International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Security Measures in SCADA Systems

Steffi Paul Kalib[1], Manoj K. Rawat[2]

[1]Lakshmi Narain College of Technology, Indore, Madhya Pradesh, India

[2]Lakshmi Narain College of Technology, Indore, Madhya Pradesh, India

Abstract: ***In the past few years the security issues in the supervisory control and data acquisition (SCADA) system have been widely investigated, and many security mechanisms have been proposed from research communities. The international standard organizations also have published several standard documents for secured SCADA systems. In this paper, we overview the SCADA system architecture and consider the constraints due to the system's own characteristics. And then, we explain the technological challenges for the SCADA security and summarize the current results which have been brought out by the efforts from the international bodies as well as research communities.***

Keywords: SCADA, Industrial control system, Network security, Digital forensics.

1. Introduction

The main purpose of the supervisory control and data acquisition (SCADA) system is gathering real-time data, monitoring and controlling equipment and processes in the critical infrastructure. A SCADA network provides connection between servers which reside inside a control center and control devices which are located at fields, sometimes at remote locations.

Major concern about cyber-attack stems from the notion that the SCADA network is no longer an isolated network which prohibits outsiders from entering the network, nor is the specialized network based on private platforms and protocols, allowing only technical staffs with special knowledge to access to the resources. The reasons of claiming that the SCADA network is not a protected closed network is twofold. First, the communication architecture is more relying on the open standard communication protocols. The use of the open communication protocols renders the system more vulnerable to cyber-attacks in many applications. Second, the SCADA network is moving toward being connected to corporate networks for convenience and other business reasons. Thus the SCADA network may open its doors to outsiders who can enter the corporate networks maliciously.

2. SCADA System Architecture

SCADA systems mainly perform monitoring of real-time data and controlling by automated or operator driven commands to field devices. This task of monitoring and controlling is done by the integration of embedded systems which is expected to grow 500€ Bn in 2020[1]. They form backbone of the critical national infrastructures such as electric utility, water utilities, oil and gas production, oil and gas supply, telecommunication and manufacturing. They also find applications in experimental physics laboratories for the monitoring and control of auxiliary systems such as power supply, cooling, radiation monitoring etc. the size of the plant may vary from few 1000 to 1Million input/output (I/O) channels. As number of I/O channels increases the requirement for high performance monitoring and controlling of data points and there management also increases.

Current SCADA system architectures were designed for more closed and controlled industrial environments, however it is expected that there is potential to enhance their functionality and minimize integration costs by integrating into collaborative approaches with enterprise systems and large-scale real-world services. As environments become more complex, it is not anymore viable (e.g. cost- /time-wise) to engineer individual self contained systems but rather integrate large-scale Systems of Systems (SOS). We need to consider what the next steps could be towards engineering/ designing the next generation of SCADA/DCS systems of systems that could successfully tackle the emerging challenges such as degree of centralization, optional independence of each of the participating systems, and independent evolution of them [2] [3].

SCADA systems have historically been isolated from other computing resources. However, the uses of TCP/IP as a carrier protocol and the trend to interconnect SCADA systems with enterprise networks introduce serious security threats.

The primary functions of SCADA systems are as under:-

1. The supervisory control and data acquisition (SCADA) system is generally considered a necessary part of monitoring and control for large processes, including oil and gas production, paper manufacturing, and power generation. The system often consists of hardware architecture and a software package.
2. Supervisory control and data acquisition (SCADA) systems are used to monitor and control industrial processes and infrastructure in manufacturing plants. SCADA helps to gather information about different equipment's across various industrial processes such as manufacturing, transportation, power generation, refining, and desalination in both discrete and process manufacturing industries.
3. Modern industrial facilities have command and control systems. These industrial command and control systems

are commonly called supervisory control and data acquisition (SCADA).

4. SCADA systems at their fundamental level are Industrial Control Systems. They are computer based control systems that monitor and control industrial processes that exist in the physical world.
5. They're your first line of defense against infrastructure failure.
6. SCADA systems provide monitoring, control, and automation functions that allow the enterprise to improve operational reliability, reduce costs through eased work force requirements, enhance overall Quality of Service (QoS), or meet expected QoS or other key performance factors as well as boost employee and customer safety.
7. SCADA systems are widely used in industry for Supervisory Control and Data Acquisition of industrial processes.
8. The utilization of Supervisory Control and Data Acquisition (SCADA) systems facilities the management with remote access to real-time data and the channel to issue automated or operator-driven supervisory commands to remote station control devices, or field devices. They are the underlying control system of most critical national infrastructures including power, energy, water, transportation and telecommunication. They are widely involved in the constitutions of vital enterprises such as pipelines, manufacturing plants and building climate control.

Two main components of the SCADA system are master stations and remote terminal units (RTUs)[1]. The master station, located in a control center, monitors and controls a large number of RTUs which are field devices located in physical environments. RTUs, which are microprocessors, gather data from sensors which measure current and voltage and send data to the master station. The actuator as a part of RTU controls the operation of physical equipment by commands from the master station. The master stations have a hierarchical structure. A high-level master station can control several sub-master stations. The data and command transfer between the master station and RTUs are carried over SCADA networks. The SCADA network is based on various communication channels and network technologies including Ethernet, serial links, wireless communication, and so on.

Recent trend is that the SCADA network is connected to the corporate network in order to manage the field data efficiently. Sometimes a remote access is allowed to the field devices from the outside of the SCADA network over the dedicated communication links. The communication between the master station and RTUs is governed by the standard communication protocols. The most commonly used protocols are IEC 60870-5, DNP3 which is the derivative of IEC 60870-5, and Modbus. While the IEC protocol is widely used in Europe, DNP3 is dominant in the North America, and Asia. Recently the International Electro technical Commission (IEC) is working on the new protocol, IEC 61850, which can provide more enhanced functionalities.

From a viewpoint of network security [2] the key interest is the contact points by which intruders can access to the SCADA network. The main door to the outside is the gateway by which the SCADA network is connected to the cooperate network. In all networks firewalls are installed to enforce secure accesses from the outside. In many cases the direct remote access to RTUs from the outside is allowed for remote monitoring and gathering information. These contact points should be as few as possible and be supervised under scrutiny.

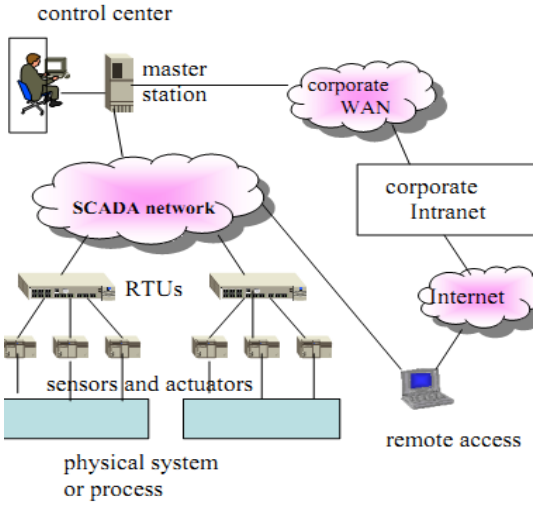

Figure 1: SCADA System Overview

3. Security Threats and Vulnerabilities

When SCADA protocols were first developed, the goal was to provide good performance and the emphasis was placed on providing features that would ensure that the task constraints on the network would be met. Far from being a design requirement, network security was hardly even a concern.

Until recently, the most common misconception regarding the security of SCADA networks was that these networks were electronically isolated from all other networks and hence attackers could not access them. Industrial plants focused much of their efforts at increasing physical security. The growing demands of the industry for increased connectivity between the factory floor and the corporate network have altered the simple, isolated control network into a member of a complex inter-network. This increased interconnectivity of networks has also raised concerns about the security of these SCADA networks. It is important to realize that with current networking technology there can be multiple access points to any network, including SCADA networks, and physical isolation does not guarantee network security.

Over the years, the automation industry has also moved away from proprietary standards for SCADA communication protocols towards open international standards. Therefore, the previously held belief that it was difficult for attackers to gain access to information about SCADA networks is no longer true. The open standards make it very easy for attackers to gain in-depth knowledge about the working of these SCADA networks.

Another factor contributing to the lack of security of SCADA networks is the use of COTS hardware and software to develop devices for operating in the SCADA network. COTS-based design can save cost and reduce design time, but it also raises concerns about the overall security of the end product (The Center for SCADA Security). COTS software is often not very secure, and this software offers a tempting target for attack. Devices that are meant to operate in safety-critical environments are usually designed to fail-safe, but security vulnerabilities could be exploited by an attacker to disable the fail-safe mechanisms. Therefore, these devices must not only be designed for safety but also for security.

Furthermore, the inclination to use COTS equipment has led to the development of a number of SCADA protocols that can operate on traditional Ethernet networks and the TCP/IP stack. These protocols are often established serial-line based protocols encapsulated through some standard process prior to being placed in a TCP packet. Many of these protocols abandon any strict master/slave relationships traditionally seen in SCADA networks, and devices designed for these networks often provide additional application-layer interfaces beyond the SCADA messaging protocol. These can include web-inter-face capability which, when coupled with the integration to the corporate network, allows for convenient gathering of production information for higher-level management [3]. Of course, inclusion of these services makes any devices on the SCADA network supporting them vulnerable to popular application-layer and TCP/IP-based attacks. Recent surveys show that the number of attacks against SCADA networks has been escalating steadily over the years.

To get an accurate picture of the threats to industrial net-works, the British Columbia Institute of Technology in Canada created a database of SCADA security incidents. The database was populated with entries of attacks against industrial net-works, and an analysis of the database shows some disturbing trends. Prior to the year 2000, almost 70% of the reported incidents were either due to accidents or due to disgruntled in-siders acting maliciously. Since 2001, apart from an increase in the total number of reported incidents, the report also shows that almost 70% of the incidents were due to attacks originating from outside the SCADA network. An attacker who gains unauthorized access to the SCADA network has the potential to carry out a range of attacks against the network. These attacks can cause significant financial losses due to loss of production capabilities. In extreme cases such attacks might also lead to loss of life. Many possible attacks are described in the literature.

Attackers aim to compromise the SCADA networks' security properties such as integrity, confidentiality, authentication, or availability. Sniffing the data transmitted across the network is an example of an attacker trying to gain access to confidential information. Since many of the SCADA protocols do not support any kind of cryptography, sniffing communications on the network is possible if the attacker succeeds in intruding into the network. An attacker could learn all the data and control commands while listening to the traffic and could use these commands later to send false messages. An attacker can also tamper with the data transmitted over the network and thereby compromise its integrity [4]. For example, the attacker can change control signals to cause a device malfunction which might ultimately affect the availability of the network. An attacker might gain unauthenticated access to de-vices and change their data set points. This can cause devices to fail at a very low threshold value or an alarm to not go off when it should. Another possibility is that the attacker, after gaining unauthenticated access, could change the operator display values so that when an alarm actually goes off, the human operator is unaware of it. This could delay the human response to an emergency which might adversely affect the safety of people in the vicinity of the plant. It is also possible to block or reroute communications to cause significant denial-of-service attacks [5]. Since many devices [5] do not have secure operating systems, attackers could attempt to plant malicious code, which could either give them greater network access or it could cause some other damage to the network.

4. Forensics for SCADA systems

Digital Forensics[6] is an essential part of cyber defense and becomes relevant when there is a security breach . It can generally be defined as the collection and analysis of data from different relevant sources (such as storage devices and network streams) in a manner that is admissible to a court of law. It is performed on digital devices and usually used to investigate the cause and consequence of an incident where if the traces of a crime such as unauthorized network access or theft of a digital file are found, it may further lead to the admissibility of evidence to a court. However, not all the application of digital forensics necessarily involves presenting the data or evidence in a court of law. For instance, digital forensics is also used for internal corporate investigation to find the cause of an incident in order to limit the possibility of the incident occurring again in the future.

From a forensic perspective[7], a SCADA system can be viewed in different layers (as illustrated in Figure 2 as an example) based on the connectivity of the various SCADA components and their network connectivity with other networks such as the Internet. In Figure 2, layer 0, which is the lowest layer, contains the individual field devices connected via a bus network. Layer 1 has controllers that receive input signals from the field devices and other controllers upon which they perform operations to steer the individual field devices, by sending output signals to them. Layer 2 consists of the supervisory network - typically a local network connected to the lower layers for specific operations such as showing current monitoring state at the HMI. Layer 3 is typically the operation DMZ, in which historians, domain controllers and application servers are located. The upper layers correspond to the enterprise IT networks, in which the regular enterprise desktops and business servers operate. Most of the forensic analysis in SCADA systems involves the first three layers (i.e. layers 0, 1 and 2) as they contain the special SCADA components and are crucial for controlling the underlying industrial processes. However, the analysis may further extend to the other, higher layers (i.e. layers 3, 4 and 5) if needed [8].

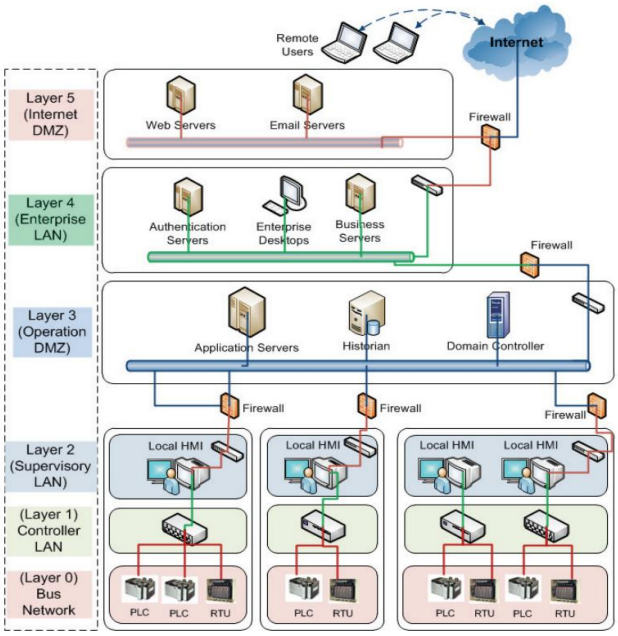

Figure 2: Layers of A SCADA System

5. Communication Systems Operated in Sparsely Populated Area

Many electric power stations are located in sparsely populated areas, where the coverage of telecommunication networks could be poor. In order to send information from a rural area to post processing, there are many different data transfer network systems. From fixed connections to commercial Mobile Networks, satellite communication and Terrestrial Trunked Radio (TETRA) Networks are used to transfer data from sparsely populated areas. GSM intially designed as a pan-European mobile communication network, not shortly after the successful start of the first commercial networks in Europe, GSM systems were also deployed on other continents. In addition to GSM networks that operate in the 900 MHz frequency band, others so-called Personal Communications Networks (PCNs) and Personal Communication Systems (PCSs) are in operation. They use frequencies around 1800 Mhz, or around 1900 MHz in North America [9].

General Package Radio Service (GPRS) is enabling improved data rate performance by allowing for more that one GSM time slot to be used by a terminal for a service at a time. The driving factor for new (and higher bandwidth) data service obviously is wireless access to the Internet [10].The third-Generation (3G) mobile communication networks known as the Universal Mobile Telecommunication System (UMTS) in Europe and as the international Mobile Telecommunication System 2000 (IMT2000) worldwide, have already been introduced [11]. The second-generation (2G) mobile system uses digital radio transmission for traffic. The 2G networks have much higher capacity than the first-generation systems. There are four main standards for 2G systems: Global Systems for Mobile (GSM) communication and it's derivatives; digital AMPS (D-AMPS); code-division multiple access (CDMA) IS-95; and personal digital cellular (PDC) [12]. The 2G networks are close to their end of life cycle.

The Third-Generation Partnership Project (3GPP) is the standard-developing body that specifies the 3G UTRA and GSM systems. 3GPP is a partnership project formed by the standard bodies ETSI, ARIB, TTC, TTA, CCSA and ATIS 3GPP consists of several Technical Specifications Groups (TSGs). The 3GPP Long-Term Evolution is intended to be a mobile communication system that can take the telecom industry in to the 2020s. The philosophy behind LTE standardization is that the competence of 3GPP in specifying mobile communication systems in general and radio interfaces in particular shall be used, but the result shall not be restricted by previous work in 3GPP. Thus, LTE technology does not need to backward compatible with older WCDMA and HSPA technologies [13]. TETRA is an open digital radio standard for professional mobile radio. TETRA can be used by a company for the communication with the mobile work forces (Private Mobile Radio; PMR) as well as by an operator to offer the same services on a commercial basis (Public Access Mobile Radio; PAMR).

A third group of users are the Emergency Services (such as police and fire departments). The TETRA radio standard is defined by ETSI European Telecommunications Standards Institute. TETRA is based on radio channels with a bandwidth of 25 kHz. Each channel is subdivided in 4 traffic channels using Time Division Multiple Access TDMA. The traffic channels can be used for both voice and data. The maximum bit rate is 28.8 kbps if all 4 traffic channels are joined together for one data connection [14]. Identifying the elements on which a comparison of the requirements with its special features of the evolving standards and the improvement that are possible for TETRA, that TETRA can play a major role in the next generations of Private Wireless System PMR systems. TETRA system can be improved to become a unique tool for security [15]. Private Wireless System can extend to cover mobile video, voice and data transmission simultaneous as low as 640 kpps data [16]. Average TETRA cells are remarkably larger than GSM cells. Firstly, TETRA uses typically a frequency of 400MHz, while GSM uses 900 or 1800MHz. The propagation losses are theoretically proportional to the square of the frequency Secondly, commercial networks are typically capacity driven and PSS networks with less users are coverage driven. This means that population density usually determines cell size in GSM [17].

The TETRA system uses end-to-end encryption in addition to the air interface encryption to provide enhanced security. End-to-end encrypted continuous data, such as video, requires synchronization of the key stream at the receiver to the incoming encrypted data stream from the transmitter. Apart from the video coding synchronization mechanisms (e.g.MPEG-4, H.263), the TETRA system uses a synchronization technique known as frame stealing to providing synchronization to end-to-end encrypted data [17]. A satellite is often referred to as an "orbit radio star" for reasons that can be easily appreciated. These so-called orbiting radio stars assist ships and aircraft to navigate safely in all weather conditions. The satellite-based global positioning system (GPS) is used as an aid to navigate safely and securely in unknown territories [17].

A satellite in general is any natural or artificial body moving around a celestial body such as planets and stars. In the present context, reference is made only to artificial satellites orbiting the planet Earth. These satellites are put into the desired orbit and have payloads depending upon the intended application [18]. A satellite while in the orbit performs its designated role throughout its lifetime. A communication satellite is a kind of repeater station that receives signals from ground, processes them and then retransmits them back to Earth. An Earth observation satellite is a photographer that takes pictures of regions of interest during its periodic motion.

6. Distributed Systems Interconnection Protocol(DSIP)

Distributed Systems intercommunication Protocol (DSiP) system allows for combining all kinds of telecommunication resources into a single, uniform and maintainable system.

The Next Generation Network (NGN) enables users seamlessly access heterogeneous networks (including ad hoc networks) for reaching a common IP-based core network. Some critical issues are to be faced in order to allow data sharing among different networks, related to items such as Access Control and Command and Control. Intense research activity on this topic has been promoted in recent years , and network level solutions have been suggested. The DSiP solution makes communication reliable and unbreakable. DSiP uses several physical communication methods in parallel. Applications, equipment and devices think that they communicate over a single unbreakable data channel. Satellite, TETRA, 2G, 3G, 4G/LTE, VHF-radios etc. can be used simultaneously in parallel. DSiP is suitable for a vast range of applications. Power Grid Control, SCADA and Public Safety communication are examples. The DSiP solution brings several benefits to communications. For example better data security, integrity & priority. Immunity towards virus infusion and DoS network attacks with intrusion detection. For communications there are data-flow handshaking and flow-control systems implemented with automatic re-routing. Early detection of communication problems helps minimizing communication disruptions because the change of the communication channel can occur earlier.

Other benefits include: authentication- and management tools, controllable data casting and compression, interfacing capabilities to equipment and software. For communications DSiP offers: transparent tunneling of any data, cost-efficient network topology, insulation from Internet-system flaws and routing according to lowest cost and/or shortest hops. Critical networks and communication solutions require efficient management and monitoring tools. The DSiP solution contains several modules for support, maintenance and configuration.

Authentication Server Software: The DSiP features centralized and mirror able Authentication Server software. This software allows for editing passwords for DSiP nodes. The nodes may have passwords that expire after a specific time for security reasons. Nodes may be allowed in the DSiP routing system and they may be excluded from it at any given time.

Configuration Server Software: The Configuration Server software is an entity for providing routing instructions and firmware updates to nodes. Nodes may be instructed to contact the Configuration Server at any time. Network Management Server Software: The Network Management Server software constantly monitors the connections in the DSiP system. A graphical tool called DSiP View enables the user to get a visual feedback over the current network function. Nodes marked green are OK, yellow indicates anomalies in the functionality and red errors. Users may select a node and query its status. DSiP-Graph is a browser tool presenting graphs over node latencies, transferred data mounts etc.

7. TCP Protocol Challenges in Fluctuating Networks

TCP protocol has problems with congestion protocol when switching to different network using other techniques at the network layer. When delay or speed of the network link changes in a situation like switching from 2G to LTE network, the TCP protocol requires relatively long time to adjust to the new network environment. Normally this would not harm SCADA connections but live video stream might suffer from this. The inefficacy of TCP protocol to adjust can be mitigated by implementing changes to the TCP stack of the sender. There is no need to implement any new software or hardware to the routers and other network communications devices. Also the receiver does not require being aware of the changes to the TCP sender side. General TCP algorithms for vertical handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in which the receiver reports to the sender that duplicate segment has been received. TCP-Eifel detection algorithm uses TCP timestamps option to detect spurious retransmissions. The Eifel detection provides a faster detection of spurious Retransmission Timers (RTO) compared to DSACK. Forward RTO-Recovery is a TCP sender-only algorithm that helps to detect spurious RTOs. It doesn't require any TCP options to operate. TCP congestion control algorithms have been designed to enable TCP to adapt to the fluctuating bandwidth available on its end-to-end path. TCP connection remains fairly stable over the lifetime of a connection. Mobile node can easily obtain information regarding the occurrence of a vertical handoff and the status of the wireless link: IEEE 802.21 standard can provide event notifications such as link-up or link quality is degrading.

Proposed enhancements are implemented in the TCP SACK algorithm and they are invoked when a cross-layer notification arrives from the mobile node to the TCP sender. This information contains occurrence of a handoff and rough estimate of the bandwidth and delay of the old and the new access links. Algorithms are incremental in nature and are also conservative it the sense that they are designed not be counterproductive in any situation.

Experiments conducted in Linux kernel version 2.6.18 show that performance of the proposed algorithms is quite close to the results obtained in the simulation experiments. In the absence of the cross-layer information, the proposed enhancements don‟t affect the normal behavior of the TCP algorithm [18]. Intermittently Connected Networks (ICN) introduces a new problem. How to control TCP traffic flow with networks that are connected to each other only intermittently? Delays can be extremely long and when the connection is made, transfer rate could be high. This creates a challenge for currently used TCP congestion protocols.

Communication protocols for intermittently connected networks must start with an algorithm with very few assumptions about the underlying network structure. The traditional back-pressure algorithm is impractical in intermittently connected networks, even though it is throughput optimal. The back-pressure algorithm is reasonable starting point for developing new protocols for intermittently connected networks. A modified back-pressure routing algorithm that can separate the two time scales of ICNs is presented in Jung Ryu‟s study, this algorithm improves performance. On top of this algorithm is a rate control protocol implemented on TCP protocol [19].

8. Considerations and Future Directions

SCADA/DCS systems are increasingly important for various domains e.g. manufacturing, process industry, as well as critical infrastructures such as the SmartGrid, Intelligent Transportation Systems etc. Considering the trends and visions depicted here, we consider that key directions should be investigated, while considering a complex collaborative ecosystem of interacting devices, systems and entities.

Monitoring: Monitoring of assets is of key importance especially in a highly complex heterogeneous infrastructure. In large scale systems it will be impossible to still do the information acquisition with the traditional methods of pulling the devices. The more promising approach is to have an event driven infrastructure coupled with service-oriented architectures. As such any device or system will be able to provide the information it generates (data, alarms etc.) as an event to the interested entities and will also be able to compose, orchestrate that information/services in a model-based manner, generating new monitoring indexes not envisioned at the design stage of the composing systems (typical characteristic/property of SoS).

Management and Visualization: The next generation factory systems will be composed of thousands of devices with different hardware and software configurations. It will be impossible to continue managing such infrastructures the way we do it today. We will need to automate as much as possible primarily the monitoring part and also the soft-control of such systems. As such it should be possible to dynamically discover devices, systems and services offered by the infrastructures. It should be possible to do software upgrades and mass reprogramming or re-configuration of whole systems. Additionally (remote) visualization [20] of the real infrastructure is a must as it will give the opportunity of better understanding and maintaining it. The increased complexity will not allow per device management, therefore self-* features are desirable, at least at system level. More specifically self-configuration (automatic configuration of components), self-healing (automatic discovery, and correction of faults), self-optimization (automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements) and self-protection proactive identification and protection from arbitrary attacks) might ease large scale management and maintenance.

Security: Trust and Privacy: As next generation SCADA/DCS system will heavily interact with other systems (and in cloud services), apart from ongoing complex security concern, additional issues related to proper security, trust and privacy need to be investigated. We consider mostly today that all devices and systems are operated under the same authority or the same user. However this might not hold true in the future. Systems may be composed from simpler ones that may be administered by different entities and possibly not under the same security domain.

Scalability: Scalability is a key feature for large scale systems. For industrial systems it is expected that scaling up of resources available on single devices will emerge anyway. As such the impact should be considered e.g. at SCADA/DCS etc. in order to assess what capabilities can be assumed by large scale applications e.g. monitoring. Scaling out is also a significant option to follow, especially relevant to nodes having attached a large number of devices e.g. a SCADA system or even a monitoring application running in the cloud with thousands of metering points.

Real-time Information Processing: We anticipate that the real-time information acquisition is a challenging task; however for next generation applications to be able to react timely, we also need real-time information processing. The latter includes possible pre-filtering or pre-processing of information for a specific (business) objective and complex analysis of relevant (stream) events. Since real-time event processing relies on several steps, we need to tackle the challenges raised by them such as event-pattern detection, event abstraction, event scheduling, event filtering, modeling event hierarchies, detecting relationships (such as causality, membership or timing) between events, abstracting event-driven processes etc.

Mobility Support: The recent advances in mobile devices have already led to significant changes in the way business is conducted. Especially in customer interactions but also in industrial processes such as maintenance new approaches can be adopted where workers fully equipped with on-demand real time information can interact via mobile devices with business systems as well as local devices. We need to investigate the support for mobile devices e.g. being used as HMIs, the support for mobility of devices i.e. where devices are themselves mobile and the implications of this, the support for mobile users and interaction with static and mobile infrastructure, the support for mobility of services e.g. where services actually migrate among various

infrastructures and devices following e.g. user's profile constraints.

Simulation: Industrial environments are complex systems of systems. As such any change to a part of them may have unexpected results in other depending or collaborating parts. However independent evolutions of smaller systems are a must to achieve adaptively and resolvability. As such a system emulation is highly needed in order to be able to identify early enough possible conflicts and side-effects. Such simulations may be used in pre-deployment time: evaluation of behavior of changes to be applied and monitoring of them, as well as after deployment and during runtime.

Interoperability: As next generation systems will be highly collaborative and will have to share information, interoperability via open communication and standardized data exchange is needed. System engineering of complex interoperable systems has profound impact on their evolution, migration and future integration with other systems. The future industrial infrastructure is expected to be constantly evolving. As such it is important to be (i) backwards compatible in order to avoid breaking existing functionality as well as (ii) forward compatible which implies designing interfaces and interactions as rich as possible with possible considerations on future functionality to come.

9. Conclusion

In this research paper, we have given a brief overview of supervisory control and data acquisition systems. In addition to that the primary focus was on the security issues dealing with SCADA systems that also resulted in discussions on SCADA forensic which a specialized research branch is dealing with SCADA security.

References

[1] D. Bailey, E. Wright, "Practical SCADA For Industry, ISBN 9780750658058, Newnes, 2003
[2] R. Kalapatapu, "SCADA Protocols and Communication Trends", ISA EXPO, 2004
[3] M. Brandle, M. Naedele, "Security for Process Control systems: An Overview", In IEEE Security &
[4] T. Chen, S. Abu-Nimeh, "Lessons from Stuxnet", IEEE Computer Magazine, April 2011, Volume: 44, issue: 4, pp. 91-93
[5] K. Mandia, C. Prosise and M. Pepe, "Incident Response and Computer Forensics", McGraw-Hill/Osborne, Emeryville, California, 2003
[6] W. D. Jones, "Gone Missing: The Public Policy Debate on Unleashing the Dogs of Cyberwar", IEEE Spectrum's risk analysis blog, June, 2012
[7] M. Naedele, "Addressing IT Security for Critical Control Systems", 40th Hawaii International Conference on System Sciences (HICSS-40), Hawaii, January 2007
[8] F. Adelstein, "Live Forensics: Diagnosing Your System Without Killing It First", In Communications of the ACM, February 2006, Vol. 49, No. 2, pp. 63-66
[9] A. W. Colombo and S. Karnouskos, "Towards the factory of the future: A service-oriented cross-layer infrastructure," in ICT Shaping the World: A Scientific View. European Telecommunications Standards Institute (ETSI), John Wiley and Sons, 2009, vol. 65-81.
[10] D. Idoughi, M. Kerkar, and C. Kolski, "Towards new web services based supervisory systems in complex industrial organizations: Basic principles and case study," Comput. Ind., vol. 61, pp. 235–249, April 2010.
[11] P. Kennedy, V. Bapat, and P. Kurchina, In Pursuit of the Perfect Plant. Evolved Technologist, 2008.
[12] M. Jamshidi, Ed., Systems of Systems Engineering: Principles and Applications. CRC Press, Nov. 2008.
[13] N. Cai, J. Wang, and X. Yu, "SCADA system security: Complexity, history and new developments," in 6th IEEE International Conference on Industrial Informatics (INDIN), 2008.
[14] A. Durantini, "Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications", Fourth International Conference on Networking and Services ICNS, 2008.
[15] J. Rajamäki, J. Holmström and J. Knuuttila, "Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities", Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT) 2010.
[16] J. Holmstrom, J. Rajamaki & T. Hult, "DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication" in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 2011.
[17] DSiP information sheet, Ajeco Ltd, 2011.
[18] L. Daniela, "Cross-layer Assisted TCP Algorithms for Vertical Handoff", Department of Computer Science Series of Publications Report A-2010-6, University of Helsinki Finland, 2010.
[19] J. Ryu, "Congestion Control and Routing over Challenged Networks", The University of Texas at Austin, 2011.
[20] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung and Y. Lee, "Development of Ad hoc Network for Emergency Communication Service in Disaster Areas", Proceedings of the 9th WSEAS International Conference on APPLICATIONS of COMPUTER ENGINEERING, 2010.
[21] R. Robles & T. Kim, "Communication Security for SCADA in Smart Grid Environment", WSEAS Conference in ADVANCES in DATA NETWORKS, COMMUNICATIONS, COMPUTERS, 2010.

Author Profile

Steffi Paul Kalib received the B.E. in Information Technology from RGPV, Bhopal, M.P. She completed her M.tech project work from Department of Atomic Energy, RRCAT, Indore, M.P. Currently she is M.Tech scholar in Computer Science and Engineering from Lakshmi Narain College of Technology, Indore, M.P, India.

Dr. Manoj K. Rawat received the B.E. in Computer Engineering and M.Tech in Software Engineering from MNNIT, Allahabad, U.P. He completed his project work at MOTOROLA Company situated at NEPZ, Noida. Then he completed his Doctorates (Ph.D.) in Computer Science and Engineering from SU, Rajasthan. He has 15 years of teaching experience at various positions in different parts of India. He now is HOD Computer Science Department in Lakshmi Narain College of Technology, Indore, M.P, India.