Paradigm shift and challenges in IoT security

Ashok Chopra
Associate Professor – Management & Commerce. Program Leader Ph D; MBA (Full Time & Working Professionals).

E-mail: achopra@amityuniversity.ae

Abstract. All Our world is experiencing major technological changes and this time it is centered not on internet but Internet of Things. Actually, Internet of Things is sincere effort to connect all unconnected especially smart objects by doing so human wants to challenge their own way of thinking that shouldn’t all objects be connected to one central network and among themselves so that as human we can control them all. So, paradigm is let us provide capability of objects to exhibit the ability to communicate to each other as well to one central system thus to human beings. This effort would certainly bring new improvements and efficiency in our lives. It is this very premise behind Internet of Things (IoT) that would see new transformation and revolution in industrial world from manufacturing, logistics and supply chain in current industrial world of 4.0 and future newer versions. Over last few decades Information Technology (IT) has been witnessing strong and active cyberattacks and creating protection threats to the cyber security networks. Information Technology industry has learnt lot from these threats and have also documented them to find right and appropriate solutions. In contrast Operational Technology environment surrounding Information Technology were kept in abeyance in many organizations. Thus one hardly finds history and documentation of cyberattacks systems built around operational technology. This also makes fewer learning opportunities and record of catalogued incidents and their corresponding risk mitigation strategy not rich in record. It is worth knowing that the world of operational technology addresses wider scope and higher depth in comparison to Information technology. In Operational Technology the word security and safety are synonymous with each other. It is reality that many of the industrial security standard also incorporate equipment, instruments and safety recommendation by experts thus lay the foundation of IoT security. This paper provides a historical perspective of Operational Technology security, the security system measure, how over a period of last few decades the subject matter has evolved, what are few of the real challenges industry is facing. The final phase of paper focuses on some of the real practical measures and steps have been to taken to in creating more safe and secure industrial environment including best practices in creating synergy between Information Technology networks security and old aged legacy industrial environments. Keywords: Internet of Things Security, Paradigm Shift, Challenges, Operational Technology, Security Systems IoT Security, and Networking Technologies, Protocols “IoT Fundamentals, IoT Evolution.

1. Introduction
The common belief is if at all third world war would break it would be fought in cyberspace. Security and safety has never been more important than it is presently because Internet of Things (IoT) is extending its umbrella coverage not only to network security but is also concerned about security issues. Today’s modern communication systems such as traffic controlling signals which regulate efficient flow of vehicles, to power grid that provide us basic necessity of light/power to Air avionics which makes our aero planes flying in regulated manner, safety and security of network devices, the software
programs, applications and apps are essential to all modern communication. “It is always challenging and complex to provide security and safe to all above and making sure that all these must operate efficiently and effectively with other external forces like defence and continually looking forward to desired outcome” (Sak Brian 2017). In order to further leverage these all one should be able to synergize with traditional technologies and legacy systems where security was hardly major concern. With so many potential security threats and possible cyberattacks an absolute safety is always an issue especially when through IoT we are trying connect possible all unconnected objects.

To better have grasp on present scenario in industrial environment it is the utmost need to understand difference between realities and presumptions. Few areas and disciplines in information technology create more fear, uncertainty and doubt than cyber security. More than any other situations cybersecurity incidents in industrial environment can cause threat and danger to human lives and cause catastrophe to equipment base and the physical environment. It is this physical manifestation and impact of operation technology that attracts the attention of bureaucrats, technocrats and media fraternity that elicits broad-based public concern.

Looking at past hackers and attackers were initially trained and thorough knowledge of Information Technology and systems thus were easily involved in attacking networks and computers. Over a period of time technology and knowledge advanced makers hackers and attackers to make attack easy and simple. To further make situation worse the tools used in attacks and hacking have become easily available. To further compound the situation, it was seen that many of protocols used in IoT were old aged with low security and poor legitimacy thus making hackers and attackers with low technical capability and ability to add to vulnerability of attacking the networks with higher frequency and causing major dent to situation of security. It was always perceived that attackers were offered bigger reward and had better sense of achievement as compared to people involved in defending the network. On the other hand it was found that defenders had better understanding and detailing of their process and systems and were able to buy numbers of devices and tools to defend their systems further adding fuel to fire of more evolving changing methods of carrying out attacks which were increasingly difficult to defend against and respond to. Intruding a smart network of objects through Internet of Things can penetrate deep into web and data of network. This paper is serious attempt to provide insight into best practices which can be deployed and employed in Information & Operational Technology especially in an Internet of Things environment. Paper focuses also on proper and formal analysis today’s an Internet of Things infrastructure deployed in modern industrial environment.

2. Literature Review

Security is always an important issue in every sphere of life. Internet of Things has further concern of security as we are trying to connect all possible unconnected objects. Internet of Things, its architecture and design goals are always challenge in regard to security. Especially security and privacy concealment concerns at different layers in Internet of Things is real challenge. (Kumar Satish J et al 2014)² “Informed and identified, many open issues related to the security and privacy that need to be addressed by research community to secure a trusted platform for the delivery output of future Internet of Things. It was also stressed the applications of IoT in real life needs huge cooperation and inter disciplinary effort. In future, research on the IoT will remain a hot issue. Lot of complex unresolved problems and issues are waiting for researchers to deal and offer secure platform for interconnecting the unconnected objects. The IoT core infrastructure layer consisting of engineering science have started showing maturity signs (Sethi Pallavi et al 2017)³ “However, a lot more needs to happen in the areas of IoT applications and communication technologies. These fields will definitely mature and impact human life in inconceivable ways over the next decade”

Worldwide there is geometric increase and growth in web, mobile and IoT application programs. Previous studies have focused on managing the obtained data. However, managing the heterogeneous resources imagination that get that data is an area that demands more attention. (Samaniego Mayra et al 2016)³ “This work addresses the management of resources in the Internet of Things. This is achieved...
by proposing a virtual-resource edge sharpness layer, which enables access and configuration to constrained physical resources. The computer architecture presented focuses on the use of virtual resources as a management concept and identifies different approaches in the performance valuation on edge computing devices. Using the IoT protocol CoAP, virtual resources are exposed in the edge network. An evaluation of a Go CoAP virtual resource is presented”. (Borgohain Tuhin et al 2019)⁵ “Surveyed all the security flaws existing in the Internet of Things areas, that may prove to be very detrimental in the development and implementation intrusion detection, systems cryptographic and carrying out of IoT in the different fields. So adoption of sound security measures standards and methodology countering the above detailed security flaw as well as implementation of various intrusion signal detection systems cryptographic and stenographic security measuring yard in the information exchange process and using of efficient methods for communication method acting for communicating will result in a more secure and robust in IoT infrastructure. In conclusion, they would like to suggest that more effort on development of secured measure for the existing IoT infrastructure is solicited before going for further development of new implementation methods of IoT in daily life and that would prove to be a more fruitful and systematic method.’ IoT is new disruptive Technology which can revolutionize the current ecosystem of many industries. (Sfar Arbia Riahi et al 2012)⁶ “Most of these challenge result from the inherent vulnerability of IoT object and the tight pairing of the physical world to the virtual world through intelligent objects. This tight fundamental interaction highlights a systemic attribute of IoT security that they proposed to use as a roadmap overview in this work. They then surveyed security related interactions and solutions: Privacy, Trust, Recognition and Access Dominance In improver to highlighting scientific and technological lock they have shed light on the main calibration activity and the open issues”. They showed that the evolution of objects towards greater self-sufficiency intensifies the issues of security and privacy. Finally, we concluded that the liberty of objects to perceive and act on their environment will cause IoT security to move towards greater perceptive and actionable autonomy based on a cognitive and systemic approach. In present scenario data logical-conceptual analysis in IoT has become necessary part of daily life. It, necessitates logical action for knowledge interaction and sharing. Ontology modelling stands out a lot in adding logical-conceptual analysis with the standardized description formats which give great ability to merge and exchange heterogenous information. (Feifei Shi et al 2014)⁷ “The donation of this survey view consists of a superior general description of data logical-conceptual analysis in IoT, including related concepts, general architectures, key techniques, proficiency, applications program and challenges. Techniques Technique involved in data logical-conceptual analysis have been introduced, and it is true that ontology modelling has become the most pervasive technique until now. Every entity, context, user and activity can be modelled through ontologies, with strong expressivity, expansibility and reasoning ability. This work provides a general overview of data, logical-conceptual analysis and makes a comparison between different ontology models and automatic tools.”.

3. Methodology

This is a conceptual paper thus it is always a challenge to have right framework for writing. This paper thus draws major contribution from literature review as part of secondary data. The literature review involved three step approach.

Step 1: Identification of right publications and application of right and practical screening of selected publications. The above ensures that only quality publications are selected and included for review. To achieve above articles of conferences, annotations, operational papers and book review articles were not taken into consideration. In fact aim was to focus on reputed journal publications, and book chapters. Criteria like ranking of journals or any similar criteria was not taken into consideration for applying filters. Indeed publications that cover topic like operational technology and Internet of Things Security may not always be focus of top most journals (because of ever evolving status of the topic). In fact chosen keywords for literature search/review were selected to cover topic like Internet of Things Security, Paradigm Shift, Challenges, Operational Technology, security systems Networking
Technologies, Protocols IoT Fundamentals, IoT Evolution were used. Furthermore, relevant papers had to be included with the term “Security in the title, abstract, introduction, main analysis or keywords to meet the search criteria. Consequent to the above search identified 36 articles considered relevant for the purposes of analysis. The citation information, abstracts, and keywords of all articles were exported to an Excel spreadsheet for further analysis.

Step 2: Involved practically relating theoretical screening benchmarks. Because the focus of the study is on the, only IoT Networking Technologies, IoT Network layers, Smart Objects, Data and Analytics for IoT, Connecting Smart Objects abstract or experimental studies that had Security issues model characteristics as their main focus were retained for further analysis. In particularly and specifically, all abstracts were undergone prudently and the full papers were retrieved of only those that highlighted IoT Network Layer and security aspects of IoT elements. After a second round of elimination and screening, 15 articles were retained.

Step 3: After going through marathon exercise of filtering, analysis of references and in-depth interviews with expert panellist’s fifteen articles met the qualifying criteria which got entered to penultimate round for final detailed analysis. At this stage secondary data also were drawn from cited references. In depth and detailed discussion with area and research experts helped. This step added three additional article/papers for providing much needed information and contribution to existing battery of gathered knowledge. This pragmatic analysis of literature consists of total of eighteen papers/articles. To further explore these articles an open coding content analysis technique was undertaken. When using this technique, notes and headings are written in the text based on their association with the research focus. While leading on reviewing the studies, it was acknowledged that each study can contribute to several different headings.

4. Main Analysis
The first part of analysis gives the historical perspective of Operational Technology Security analysis. It shows how over a period of time operational technology has not only evolved in a particular manner but also faced some common type of challenges

This section explores firstly the historical overview of Operational Technology security as currently deployed in many sectors. Further it focuses on trivial challenges sector faces followed by explaining key differentiators between securing an Information Technology Security versus Operational Technology Security. The final part focuses on how to create secured and elaborated industrial environment including the best professional practices which are deployed in inherited old age legacy systems which are major cause of industrial risk in today’s world. It uncovers the all above in below mentioned sections:
- Short Historical Overview of Operational Technology from Security Perspective
- Main Challenges in Operational Technology Security
- Variation between Information Technology and Operational Technology Security Perspectives
- Risk Analysis Configurations: OCTAVE and FAIR
- Stepwise Approach to Security in an Operational Environment
- Short Historical Overview of Operational Technology from Security Perspective:

The history of hacking is very interesting. It all started with self-skilled and self-learnt information technology individual who in order to have fun started hacking and attacking network. This also caused fear among mass who started losing important data and their work. As the time passed newer programs were written to make attack bigger, deadly and fearful but these were still easier to carry out. As the time passed these tools were made easy to be available and obtainable. As the advancement and effort increased in connecting the unconnected smart object the emphasis was less on security part of connectivity which made initially objects in Internet of Things to be weak in nature. This led to amateur hackers to launch deadly attacks with increased number of attacks without much complication creating overall threat to people involved in manning, managing and protecting the networks. It is always
believed that attackers have advantages in carrying out attacks and people managing network and protecting them lacked knowledge and depth of understanding such attacks. It has been seen many times attackers for sake of fun and immature thinking launched hacking. Slowly came a time for ethical hacking, which added challenge to information technology professional to protect their IT network, which otherwise gave poor attention to protection part of the network. Over a period of time network specialist need to understand fact that attacks would not only be sophisticated but deadly too and defenders have to be proactive, smart and better equipped as compared to what they are today. The graph below shows number of attacks carried from year 2010 to 2015. One would notice that attacks were more than doubled from year 2014 to 2015 challenging security personnel to look to them more seriously. Graphical record of susceptibility revelations in industrial control management is shown in Figure 1.

![Graphical Record of Susceptibility Revelations in Industrial Control Management](https://ics-cert.us-cert.gov).

**Figure 1.** Graphical Record of Susceptibility Revelations in Industrial Control Management: Source [https://ics-cert.us-cert.gov](https://ics-cert.us-cert.gov).

Main Challenges in Operational Technology Security: among the main challenges include Attrition of Network Architecture; Universal Legacy Systems; Modbus; Distributed Network Protocol Three; Inter-Control Centre Communications Apprehensive Operational Protocols Protocol; Object Linking and Embedding for Process Control; International Electro technical Commission Protocols; Various Other Protocols; Device Uncertainty; External Vendors Dependence; Knowledge of Security;

Attrition of Network Design: There are many issues in securing industrial environments. The two most of these issues are Primary and Fundamental design of network and Continuous Maintenance. The basic design issue arose from theoretical belief that networks were originally safe due to physical layer separation of enterprise network with literally no connectivity to the outside world. Industry also had belief that hackers/attackers had low knowledge to carry out attacks. Industry also had belief and notion that they are following well defined industrial best practices (Purdue Model for Control Hierarchy) and standards.

Universal Legacy Systems: There are many systems in Operational Technology which are legacy because of long lifecycle and static/stationary nature/installation. This static nature makes them unsafe from security perspective because of vulnerability of unavailability of updates and patches. “Beyond the endpoints, the communication structure and common central compute, resources are often not built to comply with modern standards.”
Modbus: Modbus has existed in use since 1970s. Governed by Modbus Organization is one the common protocols widely used in industries like power and manufacturing. Modbus has multiple variants e.g. TCP/IP, serial. First of its kind created by PLC (Programmable Logic Controller). Common Security challenges include Authentication of communicating endpoints, it further allows inappropriate source to communicate incorrect commands to the receiver/recipient. The inability to restrict the transmission feature have not been incorporated in some versions.

There is always fear existence for receiver to comply the instruction that was not in particular targeting it. Furthermore, an attack can potentially cause harm/loss to unauthorized receiving device causing inappropriate need to investigate the finer details of the network topology. Figure 2 shows the purdue model for control hierarchy

![Purdue Model for Control Hierarchy](https://businessinsights.bitdefender.com/how-to-manage-the-headache-of-defending)

Distributed Network Protocol: has been is use for serial communication between Intelligent Electronic Devices and controllers like many other supervisory control and data acquisition and industrial control systems practices. Distributed Network Protocol exited and is in use for number of deployment scenarios and across many industries e.g. power, utilities, transmission, medical in both continuous and discrete process modes. There exist both secure and unsecure implemented versions of Distributed Network Protocol Version 3. Though highly dependable delivery of message is paramount but there exists specific weakness from perspective of security. Normally parties involved permit unsolicited responses in case of Distributed Network Protocol Version 3 which may cause non warranted response. The main reason is inability to establish trust in system’s current state thus authenticity may be major cause of catastrophe. This same as to security insufficiency present in Gratis ARP messages as exist in Ethernet switches widely used in various applications. Though in modern Ethernet switches problem has been addressed by dynamic Address Resolution Protocol inspection (DAI) in modern switches.

Inter-Control Centre Communications Protocol: Like many other control protocols, is in heavy use across North America especially in the Utility Sector. Inter-Control Centre Communications
Apprehensive Operational Protocols was from beginning designed to operate and work across a Wide Area Network. Besides this role, initial versions of Inter-Control Center Communications Protocol had major gaps in the area of security. One key susceptibility is that the system did not require confirmation to communicate. Second, encryption across the practice was not enabled as a default condition, thus divulging connections to man-in-the-middle (MITM) and carry on repeated attacks.

Open Platform Communications is based on the Microsoft interoperability methodology Object Linking and Embedding Object Linking and Embedding. This is the classical case of synergy between Information Technology standard (from the domain of Personal Computers) and industrial control network. In such domain Open Platform Communications is normally operates at the higher level control space highly depended on platforms based on Windows OS. The fact remains that many of such devices (based on Windows) are outdated, unsecured and are vulnerable inherent weakness and security issues. The newer versions however have high security built in and also offer newer versions and modes of secure communications across networks.

International Electrotechnical Commission Protocols:
Intelligent Electronic Devices used at Electric Power Sub stations are under the preview of IEC 61850, a standard which defines communication protocol and is part of International Electrotechnical Commission’s technical committee. The objective of IEC 61850 is to permit interoperability between vendors and standardized communication protocols to use this protocol, especially for engineering vendors of power utility systems with weak and poor design.

Initially three message types were introduced and these mainly are: Manufacturing Message Specification, Generic Object-Oriented Substation Event, and Sampled Values. Web Services was later added as fourth service.

- Manufacturing Message Specification, a client/server protocol which operates at layer 3 and leverages TCP/IP.
- Generic Object-Oriented Substation Event, and Sampled Values is operating via multicast over Ethernet and operates at layer 2. It allows Intelligent Electronic Devices to exchange data “horizontally,” between bays and between substations, especially for interlocking, measurement, and tripping signals.
- Sampled Values is a Layered 2 protocol that functions via multicast over Ethernet. It transmits voltage and current samples, typically on the process bus, but it can also flow over the station bus.

The Control and protection along with Primary Process objects in power sub-station are modelled through separate standard logical modes, fall in preview of different groups under different logical devices. These are logically related via LLNO and physical device LPHO to data functions. The reporting schemes are BRCB & URCB responsible for reporting data from Server to client.

Other Protocols: Some important and other of specialized environment protocols have huge importance from the perspective of proper accounting, handling, and understanding of the most basic protocols, transport mechanisms, and foundational elements of any network, including, Address Resolution Protocol, User Datagram Protocol, Transmission Control Protocol, Internet Protocol, and Simple Network Management Protocol.

Some other specialized environments may have other background control protocols also e.g. Internet of Things networks reach all the way to particular and individual sensors, so protocols such as Constrained Application Protocol and Datagram Transport Layer Security are used, and have to be considered separately from a security perspective.

Device Insecurity: Before 2010, security professional paid least or no or least attention to industrial computing, and as a result, Operational Technology systems have not undergone to fierce and rigorous trial as other information Technology systems. Graph below shows how the number of vulnerabilities reported are least in industrial security area as a discipline and subject has been least represented and deliberated at Black Hat Security submit
Figure 3. Showing Revealed Industrial Susceptibilities by Association of Industrial Black Hat Presentations (Source https://ics-cert.us-cert.gov).

Once one looks at empirical sources and history from year 2000 to 2012, to understand insecurity among type and nature of devices, it was found that there were number devices/equipment affected and these were mainly at higher level of operational network, which included control systems, transmission systems along the oil pipelines, or devices installed at critical areas of operations of a plant. It is matter of common sense to understand why such fiascos were there. Among many reasons the most common was ability to easily download software packages which worked against principles of operation security. Other important reason found was generic hardware devices and standard operating systems e.g. Microsoft Windows. Figure 3 shows the revealed industrial susceptibilities. Thirdly IT focused researchers and hackers are well aware the vulnerability of Windows based O/S and devices and the weak areas of such involved components. Attackers had to do very little or nothing to breach the security devices which have been long in service or installation. One such classical example is “Stuxnet, the most famous of the industrial compute-based attacks, was initially successful because it was able to exploit a previously unknown vulnerability in Windows”.

Dependence on External Vendors: Today’s Information Technology dependence on External vendors and cloud is high and very common, however, same is not true for Original Equipment Manufacture Supplier of Information Technology especially Hardware assets as equipment need not to be operated by Hardware Manufacturer. But in the arena of Industrial Security this is very much so, again causing lot of concern on security.

Security Knowledge: Investment in Information Technology part of Industrial Security has been far lower than investment in Industrial Operation’s IT part. The same can be confirmed from data which shows overall Firewall market size of mere of 4% (approx.) in year 2015-16. Another important aspect and challenge in Operational Technology expertise, is comparatively higher ages of workforce, which has low and poor initiative and interest.

- Variation between Information Technology and Operational Technology Security Practices and Systems: The main & important areas in this domain are The Purdue Model for Control Hierarchy, How Operational Technology Network Characteristics Impacting Security.
  The PMC Hierarchy (The Purdue Model for Control):

Irrespective of threats of Security the treatment has to be taken equally, consistently and regularly as Information Technology typically deals with business decision e.g. process optimization on the other the hand Operational Technology focuses on physical decision such variation in pressure or closing and
opening of valve etc. Thus, the operational technology domain must also address and treat the physical safety and environmental factors as part of its security strategy as, this is not normally associated with the Information Technology domain.

From organization perspective Information Technology & Operational Technology tools, methods and teams are separate but need to converge with each other leading through Information Technology way e.g. platforms and systems such as firewalls and intrusion prevention systems that are being used in IoT networks. Since the line of distinction between operational technology and information technology domains not clear and well defined rather is blur must strategize and work more closely with IT together to ensure end-to-end security is the main objective of both. The types of devices that are found in industrial Operational Technology environments are typically much more optimized for tasks and industrial protocol-specific operations than their Information Technology counterparts. Furthermore, the operational profiles also differ to a large extent between Information Technology & Operational Technology.

The Purdue Model for Control Hierarchy, is the respected and widely used as a framework across different industrial environments globally. It is highly in demand in manufacturing, and many other industries.

This model recognizes levels of operations and clearly defines each level. The operational and enterprise areas are separated into different zones and are kept in well-defined in a manner via an industrial demilitarized zone as shown in Figure 4:

- **Top Band consists of Enterprise Band/Zone**
  - Level 5: This Band or Zone contains highest corporate level applications such as, Enterprise Resource Planning System, Customer Relationship Management system, and important services such as Virtual Private Network and Internet Access entering from outside world to enterprise systems.
  - Level 4: Business Planning and Logistics Network: The application at this level typically include planning and optimization systems, scheduling systems, material flow application systems, localized IT Services e.g. intranet, digital telephone network, emailing systems, office applications, monitoring of security and printing etc.
■ Second Band called Industrial Demilitarized Zone
  • DMZ: acts as a buffer zone where, shared services and data can be made safely available. This zone also provides easy segmentation of organizational control systems. As a policy data traffic should not pass through this zone and all important systems pertaining to this zone should originate from and terminate on to this area.

■ Third Band called Operational Zone
  • Level 3: As the name indicates functions belonging to this zone are pertaining to activities like workflow targeted in producing desired end products and services an organization is conceived and meant for. This band also focuses on monitoring and control of entire organization systems and procedures e.g. production control, quality assurance, reliability assurance, optimization of system wide control, management of security and network and possibly other required IT services such as Domain Name System, Dynamic Host Configuration Protocol and timings.
  • Level 2: Supervisory control: Supervisory Control consist of zonal control rooms, status of controllers, control system network/administration of applications, and other application oriented controllers, e.g. human-machine interface.
  • Level 1: Basic control: controllers at this level include an Intelligent Electronic Devices (a sensor), actuator, or PLC, dedicated Human Machine Interfaces, and other applications may talk to each other to run part or all may belong to the control function.
  • Level 0: Process: at this basic level devices such as sensors, actuators and machines such as drives, motors, robots and other elements communicate with controllers or with Intelligent Electronic Devices.

■ Fourth Band Called Safety Zone
  • Safety-critical zone: devices, sensors, and other equipment used at this level are used to manage the safety functions of the control systems of an organization. From the security perspective, PMC (Purdue Model Concepts) permits right placement of security among various level e.g. Information Technology networks typically reside at Top Band consisting of Levels 4 and 5 and uses security principles common to Information Technology networks. The lower levels are where the industrial systems & Internet of Things networks are stationed. As shown in the diagram, an Industrial Demilitarized Zone resides between the Information Technology and Operations Technology levels. Without an iota of doubt for protecting the industrial layer at primary level security experts should deploy strong firewalls, local proxy servers and IPSs, so that only recognized, trusted and authorized connections from reliable sources can be ported to the right authentic ports. At the Industrial Demilitarized Zone, necessarily, and even at among the lower levels, industrial firewalls ready with capability of understanding the control protocols must be deployed to ensure uninterrupted and smooth functioning of Operation’s Technology Network. The graph shown below clearly depicts vulnerabilities associated with industrial security between 2011 -12 for the higher level of equipment assets more susceptible and vulnerable to security threats. This shows how strong is logic followed in PMC model which has been depicted in Figure 5.

Security Priorities: Integrity, Availability, and Confidentiality
Priorities in both Information Technology and Operational Technology are totally diverse. In the domain of Information Technology target areas for attack by hackers and attackers are information itself (the most vital), however, in an operational Technology arena the most crucial assets are participating equipment, processes, workers, many of fixed assets etc. Thus, there is diverge security priority difference between two domains.
Figure 5. (ISR) Industrial Security Report of Published Susceptibility Areas for year 2012
(Source: https://ics-cert.us-cert.gov).

The world of Information Technology is dominated and influenced by regulatory, commercial and legal frameworks/obligations to protect data and take care of information of those individual who may or may not be part and directly employed by organization. Thus primary focus and emphasis is on integrity, confidentiality on data available rather than on physical assets, and equipment. There is hardly any repercussion of losing a device. In comparison in a Technology Domain

At this stage information loss in Information Technology is considered more damaging than losing a computer device, because many important functions such as access and permissions may part of information. On the contrary in Operational Technology domain loss of device because of exposure and susceptibility may cause loss of production days which has more importance and relevance in production based industry.

OCTAVE
The philosophy of OCTAVE which has undergone number of revisions through tested trials based on fundamental assumption that having a robust standby team may be like a luxury which may not be always available and at disposal of the organization to carry out a comprehensive security drill and review. Because of this Allegro is less burdensome and lightweight in implementation. The steps involved in Allegro are divided in four stages and are:
Stage 1 Establishing Drivers consisting of Establishing Risk Measuring Criteria,
Stage 2 Profiling of Assets consisting of Developing Information Profile of the asset, Identification of Containers of Information Assets, Identification of Areas of Main Concern,
Stage 3 Identification of Threats consisting of Identification of Threat Scenarios,
Stage 4 Identification & Mitigation of Risk consisting of Identification of Risk, Analysis of Risk, and Carrying on Mitigation of Approach.
Figure 6. (Source https://blog.compass-security.com/ 2013/04/lean-risk-assessment-based-on-octave-allegro/)

Operationally Critical Threat, Asset and Vulnerability Evaluation is highly information focused and balanced process. OCTAVE offers unrestricted range of breadth in regard to discipline and offer superb counterbalance in terms of specificity of Security which is shown in Figure 6.

FAIR on the other hand focuses measuring part of idea, defining and other inter related attributes of risk. SMART metrics are the focus areas of FAIR which itself provide rich insight into operational part of data. The definition of FAIR also includes probability of frequency, and loss magnitude assessment. It also provides details of emergence of sub elements hierarchy along with magnitude of loss an organization can have.

Above is result of a particular known frequency known as Threat Event Frequency, in this a particular time window becomes a probability.

Phased Application of Security in an Operational Environment:
Security Experts and Practitioners entrusted with job of securing workplaces should make sure that they duly secure and provide adequate safety in the work and industrial environment. However same is not true for technicians of Operational Technology sector, as they are entrusted with job of protecting the valuable and life supporting environment of production or services offered by an enterprise.

Secured Network Infrastructure and Assets: International Electrotechnical Commission

As security expert one has to analyse and secure the basic network design. Because in majority of industrial environment like categorized energy distribution network of systems or in an integrated system of processes there always exist highest level of correlation among operation designs and network design. It is fundamental principle of Industrial Automation and Control System 99 and International Electrotechnical Commission 62443 that various functions should be divided in zone and cells and utmost security needs to be provided where ever communication is crossing the borders and boundaries of zones and cells through conduits. It is advised that security professional involved should mark and
make note of network of communication channels in a proper manner as shown in Figure 7. If proper care is provided leakage of security incidents can be prevented.

![Diagram of network zones and levels]

**Figure 7.** Status of Security among Zones & Levels in the Process Control Hierarchy Model

In State of The Art and sophisticated environment, where exists modern communication and network devices with perfect protocols and communication channels proper access control should be deployed having better and secured communication capabilities. It is advised that security professional provide clear ingress/egress points for each demarked zones

*Deploying Dedicated Security Appliances:*

Proper planned deployed network can provide bird’s eye view of connection history and line and direction of data flow. Personnel involved can get clear understanding of packet on the network. Such clear visibility can be achieved with Deep Packet Inspection technologies e.g. intrusion detection and prevention system. Such technologies have the capability of detecting various kinds of traffic of interest rather than assessing through application where one can be misled as to whether communications are being obfuscated, to whether exploits are targeting vulnerabilities, to passively identifying assets on the network.

*Policy Convergence and Network Monitoring:*

From security perspective convergence of the Information Technology and Operation Technology spaces is merging, or at least there is active coordination across formerly distinct Information Technology and Operations Technology boundaries. It is clearly found that latest networking and computing technologies entering in operational technology domain are going to be having higher maturity in Information Technology space.

5. Conclusion

Industries and mankind in pursuit of better living and modernization would keep working towards better, improved and efficient, agile and modern systems. This would in turn would keep putting pressure on security personnel in terms of connectivity of old generation systems and operational Technology assets. Thus, as default security must be applied across the board and throughout the life cycle of a product and process. And to achieve security organization and security personnel involved must make informed choices to able to best address issues.

In order to minimize and manage risk threats much is already available. Connectivity across networks can be made secured by application of right policies and correct selection of equipment. Security
appliances and right practices can further help to identify threats, attacks and unsafe practices. As the time passes reduction of risk is possible through mutual cooperation and convergence. Mankind need to learn more from mature security practices, tools and techniques available in Information Technology and through well – coordinated layers to protect critical assets deployed in industries from operational environment. By following right policies, practices devices and equipment we can strive towards better operational Technology world.

6. References:

[1] Brian Sak Technical Solutions Architect at Cisco Systems https://www.linkedin.com/in/briansak/
[2] J. Sathish Kumar, Dhiren R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014.
[3] Pallavi Sethi and Smruti R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, Hindawi Publishing Corporation Journal of Electrical and Computer Engineering Volume 2017, Article ID 9324035, 25 pages.
[4] Mayra Samaniego, Ralph Deters, “Management and Internet of Things”, The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016), Vol-94 (2016) pp137 – 143.
[5] Tuhin Borgohain, Uday Kumar, Sugata Sanyal, “Survey of Security and Privacy Issues of Internet of Things”, pp 1-6.
[6] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challalce, Zied Chtourou, “A roadmap for security challenges in the Internet of Things”, Elseveir, Digital Communications and Networks (2017).
[7] Feifei Shi, Qingjuan Li, Tao Zhu and Huansheng Ning, “A Survey of Data Semantization in Internet of Things”, Sensors 2018, 18, 313; doi:10.3390/s18010313, www.mdpi.com/journal/sensors.