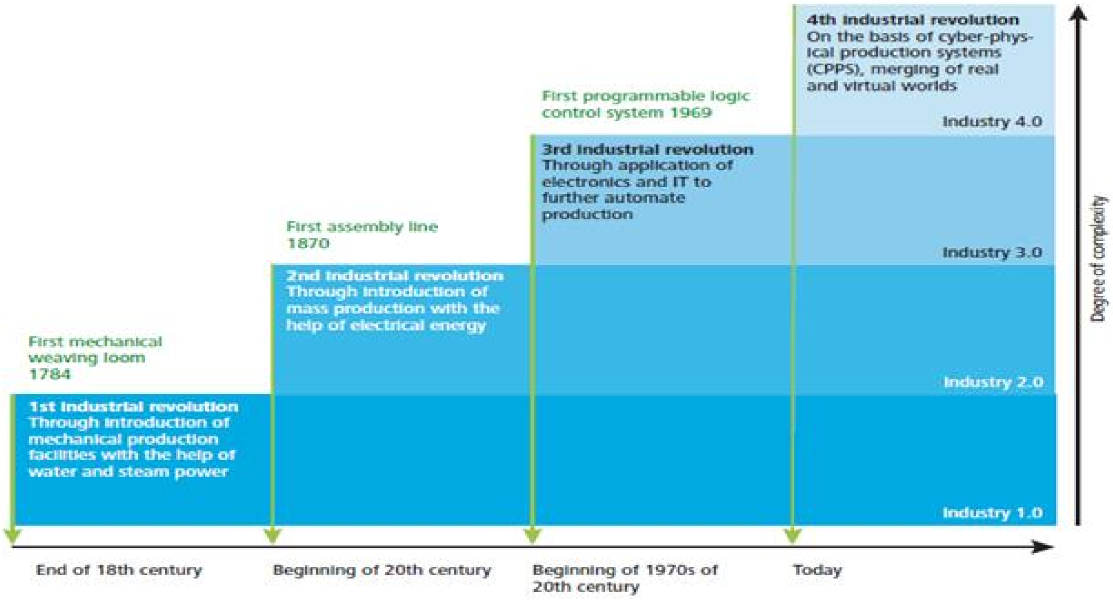
Chapter 1 Industry 4.0

1.1 Introduction

Industry 4.0 is the method of more advancement in the design and control of the entire value added process, used in manufacturing industry for production through automation (robotics) and data exchange.

In the 18th Century Industrialization starts and then it went through an extraordinary transformation with the invention of steam generation machines (Industrial Revolution 1.0), this method of production was inextricably linked to the constraints of human effort. In the 19th century the next shift took place with the launch of electricity, which permit a wide transportation of electricity. The machines were made smaller and started to work more rapidly (Industry 2.0). In the 20th century, with the evolution of electronics the assembly lines were made automated and more results oriented (Industry 3.0). Automation has created ways to optimize production and manufacturing by developing more flexible, ergonomic and safe machines.

"In comparison, the term "Industry 4.0" refers to the so-called 4th industrial revolution, concentrated on Cyber-Physical systems and on the new technologies of Internet of Things (IoT), Cloud Computing, Big Data Analytics and Artificial Intelligence (AI)" [1].


4th industrial revolution
On the basis of cyber-physical production systems (CPPS), merging of real and virtual worlds
Industry 4.0
First programmable logic control system 1969
3rd industrial revolution
Through application of electronics and IT to further automate production
Industry 3.0
First assembly line 1870
2nd industrial revolution
Through introduction of mass production with the help of electrical energy
Industry 2.0
First mechanical weaving loom 1784
1st industrial revolution
Through introduction of mechanical production facilities with the help of water and steam power
Industry 1.0
Degree of complexity
End of 18th century
Beginning of 20th century
Beginning of 1970s of 20th century
Today

Source: Challenges and solutions for the digital transformation and use of exponential technologies. www.mckinsey.com

1.2 Goal of Industry 4.0:

The goal is to implement these technologies in all the areas (not just the manufacturing one) of the industrial sector, to allow an enhancement of business performance and quality of life of workers. The implementation of these new techniques will made a company not only flexible and well efficient but also “Intelligent” through which company improve productivity. These new technologies will reduce the human efforts and the dangers to which the workers are exposed in performing tasks.

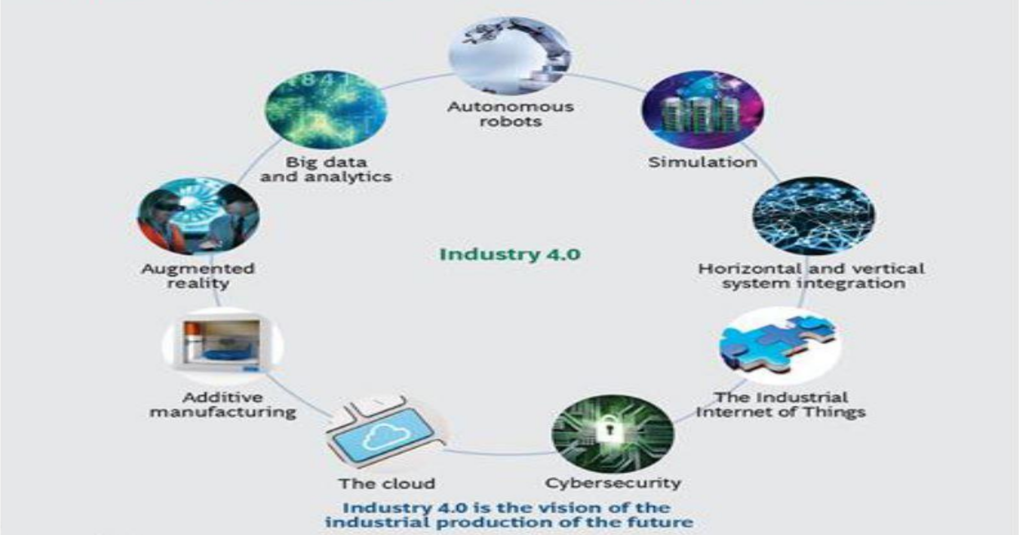
1.3 The Building Block of INDUSTRY 4.0:

Technologies that lay the foundations for Industry 4.0, some of them are already used in production. However, with Industry 4.0, they will transform production, improve the flow of production, increase efficiency and revise the conventional production methods between suppliers, manufacturers and customers, and between man and machine. The success of Industry 4.0 is that all the technologies shown in **Figure 2** can be combined to reach their full potential. If these applications implemented correctly, they can provide a general improvement for any type of business.

1.3.1 Cyber Physical Systems (CPS):

Cyber-physical systems or "intelligent" systems are complex interactive networks of physical and computational elements. Mobile and portable devices (Including robots), movable installations, integrated structure and connected devices (Internet of things) are the main components of these system. The infrastructure network like (Internet) is used for Information transmission, processing and exchange in real time. The system depends on their own intelligence and produce autonomous decisions without any direct contact. Cyber-physical systems are constructed by integrating integrated systems through wired or wireless communication networks. These systems are the foundation of our vital infrastructure, the foundation of new and future intelligent services, and will provide a better life quality in many sectors.

EXHIBIT 1 | Nine Technologies Are Transforming Industrial Production


Autonomous robots
Big data and analytics
Simulation
Augmented reality
Industry 4.0
Horizontal and vertical system integration
Additive manufacturing
The Industrial Internet of Things
The cloud
Cybersecurity
Industry 4.0 is the vision of the industrial production of the future

Source: BCG.

1.3.2 Internet of things (IOT):

The chain of physical objects implanted with electronics, sensors, actuators and connectivity are called Internet of Things (IoT). These objects connect and exchange information via a universal digital network. Each element is singular and traceable by its integrated computer system; however, they can work together within the existing internet infrastructure. Smart RFID localization technology can now identify and control itself to some extent. For each and every product, these tags have all the necessary information about the next manufacturing process. The human involvement in no longer required in material handling or production system about the next work steps, because the product identify themselves.

1.3.3 Big Data and Analytics:

In order to improve production quality, save energy, and improve device function, analytics depends on larger amount of data were newly introduced in the manufacturing world. The information comes from different sources such as production equipment and business management systems in Industry 4.0 environments turns into standard to support real time decisions. For example, Infineon Technologies makers of semiconductor chips, reduced the downtime of the product by correlating the data of a chip collected during the test phase at the last stage of the developing process with the data captured during earlier phase in the process. This method will help the Infineon to eliminate the defective pieces during the start of production and improve their manufacturing quality.

1.3.4 Autonomous Robots:

Robots are using in abundant since long time in lot of industries in order to handle complex tasks. But robots continue to evolve, they are more independent, flexible and helpful to become more useful. They will cooperate with one another and will work with people safely and learn from them. The future robots will be cheaper and stronger than those presently used in manufacturing. For example, European robot company Kuka of automated equipment, made independent robots that interact with each other and adapt automatically to their next move towards an unfinished job. People and robots are working very closely and safely due to good quality modules and sensors. Also, the supplier of industrial robots ABB launches a two-arm YuMi robot specially designed for the assembly of human-related products (e.g consumer electronics). The secure interaction and identification of parts will be made possible through padded arms and computer view.

1.3.5 Additive Manufacturing:

In order to create prototype and make single parts the companies start to introduce additive manufacturing such as 3D printing. These methods in Industry 4.0 will be mainly used for the production of small quantities of custom products that offer design benefits, such as complex lightweight structures. The stocks levels and the material handling transport routes during product manufacturing will reduce from the use of the additive manufacturing. For example, the airline industry for new designs that reduce the weight of the aircraft and reduce its spending on commodities like titanium implemented additive manufacturing.

1.3.6 Augmented Reality:

Augmented reality systems will guide many diverse tasks inside the manufacturing plants, for example damaged parts inside the warehouse will be identified and the information related to their repair are send through mobile devices. Such systems are still in his early phases, but the companies will use augmented reality more in future to help their employees to made better decision and improve workflow efficiency by providing them useful real time information. For example, repair information will be provided to an employee about a specific part who can see it in his augmented reality glasses. In addition, Siemens utilize virtual training. They developed training module for their operators that uses 3D environment depends on data from glasses to prepare their emergency team. The operator of the machines in this virtual world will learn the communication with machine by clicking on cybernetic representation. The parameter of the machine use can be changed and operating data, maintenance guidance can be recovered.

1.3.7 Simulation:

Simulations are already used in engineering, during product development phase, but in Industry 4.0 the simulations will be increasingly used for different operations of plant. These simulations used the actual information of the development of product, their manufacturing process and the machines information on which the product is developed and map this physical model to virtual model. All this information helps to test the machine configuration for next product in virtual world before applying any change in physical process. This will reduce the configuration time of machine and will increase the quality of product. For example, Siemens and German manufacturer design a machine that has the ability to simulate virtually the parts its produced from physical data. This reduce preparation time for the actual machining process by up to 80 percent.

1.3.8 The Cloud:

The cloud based software is already implemented by many companies and they use it for business and problem solving applications. However, those companies which will apply Industry 4.0 in their production sites will transfer a lot of data and information, which is out of the reach of their business boundaries. On the other hand, significant improvement is already seen in the cloud technologies and their response time lead to few milliseconds. Due to which information and machine functionalities are growingly available in cloud, helping data-based services for production systems. The systems which are used for supervision and controlling are also cloud based. The major companies which mostly offers cloud-based solutions are producers of manufacturing execution systems.

1.3.9 Horizontal and Vertical System Integration

The computer systems which are used in current industry is not merged with one another. In most cases companies are not completely linked with their suppliers and customers. Even the different departments like engineering, production and service of the same company are not joined. The different tasks at the workshop level are not completely unified. Even the engineering is not fully integrated from the product development to automation. However, with Industry 4.0, organizations, divisions, capabilities and capacities are becoming more interconnected as widespread data merging networks between industries will grow and it will help to established the automated value chain in true sense.

1.4 Safety is important aspect of Manufacturing facility:

Safety is always an important aspect that should be taken into account in the planning of production plants and their products. These are set of regulations and rules that governing the creation and working of such systems. When information technology and computers meet with mechanics and electronics in the late 1960s (Industry 3.0), there is a dramatic increase in the requirements of safety and security in the manufacturing environment. The new devices and components came to workplace due to which it is very difficult to provide operational safety, but after some time safety experts also realized that due to use of computer and electronics security is also an alarming issue. Most to the risks which occurred in industry 3.0 are still waiting for their answers.

1.5 Safety evolvement with Industrial Transformation:

Whenever an industrial transformation occurs, we will observe the evolution of the manufacturing philosophy and new methods should be developed to solve occupational safety issues. Due to Industrialization the demands for labour is increased which resulting improper work environment. The workforce was not properly trained and the owners always try to ignore; and did not spend properly to provide a useful and healthy work environment. Health and safety at work took a heavy toll, and legislators had to intervene under public pressure. In first world countries the safety regulations and standards slowly developed due to labour unions and strict labour laws. Now we can say that workplace environment is significantly improved although still some alarming statistics remains. While criticism continues, we can point to better engagement of employers and employees in solving health and safety issues in the workplace. Nowadays the use of advanced tools, better standards for risk management, and safer devices helps to controls and monitors the work environment better.

1.6 Safety reassessment is prerequisite for Industry 4.0 environments

As Industry 4.0 becomes more and more reality, it seems predictable that a new set of standard changes will occur. A series of additional safety and security requirements will arise. The companies are facing fresh safety and security challenges due to Industry 4.0 because of continuous development in automation process. Computers, internet, IT, electronic, robotics are merging together. The work procedures are altered because of the application of advanced IT appliances in the work place leads to important shifts. Safety and security required a review for the Industry 4.0 applications because these systems reshape and upgrade autonomously.

When we switch to Industry 4.0, we will have to ask:

1) whether we have paid the necessary attention to the new safety requirements or not?
2) Have we calculated the (good and bad) safety results of this new Industrial reformation?
3) Will Safety considerations have any controlling effect on all this bubbliness?

1.7 Outline of thesis:

We established some question which means that our purpose in this thesis is to start a discussion with regard to Safety in Industry 4.0. In the next section we shall begin with definition of safety and security and the priority actions required for the manufacturing industries to travel towards safety 4.0. In the third chapter, we will comprehensively discuss the safety of the technologies that lay the foundation of Industry 4.0. In fourth chapter we list some of the available devices which is already used in industrial environment for the purpose of safety. In the fifth chapter we will discuss the implementation of security in industrial environment. In the last chapter we will present a conclusion which is derived from our work.

Chapter 2 Safety and Security

2.1 Definitions

The visible and critical features are safety and security for the production facility and the products they manufacture. Several safety and security are relevant for Industry 4.0, so a clear distinction between the two terms is indispensable:

2.1.1 Safety:

Safety refers to the fact that technological systems (machinery, production facilities, products, etc.) should not endanger humans or the environment. Safety may also include additional aspects, e.g. How to avoid mechanical or electrical risks, radiation protection, risk prevention due to steam or high pressure, etc.

2.1.2 Security:

Security refers to the fact that production facilities and products, and in particular the data contained therein and the technical knowledge contained therein, must be protected against misuse and unauthorized access. In digital systems the preservation of information and services against misuse, for example. Unauthorized access, modification or destruction.

2.2 Actions required to Renovate Safety to Safety 4.0:

Safety and security is essential requirement for the operation of Industry 4.0 organizations. As the Industry 4.0 systems will rearrange themselves independently, this needs a safety and security checks during runtime. When the manufacturing plants want to transform to industry 4.0, they will have to transform their safety and security as well, by looking to the following key aspects.

2.2.1 From static to dynamic Safety:

In order to guarantee safety, it is needed that continuing risks arise from a device or machine do not surpass an agreeable or satisfactory levels. The risks contain all the manufacturing environment risks as well as the threats to the single machine. In case of extreme situation one method is to switch off the power directly and stop the machine. The conventional way to do this is to use appropriate safety wires and devices like safety relays. The term static is used for this type of mechanism because it depends on hardware's, but in intelligent manufacturing processes where there is a lot of automation and everything is constantly changing this method is not suitable. A forced shutdown is generally associated with other disadvantages, like productivity losses, longer downtime and increase maintenance time. Dynamic security concepts provide an alternative approach which will depend on the complete assessment of altering automation processes and functional safety requirements. This approach, developed before the era of Industry 4.0, allows you to control processes safely without having to interrupt them immediately in case of error. However, the efficient implementation of this dynamic approach is only possible when the functional safety is integrated from the beginning into automation projects. If this is not the case, then is important to change the order of the independent production steps or a complete process. This is an obstacle to achieve the optimal solution. While only binary signals are often transmitted with static security, for example, to stop the movement of a machine by opening a binary gate, but in order to implement dynamic security more data will be needed. Because in this method there should be several safe modes of operation that will allow to perform activities with gate open. However, all the devices involved in these operations have this information.

2.2.2 Transfer approach from Industry 3.0 to Industry 4.0:

Objective of this transfer approach is to progressively enhance the safety of ongoing 3.0 industrial plants, as we know that this will we used for substantial period of time, and get ready for the change to industry 4.0. However, the establishment of universal standards for IT solutions is difficult to achieve because of the diverse and individual nature of existing industry. The journey towards Industry 4.0 need to establish a standardized model with help of which the security solution for every industry can be implemented quickly and profitably. The only possibility to accomplish this process, that the current IT security methods adjust to different situations established on independent security goals, a situation study to recognize vulnerabilities and hazards, and then compile a list of actions that will then be implemented.

2.2.3 Safety 4.0 from uniform design to interchangeable systems

Industry 4.0 vision includes modular systems, there are various important advantages of modular design for machinery or machine components. The modules of machine can be rejoined, replaced and exchanged. There is a possibility to change a piece of machine while the production is in progress, while at the same time parts can be added to machine to expand it. So it brings flexibility to the machines. While working with identical machines the operator can make more parts. The adopted safety solution should have the potential to adjust to this late change. It is easy to see the practical advantage of modular machine concepts while at the same time it expands the scope of standardization at functional level.

The benefits of modularization are often offset by a strict safety solution that depends on fixed wiring. Electronic safety systems use permanent safety circuits made of different hardware's, even if product is enriched with programmable logic circuit. The modern control systems have the characteristic that they mostly work without following any rules. The user must be able to optimize them freely according to their own degree of modularization. The PSS 4000 is an example of automation system which combine the features of modularization and flexibility. With this system it is possible to control all safety variable without any hardware and rigid electric circuits.

Based on the assumption that this is an advantage; security and safety is critical in this framework. Today, certification bodies test and accept machines as whole unit. So if the parts of machines are changed or extra part is added to the machine, this will require acceptance from the start. There are many solutions which brings into discussion but there is no standard solution. One common method is if a single module is safe then the machine is safe. Now it is the time to bring this issue into attention of companies and decision makers through trade associations. The progress in this area cannot be achieved without a legal work.

2.2.4 Unique and protected electronic Identification for products, processes and machines:

It is important for the widely recognition and acceptance of Industry 4.0 that the information transfer between two entities is safe. All the components (people, machine, process, departments) involve in the manufacturing of product have a secure way to exchange their data. To provide an easy and smooth exchange of information, every object should have a unique electronic identification. In addition, a kind of “security passport” should be given to every object that will contain all the necessary details of every risk. The risks which is already considered and evaluated during the product development as well as the risks which is treated by the operator or user. The passport should also contain the necessary security categorization. In the context of secure identification, to evaluate the overall security of CPS in the production environment these passports will serve as physical foundation for the systems. The safety assessment makes notes of financial worth of the product, capable threats and the adjusted and suitable countermeasures. Therefore, the strategic ambition of "Secure Identities" should be extended to contain "products", "machines" and "processes" covering both virtual and physical products.

2.2.5 Product must be Protected from infringement:

The reputation of successful products can be surely damaged by product piracy. So in the countries where salaries are high, essential component to survive in global market is the protection of intellectual property. The major problems because of product piracy is not only that it affects sales, but it also changes the company appearance in people mind and create a negative impact. The people who steals product knowledge can become competitor. The major problem is not limited only to the physical replication of products, but loss of knowledge. In modern era due to large number of IT applications and software in Industrial application the theft of product knowledge is common and can be copied. In industry 4.0 era, the product protection against piracy is very essential because there is much bigger cooperation between various industries along a value chain of product. Therefore, it is fundamental to seek solutions at a technical level, and to be more specific also at company level and competition law, that ensure the confidence and clarity within the platform while protecting critical business knowledge.

2.2.6 Safety & Security plan and design should be merged

Industry 4.0 needs revised safety and security approaches and the organized application of relevant methods throughout the life cycle of the system. As a basis for this approach, a common set of knowledge should be developed. The procedures and methods which are used for safety in electrical and mechanical engineering as well as in automation can be improve by using the strategies of IT sector. These methods can be then adopted to industries like automotive and aerospace. The projects for the advancement and evolution of safety and security on different topics like cyber security, artificial intelligence should be closely merged with Industry 4.0 projects on safety. In the future the material and serious outcomes should be handover to other industries such as the automotive and aerospace.

By using these policies, safety and security models for manufacturing schemes should be built as reference designs for the Industry 4.0 initiative. These models should be compatible, up to certain degree with the present Industry 3.0 structures. These reference architectures guarantee the standardization techniques and processes that are critical for the accomplishment of Industry 4.0. These reference model also allow the definition of test procedures and the establishment of test facilities which can be used to check the whole safety of systems at all levels, from the single machine through machine grids. Reference architectures can also act as foundation for delivering security categorizations and credentials for fresh subsystems and particularly for current ones. Therefore, this method can help us in migration policy.

2.2.7 Safety and security solutions should be easy in use

People always try to escape from the procedures and applications which are not easy to use. Such human behaviors have deadly results for safety and security solutions, particularly in extremely connected surroundings. Therefore, it is necessary to design safety security methods that adapt to the needs of the users, have user-friendly interfaces and, thus, assured the completion of the application. In order to have a proper solution, at each stages from the start of design to the engineering, operation each and every step should be followed.

2.2.8 Essential Training is necessary for implementing Industry 4.0 safety:

Every person of the company has essential knowledge of IT security issues. The essential awareness should be promoted in all individuals involve in manufacturing such as workers, operators, engineers, designer as well as security software creators. When safety and security methods are applied in a company, it is not sufficient to install merely on practical product, even if it is easy to use, still employees must also be adequately trained in the relevant safety requirements. The suitable awareness movements for the manufacturing sector could aid the present deficiencies in this space, while introducing mandatory courses on this subject to advanced education bodies would support to prepare the upcoming workforce.

2.2.9 Cost of Safety and Security should be efficiently measured

Security is always a cost factor. When the machines fail, this can have direct effects (for example, lower sales) and indirect effects (for example, claims for damages by customers, suppliers and allies or destruct the image of the company). So far, yet, only some industrialists have insurance for IT problems. Therefore, methods that can more clearly calculate the risks connected with Industry 4.0 and the cost efficiency of the related security resolutions should be developed, rather than closing production services in the occasion of a real or perceived IT hazard.

2.3 Significant elements for acceptance and adoption of safety and security 4.0:

Industry 4.0 manufacturing systems are highly interconnected structures that include a large number of people, IT devices, automation components and machines. There is abundant and mostly serious exchange of documents and information among the devices of the technological system, most of them act independently. While at the same time, lot of different people are working together along the value chain. However, safety is always the most important feature of the whole system. In addition to safety aspects, wide links and at least imaginary potential for third-party admittance in the framework of Industry 4.0 result in a whole range of fresh security aspects. Only if the subsequent ideas are placed into practice, then Industry 4.0 will be accepted and adopted:

2.3.1 Security through design is central design rule

In the older methods, security is generally assured through physical actions such as access limitations or further centralized security actions against external attacks. The CPS dependent industrial systems, adding security topologies to the system at a late stage is not enough. All features of safety, and especially security, must be integrated into the system from the beginning.

2.3.2 IT security policies, designs and standards must be developed and implemented:

In order to provide interactions between these highly interconnected, open and heterogeneous components a high degree of confidentiality, integrity and availability is required. There must also have a reasonable, reliable and affordable solution to protect the knowledge of the digital process, intellectual material rights and information in particular of every single industrialist and machinist, both from abroad and in terms of components belonging to different machinists, and provide industrialist. In Industry 4.0, therefore, it is permanently essential to follow a universal safety method. In addition, from the current point of view, Industry 4.0 also requires a dual strategy in terms of safety and security.

First, present factories required to be equipped with the safety and security procedures to meet the new requirements. Due to the lengthy life of the machines and the short improvement cycles, as well as the heterogeneous and sometimes very old and difficult network connection infrastructure, this is not an easy job.

Furthermore, solutions for fresh plants and machines must be established. The conversion from the third to the fourth manufacturing revolution should be as fluid as promising and employed so that all relevant actors can easily understand it. A central portion for both pillars of the policy is that all the players during the whole value chain reach an agreement on the safety and security matter and the corresponding architecture earlier than the implementation commences.

2.3.3 Implementation, psychological and educational issues:

In addition to technical sides, effective safety and security resolutions must also take into account the marketable, psychological and educational problems.

For instance, the industry presently lagging behind to provide a standardized operating platform to implement adequate safety and security solutions, which are made for the specific wants of the industry in terms of implementation and costs. There is always minor chance to improve or upgrade the current infrastructure, because many safety solutions are initially established for other businesses or applications. In addition, security attentiveness frequently shows a key role, especially in relation to IT security issues. There are currently too many safety concerns in different industries. Given the point that Industry 4.0 will result in greater connection and collaboration among various different entities in a value chain, it will be essential for all these entities to have greater level of trust in each other’s abilities. Machine and plant creators are mostly aware of the worth related benefits of the software, which leads to a severe increase in the quantity of software modules in the manufacture of equipment and machinery. However, very little is familiar about the related IT threats. Manufacturing IT security start to be discussed in the automation industry from the public discussion about malware such as Stuxnet, Duqu or Flame. In addition, the software plays progressively vital role in providing and maintaining security and protection. But the importance is not this properly addressed in manufacturing processes.

Industry 4.0 requires far more active safety attitude. Currently, safety and security matters are mostly addressed reactively, after the completion of development process and certain security issues already took place. Though, this late implementation of security resolutions is expensive and mostly does not provide a stable solution to the problem in question. Safety and Security should not be divided into functional mechanisms, but it must be considered as a progression. To attain rapid reply times, it is also significant to offer support over checking and the widespread exchange of intersectional information. Currently, risk evaluation pointers, especially with regard to industrial IT security, are not sufficiently monitored and only a small amount of information towards safety and security occurrences is exchanged. Action in these regions will aid to stop the extent of viruses or unselective cyber-attacks.

2.3.4 Workplace and worker’s safety:

The main importance should be the improvement of workers' safety. With the solutions offered by new technologies, it is indeed possible to monitor all the activities carried out by operating employees, monitoring their well-being and preventing accidents at work. It is also important that workers should know that the application of fresh technologies will increase protection for them and it will not complicate their daily work. But it is certain that like all other high-impact innovations, the immediate transition to assisted work will not be easy, however, it will improve both performance and protection of workers. The main changes which these new technologies bring compare to the past, is that now you can automate many repetitive operations, with a very long series of consequent advantages. Some examples can be the reduction of errors and therefore minor defects and waste or the reducing the time needed to perform certain operations. Another significant contribution that it can give relief to workers from operations to be repeated identically for whole life, using them for operations that require a more active commitment. Or again, they can be joined by robot’s, which is fundamental piece for automation in carrying out his duties to relieve himself of excessively heavy loads.

Chapter 3 Industry 4.0 Technologies and their Safety

3.1 CPS

Cyber-physical systems form a core of Industry 4.0. Cyber-physical systems are physical and technical systems whose operation is monitored, coordinated, controlled and integrated by a computer and communication core [17].

A CPS combine processor items, sensors and actuators, and allows IT infrastructure to interact with the real world. The Internet of Things (IoT) are the base in this revolution of cyber-physical systems. All the objects of a CPS and various CPS are connected to make a network in which billions of systems and entities can cooperate and exchange data. With its ability to transform conventional procedures by combining technologies of different sectors, CPS offers innovations to numerous industries, involving the automotive and aerospace industries, chemical processes, smart energy and water networks, medical care, manufacturing and transportation.

These structures can destruct themselves, individuals, or belongings if used incorrectly. This incorrect use may be due to a letdown of a single components or a deliberate effort to damage its performance. Safety and security are the dual important characteristics in each CPS, which have similar objectives: to protect the CPS from unintentional breakdowns (safety) or planned attacks (security). In this framework, there is one accepted demand to look at them from a single point of view in the development and operation of complex CPS.

3.1.1 CPS should be capable to confirm the safety of its independent decisions.

The key challenges in CPS to ensure functional safety and at the same time manage all authentication and authorization methods. Because of Industry 4.0, CPS have just draw attention in the subject of plant automation. The advantages from automation is also applied to CPS which independently accomplish dynamic reconfiguration of industrial practices. But mostly the benefits are overshadowed by the fixings of these systems based on the dangers that these methods can cause on failure to both environment and people.

Safety standards like IEC 61508 describe processes and procedures to be adapted to the expansion and lifespan cycle of control systems that decrease the remaining risk to an acceptable level. To get CPS models such as independent reconfiguration to industrial automation, these ideas essentially be properly verifiable by the CPS about the functional safety of the whole process. This needs official semantics of the automation procedure and the cyber system comprising functional safety together.

3.1.2 Human robot Interactions should be safety aware:

The robotics expertise is also a crucial driver for modern manufacturing facility. These industrial robots might help their human co-workers on the factory floor in health frightening, complex, high precision, repetitive and difficult tasks.

In Industry 4.0 applications there will be a close physical interaction between robots and humans. The important requirements for these robots are, they should be safety aware and know their movements which could injured or threaten people and dynamically avoid from executing them. In Industry 4.0 age, famous robots are smart, capable to help, flexible, movable, and linked. Some of the example of these robots which are in use are Bosch APAS assistant, KUKA LBR iiwa, ABB YuMi, FANUC CR-35iA, MRK Systeme KR 5 SI, and Universal Robots UR5.

Important issue in safety aware physical human-robot collaboration is the methods to determine that in what way the robot will accomplish its movement in a safety aware style. It's important for the robot to notice safety related things and occasions and configure its movement safely. In order to model mathematically and investigate the properties of dynamical systems, the tools are provided by the control system engineering. The feedback controllers can be manufactured by using these tools to attain a chosen physical movement by providing a signal to the motors of the robot. The dynamic state of the robot is constantly monitored by a typical motion controller which compares the desired motion trajectory with sensed state, and issues instructions to reduce the fault among the sensed and wanted motion trajectory. These robots equipped with complex programs for safe and effective collaboration.

3.1.3 Collaborative robot's successful implementation in Industry 4.0:

For the evolving industrial robotics, the term collaborative robotics is used. Collaborative robots shaped the people and robots without a safety cage work side by side to do things. The use of collaborative robots in the automotive industry, assistance in smart manufacturing focused on Industry 4.0.

However, there are several safety problems regarding collaborative robots and their implementation in the industry. In human-robot collaboration, this conduct is linked to the reaction of robots when a physical contact with man arise during performing a task. In human-robot physical contact, human safety is the important objective and must be taken into account at the time of assessing robotic configurations in a work environment.

The two productive robot implementations in manufacturing related to Industry 4.0 are the robots applied in the BMW and Tesla car factories. In the BMW plant, independent moveable robots for intelligent carriage systems are used in supply logistics, whereas KUKA collaboration robot is used in addition to people, for example, to lift and place weighty parts and perform welding jobs. Similarly, the Tesla plants used robots with additional tools in their manufacturing lines to help smart products.

The collaboration among humans and robots is a fresh change in manufacturing and service industries. Robots are the parts of the Industry 4.0 approach. The objective of this strategy is to create a safe surroundings for human-robot collaboration. The agenda for safety in collaborative industrial robot environments exists where CPS is presently involved as portion of the most current development in smart production. When CPS is used the exchange of the work space between human and robot is possible.

Moveable robots are transformed and made enjoyable for human employees in the factory. They work independently with autonomous drivers and can recognize obstacles and be aware of human present in the place. Various examples of these robots are KUKA youBot, mobile industrial robot (MiR) and self-propelled OTTO vehicle (SDV).

3.2 Internet of Things

When the word, Internet of Things (IoT), came into existence, the first thing at that time come to mind was the distinctively recognizable interoperable linked objects that used radio-frequency identification (RFID) technology. By connecting the RFID tags to the Internet, we are able to identify and trace things labeled in actual time automatically and uniquely. This is what we called Internet of things (IoT). But then in future, IoT technology has been applied with various tools such as sensors, actuators, the Global Positioning System (GPS) and moveable objects that work through Wi-Fi, Bluetooth, cellular or near-field communication (NFC). Today, IoT establish himself as a universal connected infrastructure composed of various merged objects based on detection, communication, network and information process. The information exchange between the devices occurs via the network that used the standard protocols of communication. The range of intelligent linked devices get so wide that today it is using from simple wearable equipment to huge machines, everyone having sensor chips. For example, the smart shoes comprise chips that helps in tracing and evaluating data. In the same way, the security cameras fixed for observation of a place can be watched remotely from everywhere. Various smart devices providing tracking and connectivity in automobile. The effectiveness of the whole system can be improving by data collected with help of these devices and process in real time. RFID, wireless sensor networks (WSN), Machine-to-machine (M2M), and Cyber Physical System (CPS), today advanced as essential components for the wider term IOT. With RFID, microchips can convey identification data wirelessly. RFID reader allow users to automatically differentiate, trace and monitor items labeled with RFID tags. RFID are using in various different industries, including shipping, postal application, medical care, material management, retail, defense and more. Alternatively, WSN uses connected smart sensors for detection and observing. WSN is using in many applications such as industrial monitoring, environmental watching, transportation checking, health monitoring and others.

3.2.1 Security Problems and Worries using IoT devices:

IoT objects are getting more universal and connect the cyber world with the physical world. However, this leads to new and added complex security problems and worries. The features of IOT devices cause the design of IoT security further difficult than the past. These features are mainly an extensive and cost effective design, resource limitations, the diverse nature of the devices, choice of function over security, advanced privacy needs and stricter trust management. In particular, resource limitations mostly involve partial computing power, power and storage ability. These characteristic create difficulty to put on various conventional security solutions to the Internet of things, including the generalized public key pattern and IP-based security solutions. Because of the poor strategy of IoT security, mostly it is easy to compromise IoT objects rather the traditional computers. The security of IoT systems needs urgent improvements. Security breaches in IoT systems are expected to have serious consequences. For instance, serious accidents will happen by turning the vehicle remotely due to a security breach. Similarly, smart health devices are used in the industry to control the health of workers. However, the safety of these devices is also a critical concern. It is enormously unsafe to halt a safety device while working. Furthermore, privacy is also a major worry for intelligent health devices since lot of the information contain in the system is largely sensitive medical data. The current weakness of IoT security can be documented to the lack of knowing of the security challenges of the current IoT systems. Our goal is to perform a comprehensive investigation of security challenges in IoT systems to pave the way towards a better security solution.

3.2.2 Architectural view of IoT:

IoT is a method that connects several large and diverse IoT devices. Huge amounts of information are together and transmitted in IoT terminals. Based on the examination of the data together, the IoT aims to create a smart world. A common three-layer architecture of IoT systems are presented in Figure 3. IoT systems composed of three-layer name as the cloud layer, the edge layer and the things layer. Each of them can collect, process and analyze data. Bidirectional communication is generally compatible, although in general far more amount of data is transmitted towards the edge layer from the things layer than vice versa. The Things layer holds a lot of diverse things, comprising sensors and actuators. The things of IoT, also known as terminals, are combination of physical entities and cyber entities. The physical components of things enter the physical world, whereas the cyber parts elements allow computation, storage and connectivity. The specifications, involve calculation, storing, communication and power supply, can be very different in thing devices. But most of the time, resources are limited and energy is limited. Consequently, they are not appropriate for heavy jobs.

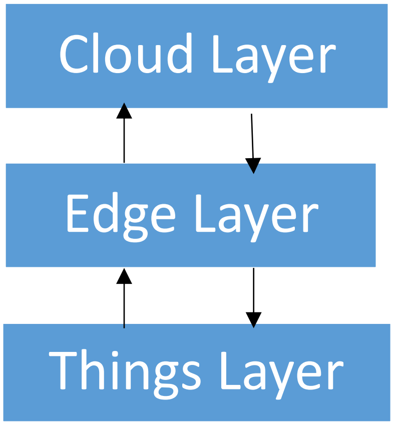


Figure 3

Instead, the cloud layer is enormously authoritative and has numerous means to perform heavy jobs, such as: For example, extracting information from a big volume of data and fulfilling very complex jobs. Moreover, there are several powerful tools and innovative algorithms which will be used to create commanding applications. Cloud layer and things layer are interconnected, however generally very separate and have no straight communication networks. To transmit the whole data from things to the cloud is very expensive. Therefore, the cloud is not an optimum option to help IOT applications which has the characteristic for instance extraordinary real-time needs, wide geographic circulation or large mobility. In order to fill the gap among the layer which has less resources and the high resource cloud layer, edge layer is placed between them. The edge layer has converted into a very significant layer in the IOT architecture. Typically, edge objects connect straight to things or back off from them. Compared to things, edge objects usually have high resources, comprising power, calculating power and storage. Perimeter objects are generally linked to the cloud through a speedy Internet. You can effortlessly use dominant cloud facilities or work with the heavy-duty cloud layer. Therefore, the edge layer in this architecture perform crucial part in connecting things and cloud. In summary, every layer in IoT architecture has its individual distinctive properties. To create an effective IoT system it is essential to work collectively. The provision of IoT tasks can be optimized taking into account the characteristics of the different levels. Therefore, the entire implementation architecture must be protected against attacks that could affect the services provided by IOT and compromise the confidentiality, reliability or secrecy of the data. Consequently, security solutions must adapt to limited architectures. In the near past, enormous struggle has been put in to take into account the security matters in the IOT paradigm. Various of these methods address security concerns at a particular level, while further methods aimed to provide end-to-end security of IOT.

3.2.3 Security challenges within IOT:

Security is a necessity for IOT structures to defend confidential information and important physical infrastructure. Lacking a decent level of protection, people should not be able to use IOT devices and their applications. Security in conventional network systems residues a challenge, whereas IOT systems pose several other challenges as a result of several specific features of IOT systems. A deep knowledge of these challenges is vital for the development of security resolutions.

3.2.3.1 Merging with physical world:

In the IoT application, the linking of the cyber and physical domain raises additional security problems, meanwhile the physical domain can nowadays be changeable over the cyber world, which can have awfully damaging results. Because several IOT systems are task dependent and uninterruptible. In these situations, traditional security rescue methods cannot be implemented. For example, the shutdown, restart and subsequent restart sequence may not function properly since the manufacturing process cannot be stopped. Furthermore, an IOT system, the physical and cyber components must be friendly for the system to work correctly. This can be tricky. For example, a physical object that solitary function properly with old operating systems that not anymore compatible with the manufacturer becomes a serious vulnerability. This weak link can endanger the entire system. Due to the tight coupling, the impact on the other side can be a great risk and the negative effects can spread in both directions. Therefore, not only confidential and private data and information can be attacked, but also physical devices. Taking into account IOT applications such as the intelligent network and intelligent health, both loss of function and loss of life can occur. Unlike conventional calculating devices, several IOT devices are not adequately protected. When attackers gain entree to these exposed and undefended devices, they can continue to attack and conquer cyber systems. The critical objective of IOT is to create a smart world constructed on the outcomes of the investigation of the data together in the systems. In general, control texts are repeatedly transmitted from the cloud or the edge level to actuators or terminals to regulate the physical domain. In this manner, the cyber system could be conceding in several places, comprising the three levels and the communication link. That is why we need to break down vulnerable systems into IOT security design to avoid negative impacts. To achieve this, we must investigate the granular entree control architecture and methods that limit the spread of security breaks.

3.2.3.2 Diverse devices and communications:

The flexible and applicable nature of IoT technology make it very significant. While IOT systems are adopted for a variety of applications, they often use different tools with different hardware and software disclaimers. Usually, we observe several IOT devices that start on a variety of operating systems with different communication networks. Therefore, conventional security methods are not appropriate to IOT schemes. For example, security resolutions on Windows systems frequently cannot be applied for further operating systems, like Android. Moreover, IP-dependent security protocols, such as SSL, HTTPS and SSH, do not implemented on low performance devices, for instance sensor devices. Sensors mostly cannot directly support IP dependent protocols. That's the reason that we used changed levels of security for different portions in individual IOT systems. The device which has the minimum security level converts into the weakest entry point and concludes the whole security level of IOT systems. As soon as, this device is attacked the other devices can be exploited. In summary, while planning the IOT security solution, it is prerequisite to adjust to security algorithms and protocols for the hardware and software applications. The security of below performance devices should be improved by supporting higher performance devices. IoT offers a much more demanding computing surroundings that requires productive security solutions where security is autonomous of device specifications, operating systems and communication networks.

3.2.3.3 Limited Resources

In order to reduce designing and production costs, dealers frequently prepare IOT devices with partial abilities. The consequence is low capacity devices with several limited resources for instance little memory space, inferior computing capacity, small communication bandwidth and imperfect power supply. Integrity, availability and confidentiality are goals of high-level security. The mechanisms that include encryption, validation, entree control, interruption exposure and firewalls are adopted to get these objectives. Though, IOT resource limitations significantly reduced the likely security solution options since numerous recognized security mechanisms cannot be adopted with lower capacity devices.

3.2.3.4 Privacy:

Large IoT systems gathers and investigate large amounts of information to develop intelligence. Privacy protection is one of the big worry. While put into practice in the medical field, the Internet of things can compromise the privacy of medical data. IoT systems need to use information to perform their tasks, however privacy is also essential to keep at an acceptable level. The problem is recognizable and requires a solution. There is also a compromise among privacy and security. Advanced data protection requirements likely to need a weaker identity. Alternatively, tough security often needs a resilient identity, especially in validation. When designing the IoT security solution, privacy should be highlighted. However, how to attain the best equilibrium among privacy and security is a wide query that must be responded.

3.2.3.5 Large Scales:

The IoT devices is increasing every day that make it very difficult to develop security solutions for IoT systems. First, many interactions between all devices significantly increase the cost of providing security. Secondly, it is very tough to apply key management patterns that are previously prone to scalability problems to huge IoT systems. The enormous amount of linked IoT devices significantly raise the attack scope, and every device are converted to a target for specific attacks. Consequently, perfect IoT security solutions must be scalable, allocated and repeatedly rearrange. The solution need to be ordered and insulated.

3.2.3.6 Trust controlling:

Trust calculation is essential part of security scheme. Since a large part of the IoT systems are systematized as peer-to-peer or ad hoc links, trust controlling residues a major challenge in the IoT, and important problem with any peer-to-peer or ad hoc network. Moreover, high movement, lack of universal identity and a transient affiliation between IoT devices make difficult the scheme of an effective trust solution. Lastly, IoT systems generally do not have centralized management and absence the structure to document the performance of IoT devices. Trusted simulations are obligatory to assess the status of IoT devices.

3.2.3.7 Less Preparation for Security:

IoT security breaks are initiated by poor security in the design and manufacture of IoT devices. Therefore, it is a great challenge to change people's attitudes. First, many current IoT device manufacturers do not have the equivalent knowledge of cyber security, as conventional cyber device producers. Therefore, they find it tough to make high-security IoT devices in the small term. For example, numerous IoT devices continue to use uncomplicated normal settings. As a result, attackers will easily hack devices by simple hacking techniques in order to get usernames and passwords. Additionally, since functionality and ease of use are smooth to sell, they are generally favored over security, and it is difficult to encourage people to participate in security. Due to the partial security budget, it is very difficult to guarantee high security for many IoT devices. In addition, several security solutions might not be acknowledging by the market and people, as they affect functionality and usability.

3.2.4 Architectural Security Design Solution for IoT:

We have already said that it is very challenging to made possible the security fulfillments of IoT devices. Different types of security solutions will be adopted to accomplish a high level of security for the Internet of things, such as: For example, the design of lightly built security algorithms and protocols, effective data protection algorithms and protocols, safety structure to shield physical systems and several automated methods to accomplish and organize security settings for IoT devices. Between these, architectural security scheme is paramount and should be first. The architectural security models will lead further security designs. Now, three distinctive architectural security patterns are presented, that comprise of end-to-end security at things, security function installed at the edge and distributed security model. These schemes will be used to model upcoming security solution patterns, such as Internet of Things (IoT) security protocols.

3.2.4.1 End-to-End (Things Layer) Security solutions:

End-to-end information exchange is essential in interacted systems, containing conventional Internet and IoT. Protocols like IPv6 are used in IoT for end-to-end communication. Allowing end-to-end protection between terminals or among terminals and other devices is essential for several IoT functions. For example, end-to-end protection in a vehicle linked application where vehicles obliged to work collectively to perform joint jobs, such as improving driving safety. Of course, once end-to-end protection is completed at the level of things layer, various present Internet-based functions can be prolonged to IoT applications. However, limited resources at this level reduce the selection of offered security procedures.

The first way to provide end-to-end protection in IoT systems is to rise existing resources, like memory and processing power of IoT devices, with the aim using conventional security solutions. Second solution is to increase other security associated hardware that assists the distinctive identity of the device. However, the limitation is that numerous current IoT devices are not furnished with additional security components. This increases the price of individual IoT device. Another solution present in the literature is end-to-end security protocols. Many of them are expansion of the current IP dependent security solution. The most common dual is IPv6 security protection and 6LoWPAN security protection. Of course, IP dependent security algorithms can be prolonged to end components, but the computational cost of these components is very huge. Struggles have been put in to simplify IP-based security protocols. End-to-end security has numerous benefits. Major one is, for end components it is not essential to rely on any additional device since they are not transmitted to further components to accomplish security objectives. Second, the system design is a type of plane design. Reduce administrative costs. The confidentiality of the third-party device can be well secured since they can choose how much data to share.

3.2.4.2 Edge layer security solutions:

Various devices, for instance intelligent bulbs and RFID tags, will not possess enough resources to provide end-to-end security. As an alternative of end-user protection, security supervision jobs can be moved from lowered endpoints to extra powerful peripheral components. In this situation, the endpoint might need to rely on the edge layer and employ the edge layer as a security means to achieve protection requirements. Moreover, with added information on the edge component and the offered computing capabilities, the edge component can execute attack recognition algorithms to sense attacks, thus the attack may be controlled as rapidly as possible. With more resources on the edge, computer concentrated jobs like information encryption, key creation and attack exposure can be moved from endpoints to those resources. This is essential for endpoints which have low resources like: Passive RFID tags and intelligent bulbs. Subsequently, the edge components and the final devices are physically closed. This not only reduces costs, but as well as increases the actual time performance of IoT applications. The border layer has additional information compare to the final device in the entire system, so that enhanced security management in the edge layer can be provided. The limitation of this approach, however, is that the terminal must rely on the edge device without restriction.

3.2.4.3 Distributed security model for IOT:

Edge dependent security solutions require endpoint components to believe Edge components. This can be uncertain in various circumstances. Verification methods will be used to create trust among endpoints and peripheral components. Maximum present scalable verification rules based on public key or symmetric key structures, however the endpoints might not possess appropriate resources to aid these required processes. Related to temporarily linked edge devices, permanently existing endpoint cloud functions are greater reliable in most cases. Through this level of acceptance, cloud can deliver identifications so that the Edge components can achieve confidence from endpoints by presenting verifiable cloud credentials. This concept can be applied in four phases. Earlier than the start of communication between the edge component and the terminal, the edge component directs an appeal to the cloud in the first step to request access to a particular terminal. At that moment, the cloud confirms the reliability of the perimeter component through a confirmation and approval verification or the confidence factor is measured using a trust model existing in the cloud. Then afterward cloud granted identifications for the edge component. In the third stage, the edge component offers the identifications of the cloud to the terminal and the terminal authenticates the authorizations. If all the previous stages are positive, the terminal can begin to rely on the edge device in the fourth step. With this scheme, the final component, the edge component and the cloud work collectively to attain an extraordinary level of security. That is why we call it a distributed security model for the Internet of things.

The cloud layer function is normally greater reliable than the edge layer function. This might reduce the threat of relying on the edge layer. With the resources obtainable in the cloud, several complex security solutions can be reinforced. Third, it is useful to allocate the security job across many levels. We can say that; the distribution of security information memory contributes to increased security.

3.2.5 IoT devices enhance Work Place:

The goal for Internet of things and Big Data to analyze and handling of information flowing inside the industry. But there should be a mechanism to use these information and new technologies in the most appropriate way with the intention to improve health, safety and enlarge human conduct in work situations. But at the same time, the insertion of fresh technology from a sociotechnical view linked to countless hazards and applications of technology bring anxiety, frustration, condensed pleasure and job satisfaction. To support the interface and enhance operator efficiency it is essential to identify what the operator feels about the system. The encouraging application of IoT devices is evaluating physiological statistics relating it with work surroundings statistics to guarantee a respectable working place for the operator. There are various prospects to automate wide range of workplace data (e.g. pulse, emotions, activity, temperature, etc.). If this data is linked to threshold values (for every person) it can provide an indicator to the operator e.g. At what time he should get a break. A demonstrator must collect information according to the operators' likings and should contain a function that informs the operator once the onset is breached and recommend to him/her an action. This might support the work headed for social sustainability and enlarge comfort at the place of work.

3.2.6 IoT Framework design for manufacturing plants

We have to describe an IoT system which collects human related data from a plant, where employees and system cooperate with each other. The system will collect data from different objects and exchange data with a principal server, that have the aptitude to accomplish data and generate substantial information from the given data that will allow the designer or an expert to make choices in a faster and accurate way. The managing of the human-related information will help to understand the workers wellbeing. The linked plants offer large proportion of data associated to machines, CPS, goods, surroundings, and people, however it is important to recognize the information useful for research. For instance, to study the machines it is probable to observe energy utilization, throughput, pressure, vibrations, etc. then merely the final information might be considering if worker's safety evaluation is performed. But it's important to discover every usable sensor in market that permit the checking of the identified variables at minimum costs. To improve the environment and the work condition, use the information together by the sensor to enhance the system with appropriate arrangements. At this point to present the distinction amongst a sensorized setting and an intelligent setting. For example, in a sensorized situation, the temperature sensor obtains the temperature information and displays a figure (e.g. 18°C). People will sense cold, and will see the figure in the display and rise the temperature. In the smart situation, the sensor will be present in the environment and also in the human. The temperature will be below a fixed threshold; the thermostat will automatically rise it. But this will require the connection with a correct actuator allows the routinely performing of remedial actions according to the rules established. Such a procedure should be directed by an accurate actor, an innovative qualified person in the framework of the upcoming factory: The IoT Engineer. The engineer will be an expert of both sensors and processes. Every method will have a suitable set of sensors that will allow to analyze it. Supervise the working environments with the help of appropriate sensorized system will develop the operational safety, avoid occupational sicknesses and distracts, avoid absence and will improve the worker’s efficiency. It also enhances the work place attaining a win-win state equally for the operators and company. Workers participation also build a progressive workplace in which comfort has been encouraged thanks to the innovative cultural safety help prepared by employee awareness. Lack of the IoT structure, where limited were information connected to one another, the similar evaluation is not possible.

3.2.7 Wireless communication technologies continuously monitor workplace environment

In new industrial transformation, it is important to design a fresh industrial model intended at reducing the hazards with respect to worker's health and safety, and assure their wellbeing and comfort in machining, handling and assembly operations. The information exchange through wireless devices provide a great support to provide a better working condition**.** Wireless communications network transport the information collected by the sensors. This information will be significant to recognize, discover, monitor and manage constantly the comparative hazards to health and safety. Though, the utilization of wireless communications in manufacturing environments introduce substantial challenges. On one side, manufacturing environment is frequently categorized by challenging transmission situations (obstacles, multi path propagation, interventions, etc.) that create complication in the development of robust wireless connection. On the other side, safety interrelated manufacturing applications are described by exact reliability and timing needs, and consequently needs trustworthy mobile recognizing and communications platform. The wireless communication technologies in this regard provide tool to apply mobile recognizing applications. The sensor dependent platform might be observed in actual time and in depth structural way. All the actions occur in the industry, from the medium levels, to the location of every object should be traced and possible risks should be estimated over automated defended actions. In the framework of the sensing enterprise, we will not merely arrange the recognition of risks but will also help in the actuation and utilization of the protective jobs pick by the safety and healthy manager over the modified support tools.

Wireless information exchange is now getting skillful to identify hazards efficiently and continually in the factory. In order to provide the reliability of such systems, mutual technical environment able to observe the working and efficiency of entirely networks and connected sensors to remote control centers required to be employed. These platforms will decrease occupational hazards by enabling the mixing of general scrutiny applications. We can conclude our remarks that the wireless communication will play substantial part to make better the work conditions, worker’s health and physiological conditions. Wireless sensor networks with clever schemes and accurately combined technical support will avoid the injuries in independent and smart manufacturing surroundings.

Chapter 4 Implemented Technological Solutions in Industry 4.0 environment for Safety

In order to have a harmless environment inside the manufacturing plant in Industry 4.0, first of all it is very essential to recognize that how will be industry 4.0 workers, and how will be environment surrounding the worker.

4.1 Worker 4.0:

The Industry 4.0 worker will be a sort of "hybrid", as it is halfway between the classic operator and a robot, able to detect data around him and send it to anyone connected. As a "hybrid", it must therefore be able to analyze, record and communicate information relating to the environment in which it operates, as well as performing its work as it did previously. So, we decided to study all the devices and their role in safety, that a worker is obliged to have on and that can be a source of data collection and communication, as well as reception of information. The devices which the worker use for safety purpose during work environment are called Personal Protective equipment's.

Among the PPE currently in use, there are many that can become "smart", for example; helmets, glasses, gloves if you want to name a few common. The reasons that can lead a company to adopt intelligent PPE, more expensive than those standard, are varied and contribute not only to the increase in the efficiency of the operator, but also to that of his safety. These devices in fact lead to a reduction in intervention times in the event of health problems, thanks to interconnectivity, greater surveillance and field monitoring and, thanks to data collection sensors, to a greater awareness of the dangers found in the circumstances. Furthermore, efficiency is also increasing of the operator, who is able to report any problems to their employees in real time solution and, with the support of these, to solve them in minimum time.

4.1.1 Sensors available for improving HSE in Industrial Environment:

The new advanced sensor technologies offer several solutions to improve health and safety through real-time observing of dangerous aspects like carbon dioxide emissions, unveil to chemical reactions, optical emission and high or low temperatures. Similarly, with these sensors we can monitor the health status of workers by evaluating key physiological variables (for example temperature, heart rate, respiratory rate, etc.). Monitoring of workers well-being (for example, temperature and moisture of underclothing, work positions); physical location of workforce in relation to possibly unsafe items or risk areas; Monitoring of the present level of PPE protection; Determination of the service life of the PPE employ by workers; cautions to workers in occasion of dangerous conditions; and the initiation of protection systems once surpassing a risk threshold.

4.1.2 PPE (Personal Protective Equipment):

The role of the PPE in monitoring the work environment has changed. PPE devices are used not only for passive protection against risks, but also as sensors to monitor the parameters of the work surroundings, the worker's condition and their position in the place of work. Additional trend was the inclusion of signaling systems in the PPE modules that allowed the worker to be alerted, e.g. message on the appearance of dangers or instructions to stay from them. Specific integrated systems, which are usually dependent on augmented reality (AR) technologies, might as well deliver employees with useful instructions for extremely specialized jobs such like maintenance, repair or welding. In addition, it is also feasible to use portable electronic devices to control the level of protection provided by the PPE, taking into account the existing dangerous aspects in a particular place of work. This performance permits the identification and estimation of fluctuations in PPE protective variables that can happen under the influence of environmental features. Implanting Smart materials in PPE objects also allows them to quickly change their protection and use constraints, as well as actively adapt their properties to the environment and the needs of each person.

4.1.3 Use of Smart materials for Safety functions in Industry:

SM (intelligent materials) are materials that can respond to environmental changes by significantly changing their properties. Now a day, the market has an inclination to deliver thermal regulation features to the PPE. In particular, phase change materials (PCM) and super absorbing polymers (SAP) utilize to overcome thermal stress. PCMs can hold and deliver definite quantity of heat in the form of latent heat in a particular temperature zone. This ability has been used in a thermal regulation vest to reduce the thermal discomforts when working in hot and cold environments. SAPs have the ability to collect and hold enormously huge quantities of liquid relative to their weight. To avoid liquid perspiration on the skin that greatly affects human sensation, SAP inlays were placed below the tight protecting clothing. Another group of SM reacts with changes in optical, mechanical, chemical or thermal properties when operated with electricity. Such materials get employ, for example, as actuators to make cool the heated protective clothes or for operator interfaces dependent on helmet-mounted screens. However, to allow proper operation of these SMs, other elements (such as power supplies, sensors and control unit) are required. In general, this set of SMEs is not adopted as an independent solution, but as portion of the ICT dependent systems integrated in the PPE.

4.1.4 Wearable Electronics use for safety purposes

Wearable Electronics are the objects permanently connected to operators and very simple and useful to operate and hold. In the near past the developments in ICT technologies have directed a growing attention in portable electronics. which has led to the progression of a group of solutions in the field of PPE, ranging from portable devices with sensor and actuator assemblies, individual to highly specialized solutions ES (Embedded Systems). Several sensors that gather data on certain environmental variable guarantee the collaboration of these systems with the SE (Smart Environment). These messages are processed and transmitted to the actuators, which allows the system to respond instantly to variations in external environments. There are currently various kinds of ES that permit observing of several physiological variables that include posture, muscle activity, blood pressure, skin conductance, exercise, oxygen content, hydration, temperature, brain activity, glucose, eye monitoring, sleep, breathing, Ingestion and monitoring of the heart. For example, it is proposed to apply an ultrahigh frequency (UHF) epidermal passive sensor to human skin precisely to ensure wireless and continuous real-time measurement of human body temperature. The fiber optic sensor integrated in the PPE allows to measure the pulse of the arm and the natural movements that accompany the breathing and the heartbeat. As part of the ConText project, non-contact textile sensors have been developed. They record the user's muscular activity and collect information on the levels of physiological stress that might be utilized to further reduce the danger of musculoskeletal disorders.

4.1.4.1 Safety Helmets:

One of the motivating answer in this area is a wearable computer merged standard safety helmet to safeguard people from carbon monoxide poisoning through constant and non-invasive checking of blood gas saturation points. Another method to help employees provide information is to use AR systems to monitor the environment and enter extra facts in the user's zone of vision. A better sample of a PPE object that can be combined with an AR module is a welding helmet employ in traditional welding. In this matter, several solutions have already been established to offer the welder with real-time help, for example, with information on the location of the welding gun. Similar technical support can be provided, complemented by initial cautionary signals produced in a hazardous condition, by means of a fully transparent portable screen located under a shielding visor of an industrial helmet furnished with an AR module, cameras and sensors.

4.1.4.2 Smart Jacket:

The ProFiTex project has developed an intelligent jacket with unified sensors, electronics and a safety cable that serves as a means for information and energy transmission. The project motivated on providing navigation direction to firefighters in smoke areas, as well as the transfer of information among firefighters and a leader using implanted beacons.

4.1.4.3 Smart Gloves:

In the protective gloves for firefighting and portable electronics is integrated. In some cases, the suggest fireman's gloves with an integrated radio system to measure temperature, haptic response and gesture acknowledgement to help employees with warnings and messages related to heat. To be more specific, the system incorporated the subsequent sensors: 2 accelerometers to interpret hand gestures or inactivity; an analog temperature sensor to monitor the human temperature on the rear of the hand; a thermocouple to quickly measure contact heat; and a barometer to detect changes in atmospheric pressure. In addition, two miniature vibration motors were integrated in an elastic portion of the glove to give haptic feedback to the firefighter in dangerous situations. This application made it possible to generate different vibration signals whose meaning depended on the pulse length.

4.1.4.4 Smart Trousers:

The merging of ICT components into standard PPE objects also provides an excellent chance to implement actual time control of PPE protection and satisfied features, as suggested in the HORST project. In the context of this specific project, the safety of foresters was enhanced by replacing typical protective pads with extremely sensitive magnetic field sensors implanted in cut protection trousers. Such intelligent PPE construction permit a moveable chainsaw to stop robotically and instantly while the mobile chain is very near to a worker's legs. Recently an analogous portable safety component has been patented to cover the body part of worker.

4.1.4.5 Smart Clothes:

The PROeTEX project, shielding clothes for firefighting has been merged into a Body Area Network that comprises: a module to monitor rescue actions depends on signals and accelerometers of the global positioning system (GPS), heat flow and sensors of gas for evaluation of chemicals and heat hazards, as well as long and short distance communication modules that provide rescue team members with the support they need to provide information. Following, the SafeProTex assignment concentrated on improving the level of clothing protection to guard workers uncovered to difficult operations and emergency circumstances, such as: As firefighters and first aid medical personnel in tasks under dangerous weather situations or in danger of forest fires. In similar project, PROSPIE, the main goal was to develop the ease of firefighters by reducing the thermal load when exposed to a hot microclimate. Due to this reason, a system was considered to monitor the thermal condition of a worker, and the cooling agents like cooling salts and PCM, as well as ventilation-based cooling.

4.1.4.6 Smart Vest

There are some PPE solutions that use ESs to decrease the capacity of work associated with physical handling, like: The vest stores the user's kinetic energy and, thanks to the electronics integrated in the textile material, releases it when necessary. An active thermoregulation system has also been embedded in protective clothing envisioned to employ in cold surroundings. The system spontaneously regulates the user comfort to alter weather conditions by monitoring the power supply to the heating elements. Similarly, light-emitting diodes have been proposed to enhance the protection of police officers and guarantee a warning system for railway workers. These intelligent PPE solutions are also furnished with integrated vibrators and audible alarms to ensure that multiple alerts can be generated in case of a dangerous situation. Another PPE damage protection monitoring method has been applied to the light and flexible law enforcement personnel vest. In this approach, a series of conductive cable sensors were applied to the textile substrate to change the resistance to damage by ballistic or sharp attacks.

4.2 Industry 4.0 networked systems in Safety:

In the field of HSE-related SNS, location systems for indoor and outdoor workers play an important role. They allow the detection of worker’s vicinity to high threat areas, typically through GPS, wireless local zone networks, UWB, RFID and image processing systems. Such example of a worker position detection device is a prototype HASARD magnetic sensor system (Signaling of dangerous areas and rangefinder) that detects the presence of a worker in the underground mining machinery operation area. An analogous solution depend on high frequency mobile sensing device has also been employed to improve workplace safety. Alternative example is a device dependent on IoT technology based on integrated WSN and RFID solutions. Supervises the position of workers and controls safe entree to hazardous zone in the place of work where safety tools are required. SNSs were too used to help the application of HSE standards. In this regards, for example, a smart coal mine observing system depend on a Controller Area Network bus and ZigBee technology can be cited to check the coal mine. It allows to determine the location of the miners and the security administrator to generate alerts when unsafe accidents occur, like gas or water leaks. An alike system is employed for mining applications allows the discovery of the precise position and course of fire spread. Following, an independent railroad cautioning system was developed depend on merged particular mobile terminals to locate workers in the workplace, warn them of the proximity of trains and lead them to a harmless area in case of emergency. Other IoT-based SNSs are designed to monitor in real time parameters such as temperature, humidity, air quality, machine vibration, electrical burden and flame exposure in the plant, and to monitor the location and exposure of pollutants from the plant inside air such as formaldehyde and CO2. Another area of SNS implementation is the supervision of safety and work methods in human-robot collaboration booths where conventional technologies, e.g. You can apply light curtains and pressure profound safety mats that detect the presence of a worker in the operating area of a robot. A further progressive example is a system depends on the location of the radio consisting of radio frequency transceivers used in the robot's work area to calculate the operator's location based on the electromagnetic field disturbances and optimize the robot's route. Minimize the likelihood of a dangerous event, it is also worth mentioning the maturity of 3D image fusion for human safety in factory work cells. The systems use the idea of an individual safety area that includes all people and machines. The dimensions and positions of the individual private zones are animatedly reorganized depend on their directions of movement and speeds. An impending impact can be noticed as the sectors overlap, and then the machine's route and / or speed can be changed.

Chapter 5 Implementation of Security 4.0

The security challenge is not like functional security; security mechanisms need to continually adjust to fresh threats. This might be because of random updates as viruses, worms, and Trojans continue to evolve and vulnerabilities may impact production and all its useful components. In order to respond flexibly to the usual threat situation, there must also be a widespread multi-level security strategy that helps protect security applications. This is tracked through a network by which these devices can exchange information with other networks or, for instance, with an enterprise resource planning (ERP) system. The outer layer of the factory, which is protected from the outside world by its own firewall concept, forms the so-called demilitarized zone.

IT security and automation requirements vary widely. Although the privacy of data in the office environment takes precedence, the availability of data in the production area is of great importance, as it is essential for trouble-free production processes. An international standard (IEC 62443) is currently being developed to integrate global security. They are dynamic in the face of cyber-world threats, and security and protection are two separate issues, but closely related. It is important that we establish methods and tools to analyze the impact of vulnerabilities on additional remaining security risks. Ideally, these procedures and tools should be used in the establishment of Cyber Physical Systems (CPS) products: safety through design.

Features to consider include:

- Safeguard interfaces against outside influences such as Internet, corporate network.

- Defense of system communication and machines according to the application methods (continuous operation, remote maintenance, remote diagnostics, special connections).

- Safety is a "mobile target". There is not just one continuous security solution.

5.1 Solution in the subject of security

The question is that how we can defend security applications from cyber threats. The short reply is only possible through a combination of different security measures to which all involved people constantly adhere. To communicate, the technique for victory is defense in the depths. A key element in the construction of medieval castles is the zone and line security model already defined in IEC 62443. It plans to subdivide the automation network into diverse areas where devices can exchange information with one another. Data exchange with devices in another area can only be done over a single line, monitored by a secure router or firewall, to filter the flow of data in accordance with established rules and prevent unauthorized access.

Even if an attacker can invade an area, only the devices in that area are hacked and everyone is safe.

5.2 Automation explanations

To protect automation solutions, IEC 62443, the sequence of IT security standards for industrial automation schemes, describes the seven "necessities" for security.

These automation solutions:

- ID and Verification Check
- Use control
- Data integration
- Data privacy
- Controlled Data Flow
- Timely reply to events
- Availability of resources

Every requisite can be extended to the following components:

- Identify and document.
- User ID
- Multi level verification for untrusted networks
- Software process and device identification.
- Unique identity and authentication.
- Powerful password-based authentication
- Generate passwords and lifetime restrictions for users.

Every component has four levels of security, which can be attained at the expense of developing automation solutions. The system integrator and the plant operator must now determine the appropriate protection levels for the application and the derived region model. The highest security level cannot always be done at level 4, as this requires a lot of work. Even the greatest practical security methods are worthless if they are not applied or worse than if they elude their awareness, because they take a lot of time or because of difficulties in understanding and unfamiliarity. Technical actions should be implemented in conjunction with policies and regulatory actions. What happens to the secure firewall configuration when the password is set to usual value specified in the directory, or if the password-to-device connection is simple. A level of protection for a part of the plant is the result of technical and organizational cooperation.

5.3 Network division

The system should be zoned according to the safety requirements of individual parts of the system. Machines and devices connected inside the zone have identical safety requirements. Technical events should separate individual parts.

5.3.1 Classification of risk dependent security needs allotted to factory and devices

The safety needs should be established on the basis of simple risk assessment approaches. Assets must be selected first. When the security goals have been identified, a threat analysis is performed. The risk analysis then offers facts about the security necessity for systems and components. Setting the security requirements in this way allows the definition of zones, i.e. Network zones with devices with similar needs.

5.3.2 Segmentation of service area

The various production areas of the network (eg ERP, MES or SCADA) are considered in particular by the functions delivered. These functions within the production system should be given special consideration during development. The main concept behind this approach is network sections straightly linked to the device only contain functions with similar security requirements. Functions may comprise, for example, software modules for handling or providing device data, as well as configuration modules that aggregate device functionality according to the configuration file. In the development plan, note that the failure of one area affects as few other areas as possible.

5.3.3 Application of Insulation methods

If the security sectors are associated with the hardware and software parts of the device, they must be appropriately disconnected by technical methods. This create the challenge, when part of the machine is distributed throughout the system. Possible technical methods to separate certain parts include firewalls or data binaries. The key finding of the device is that, as required for protection, it must provide filtering capabilities not only for inbound and outbound connections, but also for communication within the device itself. It is recommended to detect malware or anomalies in the protocol based on network connectivity between specific network segments. These protection techniques are often used directly in firewalls. For vulnerable network segments, data binaries must guarantee that the information flows only in the specified direction. Preferred are solutions in which the separation is attained by switching off devices. To optimize the implementation and adaptation to diodes, all data entering and exiting the machine must be identified. In addition, with VPN solutions, networks can be grouped together in different locations so that similar or identical assets can be managed together despite their distance.

5.3.4 Constant review of insulation methods for the efficiency and patch ability of filter devices

It must be attainable to regularly check the efficiency of practical isolation measures. In the situation of a firewall or further filtering techniques, it might also be essential to regularly examine the filtering procedures. System builders must ensure the updating capability so that the operator can perform this task or provide it as a service. The time among examination solely depends on the device. While low-connectivity devices may be safely configured with comparatively static filtering procedures, filtering procedures for devices with high functional variance and connectivity should often be reviewed and changed. Product changes and conversions / migrations can change the factory protection requirements and require additional network modifications and IP configurations. If weaknesses in the filter devices are detected, make sure that the manufacturer can quickly correct the affected modules

5.3.5 DNS and further facilities for each sector

Due to the significant increase in components that can be able to exchange information in the system, it can be expected that the principal DNS server will be gradually loaded with all system requirements. For this reason, network division should be linked as far as possible to the DNS infrastructure. Due to the often difficult networks and the huge number of network segments, it is recommended to assign multiple segments with alike security requirements for the DNS server. Since both the operator and the integrator must configure DNS, the devices and equipment must provide a suitable function for flexible configuration.

5.4 User accounts, identifications, verification and permission

Not everyone can do something. The production scheme should guarantee the safe management of user accounts and custom credentials (credentials such as passwords, codes, SSH keys, and biometric authentication data).

5.4.1 Distinct user accounts

It must be attainable to create separate user accounts for every entity. Entities means the individuals who interact with the device and other devices and systems that access the facilities remotely and locally. Only then can it be ensured that the player can be assigned the entire computer access. This helps detect attacks and investigate IT security events. It is essential to recall that the operator duty is to validate all device user accounts and allocate them to an accountable person who recognizes the origin and operation of the official account. Distinct user accounts also offer a foundation for issuing rights to persons and roles. In this case, special care should be taken to guarantee that there are no user group accounts: User accounts must be formed for each system user individually rather than allocated roles.

5.4.2 Accounts Handling

The total number of actors may vary greatly relay on the setting in which the device is employed. The top situation when the device is powered by the same set of actors for a long time. The worst case scenario is when actors change a lot or turn on the device for several shifts. The computer must guarantee the effective management of each user account, particularly with respect to adding, activating, changing, deactivating, and deleting accounts. This can regularly be complete through centralized user account management. Therefore, it is suggested that your computer support merging with present identity management systems or integration with user accounts in directory services.

5.4.3 Allocation and handling of authorization

Every distinct user account is connected to the data access, and each player must know this information for verification and approval. The handling of these credentials should be created to permit a safe and effective distribution. Specifically, this means that the procedures for recovering badges in situation of loss meet safety requirements, but must be planned flexibly so that the machine is always ready for operation. This is to avoid crashes due to complex reboot controls. While using passwords, make sure that the default passwords is also altered during reset. Credentials must be established according to the newest standards and approval. To store and store credentials, we recommend using security modules that are protected against physical attacks, such as security. TPM or smart cards. If they are not available, you should at least make sure that your credentials are not saved as plain text but only as salted hashes.

5.4.4 Validate people, software procedures and objects

All users, software processes and parts must be authenticated for each device access based on the specified credentials. After the computer successfully authenticates the trigger, limit access to this session.

5.4.5 Public-Key validation

Authentication must include as few public key encryption operations as possible. In doing so, it is important to safely and effectively manage key management and safe selection of encryption materials dependent on embedded system options. In this case, it is particularly recommended to integrate the device into the present public key structures. It should be noted that the PKI is generally unable to manage the lifecycle of the certificate specified by the operator to avoid system failure due to expired certificates.

5.4.6 Construct sectors and access ideas with equivalent verification

Players must possess authenticated not merely for specific devices but also when overpass the borders of the zone, as described earlier. If the player desires to authenticate with a device that does not fall within its range, authentication must be performed in every zone of the target component. Additionally, you must authenticate for each entree through the interface of each device. When it comes to usability, using certain automation (one-time login by passing tokens like SAML, Kerberos or OAuth 2.0) is suitable and efficient.

5.4.7 The machine should guarantee permission control of the players before each verification

As soon as the player authenticated positively by the device, its allotted rights should be checked immediately. When the allotted rights to the player is not match the rights necessary for access, you must deny access and create a suitable entry in the event log. While the rights are spread through the player account management, the unified user must identify and document certain access rights to components and services. The entree rights to the devices and services must also be editable after the device has been started as the environmental conditions change constantly. To simplify the administration of user rights and the loading of components, it may be helpful to manage them centrally (eg using XACML).

5.4.8 Powerful authorization to outside entities

All the permission to the outside system interface must be ensured through strong verification. When using encryption authentication structures, variables (such as key lengths) must be specified according to the newest standards. For example, many VPN, IPSec and TLS remote access solutions already provide strong verification in safe construction. It must be noted that the components of the manufactured device often have initial service accounts (for example, an administrator with a default password). In case of resilient verification, it also means that such type of account must be adapted to the actual accounts and identities required during computer startup. Encrypted and immutable credentials are not only uncertain, but also require replacement of expensive devices in case of data violation.

5.5 Protected protocols should be used

For attackers who have no direct entree to the device, the starting point of the attack is exchange data with outside devices. Always use the latest generation of secure protocols to ensure the confidentiality, integrity and accuracy of the data transmitted. If possible, already standardized protocols should be used.

5.5.1 Security of data exchange with IP dependent protocols

Applicable security measures can guarantee the confidentiality and integrity of information transmitted to IP dependent protocols for communication among devices in distinct sites. TLS 1.3 and its protocols (such as HTTPS) are particularly recommended. If compatibility with older systems prevents encryption, the connection must be made using a secure protocol. This Recommendation was adopted on the assumption that urgent applications do not communicate over IP-based protocols and that the delay caused by application data encryption is insignificant.

5.5.2 Reliability of data exchanged

Ensure the integrity of the contact data inside and outside the device. The submitted application data must be valid for the device to function properly. Therefore, undetected processing of application data during transmission can have severe consequences for the entire device. Here, too, open standards and joint applications based on the latest technologies, such as TLS 1.3, are available for practical implementation.

5.5.3 Class, durability and excellence of encryption processes

Specified the large number of encrypted algorithms and the wide range of possible applications, it is strongly recommended to use standard encryption methods accepted by the authorities. Suggested public sector activities include guidelines for selecting appropriate parameters (e.g. key lengths). Because of the constantly changing state of emergency, these recommendations are regularly checked by the authorities. When developing your device, make sure you can make appropriate modifications to current devices and systems. Internal studies that are not subject to specialist cryptographic analysis are by no means recommended.

5.5.4 Distinguished application of fieldbus

At least at the bus level, the integrity and integrity of the connection must be guaranteed. Considering the real-time requirements, you must determine whether the data should be encrypted at the fieldbus level and, if possible, depending on the purpose of the resource.

5.6 Protecting wireless technologies

Bridges and airspace. All wireless technologies compatible with the device must be protected according to the latest standards.

5.6.1 Guarded pattern

In addition to the practical requirements (safety), the security requirements of the wireless technology adoption are essential to meet. In a first step, the wireless technologies adoption must be securely configured: identifying the least possible band (signal strength or shielding setting) and the maximum possible immunity to interference. If backward compatibility requires that devices cannot be tightly configured, unsecured communication networks must be tunneled and protected by safe protocols.

5.6.2 Wireless entry management

When accessing via wireless technologies, the attached file must perform reliable authentication and record all interactions in the session. It is recommended to enable the access restriction after the initial configuration, provided that it will not considerably affect the efficient operation of the device. Access limitation can be organized if required. Technical application is possible by filtering MAC addresses. The similar employed to relay stations that can considerably extend the range of the physical signal. In surroundings with special security requirements, consider 802.1x usage and enable it.

5.6.3 Protection of cryptographic activities depends on time

Because wireless networks are very weak and the device is employed for a long time, you should check your security settings frequently. This comprises in particular the encryption functions of the wireless network. If the current attacks affect the cryptographic sentences, parameters or applications used, you should replace them with secure copies immediately. For an overview of presently secure encryption protocols and features, see the appropriate BSI and NIST standards and approvals. If the device used are not well-matched with tougher algorithms due to their partial computational power, the fast transformation of the main material is an alternative.

5.7 Supervision and detection of attacks

It is unrealistic to accept that even with the latest security technology, the computer is completely protected against attack. Therefore, features must be available to detect attacks and other security incidents. If possible, all collected data should be centrally stored to allow further evaluation.

5.7.1 Observation of connections to machine parts

First, all access to the hardware components must be logged and stored for an additional processing. In particular, you must register all traffic from untrusted networks. This should also include component access to services on the device. At least the identity of the player's/device participle and the duration, duration and type of access for later review should be maintained. The control system should be disconnected from the production system. If the trigger is already using the Security Information and Event Monitoring System (SIEM), you should check the system's connectivity.

5.7.2 Merging monitoring activities with the control desk

Access to other safety incident monitoring functions must be integrated directly into the device control station. This means that control stations and other systems that openly supervise the device must be able to register the device itself, which will allow direct analysis in the event of a fault. Security incidents comprise wrong password entry, resource depletion, unauthorized access attempts, and variations to security-related configuration files. Thus, the control center becomes an indispensable element for the collection and processing of safety-related data, therefore, an extra communication load should be taken into account when designing and developing the device, since these complex machines can distribute a wide range, generating high data transfer speed. In addition, it is essential to make sure that none of the recorded incidents contain confidential information such as: Key material.

5.7.3 Virus Scanners

Computers that are directly connected to devices are regularly the malware gateway. Therefore, an antivirus scanner is recommended for this component. Virus scanners detect attacks based on a predefined malicious signature. These rule-based attack detection methods have the benefit of identifying attack patterns called relative reliability. However, the indicator is unsatisfactory when it comes to detecting fresh kinds of malware that do not yet make a signature. To provide basic protection against standard malware, signatures need to be updated on a regular basis. Almost all manufacturers offer the option of selecting adaptive scans to avoid overloading the scans, which affect computer performance. Libraries that are known to be free of malware are excluded from scanning because they are signed.

5.7.4 Network IDS and abnormal detection in structured devices

To discover fresh attack patterns that have not yet been realized, extra actions should be taken to detect anomalies. This method assumes that the device behaves usually and any deviances are detected as an anomaly. Although this approach often leads to false positives in complex networks (for example, in an office network), it is suitable for machine networks whose basic behavior is often more consistent and allows easy configuration. Normal device behavior can be determined by several features, such as B: network connection patterns, user behavior, machine unit activity, sensor data, and system log files. Intrusion monitoring systems (IDS) and intrusion prevention systems (IPS) must be implemented to monitor complex machine networks or operator-approved use. In particular, exposed elements must be equipped with an appropriate function to detect unwanted behavior. It should also be noted that currently available IDS / IPS solutions do not allow inappropriate detection and processing of protocols used in the factory network. Collaboration is urgently needed here to allow malicious packages to be automatically identified at the protocol.

5.8 Recovery plan

Both the device manufacturer and the integrator must establish a recovery plan that will ensure that the equipment will be in a reliable state in the event of a failure or attack.

5.8.1 Making of backup systems

Backup systems are storing systems that can be used to back up all data on devices. Backup systems must be completely merged into the machine design process. It is recommended to perform multiple backups to ensure sufficient data availability and reliability. If you are using central backup servers, your computer must be able to securely exchange data with these servers.

5.8.2 Making of Periodic backups

All data required to operate the device should be stored in backup systems at fixed intervals. The time interval and encryption requirements must be specified by the unified operator or operator depending on the state of emergency and security needs.

5.8.3 Verify that backups are recoverable

All backups must be regularly checked for recovery. Redundancy on backup systems should ensure that backup fails if recovery fails for a backup.

5.8.4 Restore a state of trust after an attack

After the attack, the device must return to a reliable state. Regular backups can restore the device due to a failure. It is also recommended to check the components directly dependent on the device, so that if necessary they can be restored to a reliable condition.

5.8.5 Restore encrypted data

When the device is restored to a reliable state, some information is merely available in encrypted form. Backup systems essentially permit the restoring of encrypted data.

5.9 Establish security requirements for suppliers

Promote and Order What You Want If the delivered components are merged into the factory and do not satisfy safety requirements, this can compromise the machine safety concept. As the weakest tie in the chain, these devices are mostly the gateway to attackers. Identify appropriate rules for third-party secure devices and a secure process for integrating the components offered.

5.9.1 Verify the security condition of supplied devices

The safety needs set by the system manufacturer must be adhered to for each delivered component that is included in the scope of functions. Security needs can be checked by the uniform, the vendor, or both. For projects that are kept strictly confidential, the integrator must perform an audit dependent on the documentation provided by the supplier. If this is not important, the supplier may submit the first conformity assessment in the form of an offer. Make sure that the capacity of the supplied components meets the specific protection requirements. Conformance tests or third-party test results may also be employed for this purpose.

5.9.2 Recognizing your role as a supplier

If the device is integrated as a subcomponent in another product, the manufacturer must document all safety measures for the customer. The documentation should be able to check whether the delivered components satisfy the safety requirements of the target system. The product must be aware of its role as a supplier and correctly identify the organizational processes. This may take the form of a review of the safety needs to ensure proper delivery of the machine, or documentation and disclosure of the protection concept.

5.9.3 Development of outsourced software's

If the software or parts thereof are delivered by third parties, they must participate in a secure programming process. This is especially true for libraries and open source repositories. Set up controls to ensure that your company's security measures are employed in a third-party product and reduce the risk of known vulnerabilities or malicious code. External parts of the system should be contained within the risk assessment to provide you with the necessary information about these parts.

5.10 Documentation

Security measures can be easily implemented unless they are fully documented.

5.10.1 Interfaces

All security-relevant interfaces must be acknowledged and documented. This comprises in particular hardware and software debugging interfaces.

5.10.2 Traditional processes

All administrative and technical processes covered by the documents should be recognized and documented. The regulatory measures and responsible roles must come from the documents. Even a person who does not know this process should be able to determine the steps to take in a particular situation. Recognized processes must be internally documented.

5.10.3 Documentation of risk analysis

The results of the risk analysis must be documented and saved for later use. This is especially true for documented threat models. The documentation should specify how risk analysis and information is based to assess the impact and likelihood of attacks. The risk analysis should only be documented internally because attackers can use the general risk analysis to identify the most dangerous threats. Requirements that result only from security measures and security requirements should be included in external documents.

5.10.4 Distributed rights

The distribution of rights between the players must be documented. It is especially important to record changes in the distribution of rights so that they can later be used for security analysis.

5.10.5 Machine inventory

The manufacturer must create a device user manual that covers all aspects of the device, communication and management (including hardware and software). Ideally, the device should be able to register the currently installed components, including their properties. The component diagram should show the functional relationship between them.

5.10.6 Document management

Define organizational processes for creating, distributing, and sharing documents. Regularly check the relevant documentation for updates.

5.10.7 Security incidents

All safety related incidents must be documented and maintained. This includes incidents in the organization and, if possible, security incidents observed on devices already in use. Security incidents must first be documented internally. If the security incident also involves third parties or the cause of the incident is a threat to the environment, you should prepare a report and send it to interested parties.

5.10.8 Strategy and security controls

The machine safety concept and all safety measures as well as the function of safety measures should be documented. This comprises implementation and configuration, as well as maintenance information. This is the foundation for checking security requirements. Ideally, the manufacturer should provide a guide on device safety.

5.10.9 Organizational processes and roles

All safety-related regulatory processes, as well as those responsible and concerned, should be documented. External contacts should always be documented and explained to external entities.

5.11 Developer training on security

Knowledge is the only alternative to knowledge. Increasing the skills of IT employees in general, in particular IT security, network security and IT functions in production plants is an urgent and necessary task for sustainable development and a better security environment. Requires adding new requirements to selected professional profiles (e.g. through training). Because security approvals prevent you from switching devices as expected (for example, by installing software updates after approval), IT security, such as security, has been improved by Increasing the code quality for all devices installed in the device is of great importance.

Therefore, training should focus on improving experience in developing secure programs. The increased level of security of the device itself and its future operation requires advanced knowledge of network technology, system architecture, protocols and IT standards. The following sections list important information that will facilitate the organization of seminars and seminars already delivered.

5.11.1 Awareness

Any security measure is as strong as the weakest link. Lack of attention, ignorance and neglect can lead to critical loopholes. Every employee must understand that safety is more important and his contribution can have a decisive impact on the quality of plant safety. All supervisors, management, employees and temporary employees should emphasize the importance of their actions and teach them about consistent behavior. General instructions on basic IT security not only protect the resources, the product, but also the entire organization. Only those who know the risk can be quite cautious.

5.11.2 (Software) developers and designers

Designers, programmer's engineers and trained software developers (e.g. IT specialists for application development) should be regularly trained in the importance of code security. To avoid common mistakes and improve the quality of the programming process, it is important to understand popular concepts such as Secure Software Lifecycle (SDL), basic authentication, authorization and session management updates.

5.11.3 Plant planners and project designers

In addition to Development engineers, product planners and managers play an essential role. If they do not recognize what the customer (operator) wants for the gradually complex merging of a new resource into the current production stage, product managers find it difficult to give developers detailed specifications about the features and important features of the resource. This includes requirements for operating systems, network technologies, protocols and interfaces. The main emphasis is on technical issues, but organizational and social parts are equally essential, if not more important. Even with decent training, you can only make progress operationally, as decision-makers and managers support the IT security of your products and solutions. Training on secure software development cycle methods only makes sense if the organization creates technical and regulatory requirements to adapt development and design processes to SDL. This includes making security a coherent design goal and providing employees with time and resources to implement from the very beginning. Politicians should be aware that lasting improvement in security can only be achieved by permanently reorienting the company.

5.11.4 Responsible party for product security

Though most companies do not yet have a Product Safety Specialist, the need for this work is beyond dispute. The PSO must be well grounded in IT infrastructure and ICS / SCADA technology to perform its tasks. In addition, the PSO must process security management to be able to identify and communicate with the security manager (information) and product managers about the security strategy of their products. To achieve this, PSO needs more detailed information on:

- Security analysis and risk management.
- Risk Analysis and assessment.
- Regulations and guidelines
- Vulnerability and incident management.
- Product/factory life cycle
- Channel report and event report.

5.11.5 Training methods

Because the material to be taught is every so often very complex and specific, and the members in the group have very diverse skills, it is hard for standardized training to convey all the content required. Many well-known educational institutions offer introductory courses on IT security in manufacturing and industrial security, which can serve as a foundation. In addition, the more focused security cycle in the world has proved to be a useful introduction to the topic. According to the literature, a slightly adapted introductory course is the most effective option for a small indoor unit. This can serve as the basis for a training plan that meets your business needs.

Conclusion

Obviously, as technologies that drive industry 4.0 evolve dramatically but the industrialist’s actions are not sufficient to pursue safety. Therefore, the risks will increase and some profits are lost in avoiding accidents. Researchers, field and industry experts must work together to implement safety procedures and guidelines to guarantee a plane and safe evolution to this new industrial shift. Today, the world's best companies recognize safety as a key element in the pursuit of operational excellence. The researchers found that these companies could see operational improvements through the use of advanced safety technologies. However, it is also necessary to design new standards or enhance current ones in order to adapt to new realities and improve the use of new technologies. The design and composition of new work surroundings must continue to focus on people, their safety and their comfort. Future HSE integration initiatives should start with virtual task analysis, dynamic occupational risk assessment, cognitive workload analysis, and skills management tools. Sensors should be established to constantly monitor employees and ensure their safety. It is necessary to model human behavior, its intentions and reactions to stress, difficulties and uncertainties. Safeguards against unauthorized access to recorded data and information in the production system should be constantly updated. Security experts can take the necessary remedial action regardless of whether they provide additional training, review standard operating procedures, or update the design of the device. The information itself may indicate potential improvements in procedures or processes and best practices that can be adopted as standard operating procedures.

References:

[1]. Adel Badri, Bryan Boudreau-Trudel, Ahmed Saâdeddine Souissi, Occupational health and safety in the industry 4.0 era: A cause for major concern. Safety Science 109 (2018) 403–411.

[2]. Mattsson, S., Partini, J., Fast-Berglund, A., 2016. Evaluating four devices that present operator emotions in real-time. Procedia CIRP 50, 524–528.

[3]. Gisbert, J.R., Palau, C., Uriarte, M., Prieto, G., Palazón, J.A., Esteve, M., López, O. Correas, J., Lucas Estañ, M.C., Giménez, P., Moyano, A., Collantes, L., Gozálvez, J., Molina, B., Lázaro, O., González, A., 2014. Integrated system for control and monitoring industrial wireless networks for labor risk prevention. J. Netw. Comput. Applicat. 39 (1), 233–252.

[4]. Fabio Gregori, Alessandra Papetti, Monica Pandolfi, Margeherita Peruzzini, Michele Germani. Improving a production site from a social point of view: An IoT infrastructure to monitor workers condition. Procedia CIRP 72 (2018) 886–891

[5]. Fernández, F.B., Pérez, M.Á.S., 2015. Analysis and modeling of new and emerging occupational risks in the context of advanced manufacturing processes. Procedia Eng. 100, 1150–1159.

[6]. Beetz, M., Bartels, G., AlbuSchaffer, A., BalintBenczedi, F., Belder, R., Bebler, D., Haddadin, S., Maldonado, A., Mansfeld, N., Wiedemeyer, T., Weitschat, R., Worch, J. H., 2015. Robotic agents capable of natural and safe physical interaction with human co-workers. In: IEEE International Conference on Intelligent Robots and Systems, art. no. 7354310. pp. 6528–35.

[7]. Yusie Rizal, Computer Simulation of Human-Robot Collaboration in the Context of Industry Revolution 4.0. DOI: http://dx.doi.org/10.5772/intechopen.88335.

[8]. Kuschnerus, D., Bilgic, A., Bruns, F., Musch, T. 2015. A hierarchical domain model for safety-critical cyber physical systems in process automation. In: IEEE International Conference on Industrial Informatics, art. no. 7281773. pp. 430–436.

[9]. Siemieniuch, C.E., Sinclair, M.A., Henshaw, M.J.C., 2015. Global drivers, sustainable manufacturing and systems ergonomics. Appl. Ergon. 51, 104–119.

[10]. Li Da Xu, Eric L. Xu, Ling Li, "Industry 4.0: state of the art and future trends" International Journal of Production Research, 2018 Vol. 56, No. 8, 2941–2962. https://doi.org/10.1080/00207543.2018.1444806

[11]. Kewei Sha, Wei, T Andrew Yang, Zhiwei Wang, Weisong Shi, "On security challenges and open issues in Internet of things". Future Generation Computer Systems 83 (2018) 326-337

[12]. https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf

[13]. Industrie 4.0 safe and smart. White paper http://brochures.pilz.nl/bro_pdf/Industrie%204.0_EN.pdf

[14]. Philipp Gerbert, Markus Lorenz, Michael Rüßmann, Manuela Waldner, Jan Justus, PascalEngel, Michael Harnisch, Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries. https://www.bcg.com/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries.aspx

[15]. https://www.bcg.com/capabilities/operations/embracing-industry-4.0-rediscovering-growth.aspx.

[16]. Securing the future of German manufacturing industry Recommendations for implementing the strategic initiative INDUSTRIE 4.0 Final report of the Industrie 4.0 Working Group April 2013. https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

[17]. K. Carruthers, "Internet of Things and beyond: Cyber-physical systems," *IEEE Internet Things Newslett.*, vol. 10, 2014. [Online]. Available: https://iot.ieee.org/newsletter/may-2016/internet-of-things-and-beyondcyber- physical-systems

[18]. Alberto Carelli, *Student Member, IEEE*, Alessandro Vallero, *Member, IEEE*, and Stefano Di Carlo, *Senior Member, IEEE,* Performance Monitor Counters: Interplay Between Safety and Security in Complex Cyber-Physical Systems, IEEE transactions on device and Materials reliability VOL. 19, NO. 1, MARCH 2019

[19]. Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G., Okrasa, M., 2017. Towards a conceptual framework of OSH risk management in smart working environment based on smart PPE, ambient intelligence and the Internet of Things technologies. Int. J. Occup. Safe. Ergon. 23 (1), 1–20.

[20]. Industrie 4.0 Security Guidelines Recommendations for actions "Leitfaden Industrie 4.0 Security" ISBN 978-3-8163-0689-4 www.i40-security.de

[21]. B. Burchard ; S. Jung ; A. Ullsperger ; W.D. Hartmann Devices, software, their applications and requirements for wearable electronics, ICCE. International Conference on Consumer Electronics (IEEE Cat. No.01CH37182)

[22]. A. Mason, S. Wylie, Olga Korostynska, A. Al-Shamma, Flexible e-textile sensors for real-time health monitoring at microwave frequencies, March 2014, International Journal on Smart Sensing and Intelligent Systems 7(1):31-47, DOI: 10.21307/ijssis-2017-644

[23]. Jason B. Forsyth, Thomas L. Martin, Deborah Young-Corbett, Ed Dorsa, Feasibility of Intelligent Monitoring of Construction Workers for Carbon Monoxide Poisoning, July 2012, IEEE Transactions on Automation Science and Engineering 9(3):505-515, DOI: 10.1109/TASE.2012.2197390

[24]. Dorin Aiteanu, Bernd Hillers, Axel Gerd, Peter, A Step Forward in Manual Welding: Demonstration of Augmented Reality Helmet, Conference: 2003 IEEE / ACM International Symposium on Mixed and Augmented Reality (ISMAR 2003), 7-10 October 2003, Tokyo, Japan

[25]. Ville Myllari, Mikael Skrifvars, Seppo Syrjala, Pentti Jarvella, The effect of melt spinning process parameters on the spin ability of polyetheretherketone, December 2012, Journal of Applied Polymer Science 126(5):1564-1571, DOI: 10.1002/app.36930

[26]. Zemgwei Guo, Bengt Hagstrom, Preparation of Polypropylene/Nanoclay Composite Fibers, October 2013, Polymer Engineering and Science 53(10), DOI: 10.1002/pen.23463

[27]. D. Mrugala, F. Ziegler, Jan Kostelnik, W. Lang, Temperature Sensor Measurement System for Firefighter Gloves, December 2012, Procedia Engineering 47:611-614, DOI: 10.1016/j.proeng.2012.09.221

[28]. Hyunjeong Han, Huiju park, Eunkyung Jeon, User Acceptance of a Light-Emitting Diode Vest for Police Officer, October 2013, DOI: 10.5805/SFTI.2013.15.5.834

[29]. Meike Reiffenrath, Melanie Hoerr, Thomas Gries, Stefan Jockenhoevel, Smart Protective Clothing for Law Enforcement Personnel, April 2015, DOI: 10.7250/mstct.2014.010

[30]. Matteo Petracca, Stefano Bocchino, Andrea Azzara, Paolo Pagano, Marco Ghibaudi, Riccardo Pelliccia, WSN and RFID Integration in the IoT scenario: an Advanced safety System for Industrial

Plants, March 2013, Journal of Communications Software and Systems 9(1):104-113, DOI: 10.24138/jcomss.v9i1.162

[31]. William H. Schiffbauer, Gary L. Mowrey, An Environmentally Robust Proximity Warning System for Hazardous Areas.

[32]. Xiaojun wang, Shushan Hu, Cunchen Tang, Riji Yu, Feng Liu, Intelligent coal mine monitoring system based on the Internet of Things, November 2013, DOI:10.1109/CECNet.2013.6703350, Conference: Consumer Electronics, Communications and Networks (CECNet) 2013, 3rd International Conference

[33]. Boris Malinowsky, Hans Peter Schwefel, Oliver Jung, Quantitative Safety and Security Analysis from a Communication Perspective, December 2015, DOI:10.4108/icst.valuetools.2014.258185, Conference: 8th International Conference on Performance Evaluation Methodologies and Tools

[34]. Eric Rondeau, Stephane Le Calve, Vincent Lecuire, Houssem Eddine Fathallah, Development of an IoT-based System for Real Time Occupational Exposure Monitoring, November 2015, Conference: The Tenth International Conference on Systems and Networks Communications

[35]. Vittorio Rampa, Federico Vicentini, Stefano Savvazi, Matteo Giussani, Marcello Ioppolo, Matteo Giussani, Safe Human-Robot Cooperation through Sensor-less Radio Localization, July 2014, DOI:10.1109/INDIN.2014.6945596, Conference: 12th IEEE Conference on Industrial Informatics (INDIN'14)