ISSUES OF CYBER SECURITY IN SCADA-SYSTEMS - ON THE IMPORTANCE OF AWARENESS

Erik JOHANSSON
Royal Institute of Technology (KTH)
Sweden
erikj@ics.kth.se

Teodor SOMMESTAD
Royal Institute of Technology (KTH)
Sweden
teodors@ics.kth.se

Mathias EKSTEDT
Royal Institute of Technology (KTH)
Sweden
mathiase@ics.kth.se

ABSTRACT

The concern in our society for "cyber attacks" is increasing and cyber security has become a hot topic when it comes to protecting nation's critical infrastructures. A new technological landscape has not only made the SCADA-systems more open but also more vulnerable to cyber attacks due to existing vulnerabilities. An effective state of the art approach for understanding weaknesses of SCADA-systems is to create graphical models over the system architecture, and perform analyses based on this.
Based on practical assessments, literature and interviews surveys with both industry professionals and academics this paper highlights some common pitfalls when using graphical models commonly used as a basis for cyber security assessments of SCADA-systems.

INTRODUCTION

Nation's critical infrastructures, such as water and sewage systems; telecommunications, internet and computing services; air traffic, railroads and other transportation, is increasingly dependent on the proper functioning of the electric power system. The operation of the electric power system is highly dependent on computerized industrial control systems, in this paper denoted as SCADA-systems. These SCADA-systems perform highly advanced logic that automatically controls the power distribution network as well as provide the operators with vital information and efficient support needed to make advanced decisions such as identifying emerging problems and take actions preventing them. At the same time as SCADA-systems enables more efficient, qualitative, and safe infrastructure products and services their vulnerabilities are also direct vulnerabilities of the power system itself and thereby nation's critical infrastructures.

Management of SCADA-systems

In addition to the potential severe consequences of a compromised SCADA-system, security management of these systems is complex. Security is inherently suffering from a weakest-link syndrome, and consequently can a single misconfiguration in the SCADA-system be a vulnerability that jeopardizes the whole power system. This is truly a challenge since SCADA-systems in power distribution are extremely complex: they contain highly advanced functionality; they are heterogeneous and include several third party components; they are geographically dispersed; they are extensively networked, both internally and with external systems; and they depend on the human organization that manages and uses them [1]. Altogether SCADA-system security management can be described as keeping track of moving target that consists of a great number of details that are interrelated in complex ways.

Abstract representation of SCADA-system

Since these SCADA-systems are so complex, it is completely impossible for a single person to keep every piece of relevant information in his or her head. Therefore we need simplified descriptions, or maps, depicting the system. To use graphical representation of a system, such as computer network diagrams, is also a widely adopted practice within security management.

The challenge is however to make sure that our simplified models are reflecting the true state of affairs for the relevant properties of the systems. In reality these relevant system properties are seldom included in our models. For security oriented models it is for instance vital that information about firewall configurations and locations are included, whereas we are perhaps not as interested in the length of its source code or graphical user interface. With a graphical model that includes the relevant properties of the system, security can be effectively managed.

WEAKNESSES IN GRAPHICAL MODELS OF SCADA-SYSTEMS

To leverage the support to security management that graphical models can provide, they must represent factors that influence security in an adequate manner. This is however not always the case. Many of todays system maps were developed with other purposes than security in mind. Based on practical assessment, literature and interviews surveys with both industry professionals and academics typical weaknesses are here highlighted. Inadequate system models may lead to disillusionment and consequently poor awareness of the cyber security posture.

Management of networks

A fundamental concern regarding SCADA security is the increased connectivity to other, internal or external, computer networks. The typical and often recommended solution is to only carefully connect the SCADA-system to the controlled office LAN which in turn can be designed to mitigate cyber threats from the internet at the network perimeter by using firewalls, application proxies and related technologies. The operations of office networks are however not always regarded as a core competence at the enterprise, especially for small and

medium-sized enterprises (SMEs). Consequently these networks are frequently outsourced under the rationale of achieving cost savings or improved quality of service.
The business case for the outsourcing vendor is to be as cost efficient as possible and consequently it looks for economy of scale in the internal operation. A solution to this problem is naturally to operate several customers' networks in the same physical network but logically separated, cf. Figure 1.

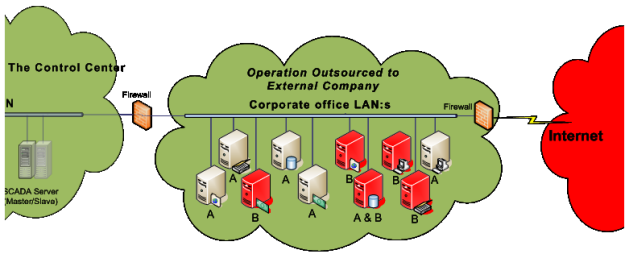

Figure 1. During the authors' practical security assessments at one facility "A" we identified that its corporate office LAN was closely interconnected with another company "B". The separation from other organizations was more or less chimaeras due to awful configurations and badly chosen passwords on critical part of the infrastructure equipment maintained by the outsourcing partner.

This fact is often missed in graphical models (other customers' equipment are often simply disregarded) and from a security point of view this could however become an additional threat. Misconfigurations in any of the other outsourcing vendor customers' equipment may affect the network security but the lack of knowledge of this network architecture may lead to a situation where safeguards such as firewalls are not restrictive enough.
Taking this further, the backbone network used by the outsourcing partner can in turn be controlled by another party and capacity over this network may be shared with other external parties, which introduce further threats [1].

Unidentified communication interfaces

Also internally in the organization it can be difficult to keep track of exactly how all the SCADA components are connected. For example, many of the components are equipped with functions or services that allow suppliers and control engineers can access them. Such interfaces are present because they bring many benefits to system management as they enable staff and external suppliers to install, update and configure software of various components over the Internet or a public switched telephone network, without physically visiting them.
If these remotely accessible interfaces at all are depicted in diagrams of computer networks they are typically considered secure since they shall be disconnected by default or is considered secured through authentication. Weak authentication of dial-up modems is however a common vulnerability and both password protection and dial-back routines are possible to circumvent [2]. Default passwords and generally weak passwords are a common phenomenon for field devices [2] and it is not uncommon that supposedly disconnected interfaces actually are plugged in and accessible on a constant basis. Unknown and possibly unsecure interfaces from field devices to public networks open these up for a wide range of threats, cf. Figure 2.

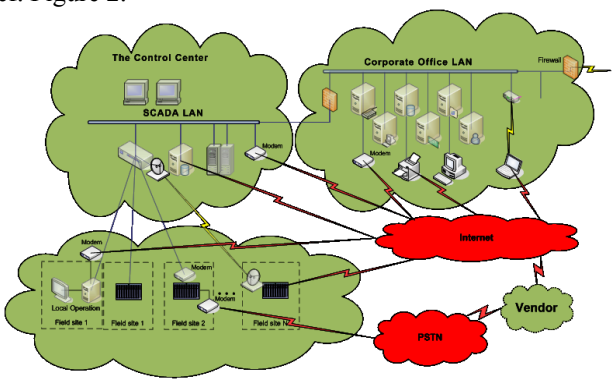

Figure 2. There are often many different communication interfaces to the SCADA system which are not depicted in the architectural model.

Since the interfaces usually are intended for support personnel access to them usually provide privileges that could be used to reconfigure devices, assign new set points or alarm levels, delete configurations or remove protection equipment functionality. Hence, unauthorized could to severely compromise the functionality of field devices and also influence the behavior of other parts of the system.

Software provide unknown services

One reason for why there exists more connectivity to the surrounding environment than what is desired is perhaps that much software provides such connections by default. Operating systems and application software are often developed with interoperability and ease of use as high prioritized requirements, resulting in a wide range of services made easily accessible and turned on by default. A great deal of security can be achieved if unnecessary and unneeded services and ports were deactivated, i.e. the systems are hardened. However, even if it is known what services that are activated, these are typically described in graphical models of the system. A difficulty here is that the system suppliers might be unsure of what services that are needed for their system to function properly and might be unwilling to leave guaranties for the system if services are disabled or removed.

Management of firewalls

In traditional models of the SCADA-system we typically depict the firewalls location but not IP-addresses and ports that it is open for. The real case is probably that the firewalls allow other data flows than what is known. Tests performed by Idaho National Laboratories did for example find weaknesses in all firewall configurations tested through the National SCADA Test Bed Program [2]. The configurations required for communication between the control center network and the administrative network and internet are typically complex and diverse. As a mix of COTS technologies are applied within the control system domain the number of protocols, ports and services used increases and often to an extent that makes it difficult to keep track of. Hence, in the same way as there might be a lack of information

about what services that must be to be activated for the computers to work, information is typically lacking regarding the parameters required to configure firewalls restrictively without jeopardizing operations [3].

Logical and physical configuration mismatch

Network segregation and controlled data flows is an important factor for achieving secure SCADA systems. If the control center and its network are connected to other networks the undisputed recommendation is to do so through a firewall. Diagrams often reveal the logical dimension of networks and here depict a clear separation of networks and the devices that control the flow over boundaries. However, in the physical dimension several of these logical devices might be implemented in one single physical entity by, for example, configuring a switch or router to treat some of its ports as separate logical networks, i.e. virtual LANs (VLAN), cf. Figure 3.

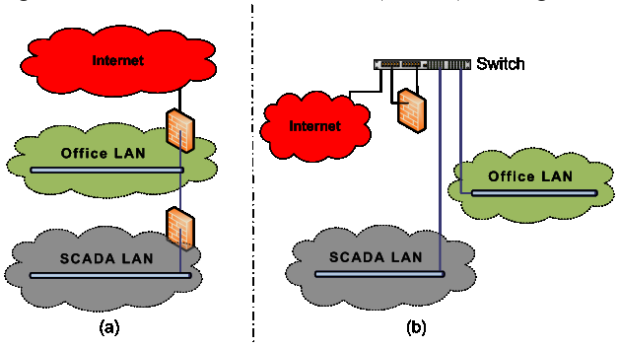

Figure 3. Logical and physical mismatch. In the logical schema to the left (a) one gets the impression that the different networks are well separated. However, in reality it looks like (b) the networks are physically connected to the same switch and the separation is only made logically by the VLAN configuration.

Although this is sometimes recommended by suppliers of infrastructure equipment, this is has weaknesses from a security point of view. Separating networks only through the logic implemented in software will make it possible to bypass this virtual separation if the software contains flaws that can be exploited from one of the networks connected to the device. Furthermore, maliciously created packages might circumvent the virtual separation and extreme conditions can alter the configuration of the equipment. Some network equipment do for instance starts behave like a network hub (data is transmitted/receive on all of its ports) when they are overloaded with network traffic. Graphical models used for security analysis should because of these factors consider the physical dimension as well.

Extended access perimeter

It is common security practice to make sure that the logical security perimeter resides within the physical security perimeter. In this way the protection is reinforced by making physical access a prerequisite for obtaining logical access. The physical barriers around buildings, facilities, rooms, equipment, establish these physical security perimeters. Physical security controls meant to protect physical locations include fences, walls, reinforced barricades, gates, or other measures. However, the increased use of portable computers and wireless technologies within both control centers, office LANs and substations often extends the logical access perimeter outside of the physical security perimeter, see figure 4.

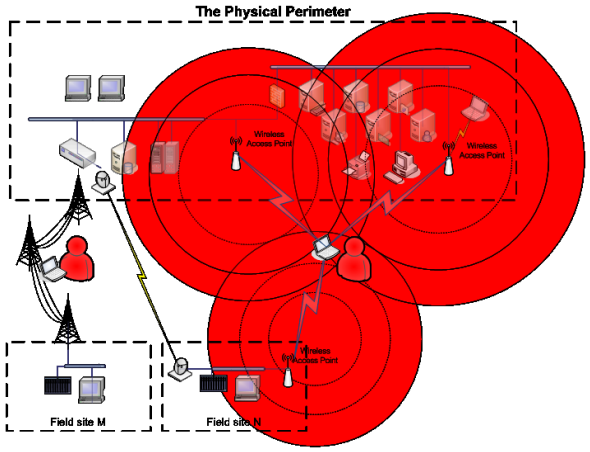

Figure 4. The use of wireless technologies easily extends the logical access perimeters beyond the physical security perimeter.

Geographically distributed processes (such as electric power distribution) are often controlled using a range of communication means, including radio links and power line carrier (cf. Figure 4). The often poor physical security of these communication channels in conjunction with the fact that both power line carrier and radio communication suffer from poor security [6], this open up another plausible security hole often unaccounted for in architectural models.

THE ACTUAL SCADA-SYSTEM

Our department has been doing research in the field of industrial control systems for decades and during the last years we have performed an increasing number of assessment focused on SCADA security [5][6][7]. Earlier the interest and focus of utilities, vendors and researchers have been on functionality and increased availability and safety-critical aspects [8], but as the interconnections between critical parts of the industrial control systems and other, not as reliable, networks increased the cyber security has come in center of attention [1]. This gap between the reality and the graphical system models that exist is dangerous since it oppresses the awareness of the increased threats to SCADA systems. Figure 5 illustrated some of the complexity and weakness that frequently can be found in actual SCADA system configurations of today. Consequently, this trend of integration together with the gap of awareness entails a fundamentally altered risk situation.

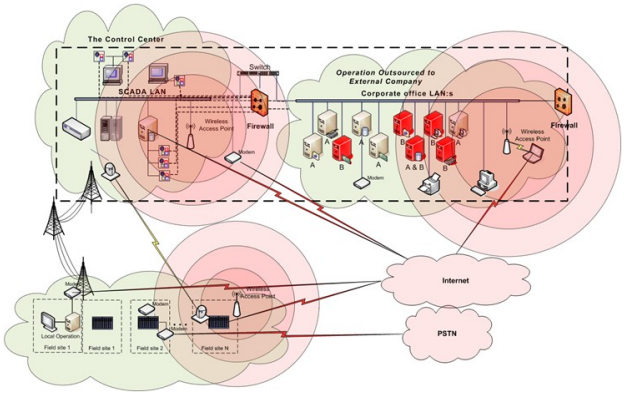

Figure 5. Illustration that summarize the complexity and weaknesses of today's SCADA system configurations.

CONCLUSIONS AND DISCUSSION

In this paper we have highlighted a number of vulnerabilities that can be difficult to detect when using traditional architecture models. The immediate response from these representations might perhaps be to not use architectural models at all. However that would not make the situation better. If you don't have the big picture clear, knowledge about details would be taken out of context and quickly become meaningless. Imagine for instance how tedious and costly it would be to physically follow every network cable as soon as the system is to be reviewed or maintained. This paper essentially promotes two general reflections about SCADA-system architecture models.

Firstly, it is vital to design the architecture model so that it contains the relevant entities and properties [5]. If these are not included, the analyses that we want to do can simply not be done. From our experience we often find that hardware related aspects of the system are fairly covered in the architecture, but software related aspects and organizational issues are too often absent. It is important to remember that one model is not inherently more "true" than another just because they include different type of information, they are simply different views of the same system. But in a hardware oriented architecture it is for example impossible to determine if the access control is set properly, for this we need to know who is accessing what, both physically and logically, and under what circumstances.

Secondly, it is of vital importance to be aware of the credibility of the architectural model [9]. For instance, how thorough was the information collection endeavour that populated the architecture model in the first place and when was it done? Practically this is reflected by how much we can trust that for instance an IED does not have a modem actively connected to it. Do we dare making important decisions based on this fact when this particular piece of information is based on a quick interview with the former system administrator five years ago? On the other hand is quite costly to make thorough audits and update the current architecture model. So the consequence of not being sure in the end needs to be traded against the benefits of being sure, i.e. something that should be part of a risk analysis.

REFERENCES

[1] Krutz R., 2006, *Securing SCADA Systems*, Wiley Publishing, Indianapolis, Indiana.

[2] Fink R., D. Spencer and R. Wells, 2006, *Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems*, US Department of Energy.

[3] BCIT Group for Advanced Information Technology, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, London, UK, 2004

[4] Office of Energy Assurance, 2003, *21 Steps to Improve Cyber Security of SCADA Networks*, U.S. Department of Energy.

[5] Johansson E., P. Johnson and T. Cegrell, 2006, Assessment of Information Security in Electric Utilities - The Importance of Prioritization, *Proceedings of CIGRE 2006*.

[6] Johansson E., et al., 2007, *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter*, Swedish Emergency Management Agency.

[7] Johansson, E., 1996, *Safety-Critical Control Systems - The Challenge of Migrating from Hardware to Software*, Royal Institute of Technology, Stockholm.

[8] NISCC, 2005, *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Coordination Centre, London.

[9] Johansson E., 2005, *Assessment of Enterprise Information Security – How to make it Credible and efficient*, The Royal Institute of Technology, Stockholm.