Addressing IT Security for Critical Control Systems

Martin Naedele
ABB Corporate Research
5405 Baden-Dättwil
Switzerland
martin.naedele@ch.abb.com

Abstract— **Control systems for critical infrastructures like national power grids make increasingly use of open technologies and protocols, and the Internet. In this environment, the risk of electronic attacks on these control systems has to be evaluated and mitigated. This paper addresses the key challenges commonly mentioned in the context of control system security (also referred to as "SCADA security") and discusses feasible solutions for most of them. The paper argues that the main obstacle to control system security is not technical, but financial. A couple of exemplary research projects from one automation vendor that aim to reduce the plant owners' cost of security are presented to demonstrate what kind of research will bring control system security forward.**

I. Introduction

A. Control systems and the Internet

Industrial automation and control systems are used in many critical application domains like electric power generation and distribution; gas and water supply; transportation, and manufacturing of goods including hazardous and toxic production processes.

Depending on the type and purpose of the automation system, its components are distributed on a local, wide-area, or even global scale. In the past, automation systems were not linked to each other and were not connected to public networks like the Internet. Today, the market puts pressure on companies to make fast and cost effective decisions. For this purpose, accurate and up-to-date information about the plant and the process status have to be available not only on the plant floor, but also at the management level in the enterprize and even for supply chain partners. This is equally true for power utilities [1]. Such change in commercial environment results in increasing interconnection between different automation systems as well as between automation and office systems. Initially, such interconnections were based on specialized, proprietary communication mechanisms and protocols. Today, open and standardized Internet technologies as well as the Internet itself are increasingly used for that purpose.

Large scale interconnected network infrastructures for power utilities are currently explored in a number of projects and approaches [2], [3], [4].

B. The threat of electronic attacks

With the usage of COTS technologies, open protocols, and fully networked systems the opportunity for electronic attacks increases and the threat of such attacks has to be addressed [5]. The risk of electronic attacks on critical control systems is real. Several incidents have been reported in the press in past years. More recent examples are:

A survey published in the Pipeline and Gas Journal in February 2006 [6] reports that about 20 percent of the repondent utilities did already encounter external attacks on their SCADA systems, and 33 percent expect such attacks in the following 24 months.

Confidential information, including incident response plans, were leaked out of a Japanese power plant through a virus infested computer with peer-to-peer file sharing applications in two independent incidents in the first half of 2006, following a similar incident in a different plant in 2005 [7].

An expert from the US DHS warns that intelligence agencies increasingly see indications of terrorist interest in SCADA and embedded systems [8].

So there is clearly evidence for some security related incidents and risk. How big that risk really is, is hard to estimate, though. The only serious attempt to collect unbiased data, an initiative of the British Columbia Institute of Technology, still doesn't have a collection of data that allows statistically significant statements [9].

Nevertheless, considering the potential consequences of an attack on critical infrastructures, efforts to secure the control systems of these infrastructures are certainly important. It is also true that control systems have certain characteristics that clearly distinguish them from office IT systems, such as the priority of availability over confidentiality, real-time response requirements, and long (multiple decade) system life times.

C. Contributions

Nevertheless, many statements on control system security by security vendors, consultants, and government agencies appear to be overly alarmist, like [10] or

> "Many are beginning to believe the FUD about SCADA is merely the cyber-security industry employing scare tactics. This presentation will erase all doubt. Understanding SCADA security is easy: there is none. [...]"[1]

This paper tries to put the issue into perspective and to provide direction for future research by explaining feasible solutions to the most commonly named challenges, and by pointing out the most significant challenge that remains.

[1] Abstract for talk by security vendor ISS [11] at www.blackhat.com/html/bh-federal-06/bh-fed-06-speakers.html#maynor

1530-1605/07 $20.00 ©2007 IEEE

II. Secure control systems - Challenges and solutions

In the last couple of years, challenges regarding the IT security of control systems have often been exaggerated by various stakeholders. While this hype certainly had the positive effect of raising awareness on various levels, ranging from plant owners/operators to politicians, it also has some drawbacks: Some control system owner/operators may hesitate to start any security activities because they feel overwhelmed by the problem, others may refuse to do anything by themselves and blame the control system vendors instead, and yet others may fall victim to sellers of "silver bullet" or "snake oil" solutions. Also, a focus on challenges that in reality could easily be resolved obscures the view on those few issues that the community should concentrate on addressing.

This section surveys a couple of often-mentioned challenges around control system security and explains how they can and should be addressed by means that are available today. Most of these challenges have been repeatedly mentioned in a variety of publications and venues over the last couple of years, but most of them can also be found mentioned in [11], the presentations of the 2006 SANS SCADA Security Summit [12], and the energy sector control system roadmap prepared for the US Department of Energy and Department of Homeland Security [1].

A. Organizational and perceptual challenges

Security is in the first place not a technical issue. In consequence, some of the largest challenges in making control systems more secure relate to human behavior and the perception of the problem.

1) Policy: For many control systems there exists today no clearly defined security policy. A security policy describes who is allowed (and not allowed) to do what in the system. The security policy is thus the basis for any technical, procedural, and organizational security mechanism. While it may be true that such policy does not exist in many plants, this is not a control system specific issue. Plant management is responsible for creating, communicating, and enforcing a security policy. Material to aid in this task can be found on the web (e.g. http://www.sans.org/resources/policies/) or from consulting companies.

2) Unclear distribution of responsibility for control system security between business IT and process operations: According to various reports, this really is an issue in many plants [13]. However, this is not a control system specific issue. It is necessary to educate both sides so that they develop a shared understanding about security requirements as well as the needs and operating constraints of control systems and what this means with respect to the applicability of certain security mechanisms. Implementing such training program and establishing clear responsibilities are not a security engineering tasks but normal change management.

3) Monitoring and detection: According to the concept of time-based security [14], any effective security system must not rely on protection functions (filter, access control) alone, but has to have the capability to detect an ongoing attack and to react on it. The detection and reaction steps typically require human intervention, e.g. for analysis of log files or evaluation of alerts. A common problem during operation of such security system is that no qualified resources are available to execute detection and reactions tasks. This is especially a concern for small IT operations where the number of security experts needed for an around-the-clock incident response capability would cause overhead costs that seem unacceptable to the plant management. Outsourcing security monitoring and incident response to a managed security service provider is one option in this situation, which is also applicable to control system environments. Here the risk incurred by the remote connection to the monitoring center of the service provider is to be considered and mitigated. Plant responsibles may be hesitant to allow active incident handling to a party outside the plant and with little automation knowledge. This could be addressed by requesting that any active incident response has to be executed in collaboration with an on-site plant operator. It is also expected that in the near future more and more managed security service providers with specialized automation domain knowledge will appear on the market. An alternative to using a managed security service provider is presented in Section III-A.

4) Awareness of external connectivity: An initial reaction of plant responsibles on being confronted with IT security issues for the control system for the first time is often the belief that they are not affected because their control system is not connected to the Internet. While this may actually be true for specific plants and specific points in time, experience shows that the existence of direct (e.g. vendor/service dial-up modem into control system) and indirect (e.g. connection to enterprise intranet in order to exchange ERP data) links between the automation system and external public networks is often underestimated [15]. If the plant security strategy, or lack thereof, is based on this assumption, plant management is responsible for verifying that this assumption holds and continues to hold over time. Inhouse IT staff or external consultants will easily be able to determine whether external connectivity to the Internet or other remote access opportunities exist, and policies as well as procedures have to be adapted to ensure that none will be created in the future without management approval and risk analysis. Of course, one shouldn't forget that insider related IT security risks may exist even in plants without any external connectivity.

5) Awareness of being affected: Similar to the previous point, plant management sometimes ignores the threat of IT based attacks on the system on the assumption that there is nobody who would want to attack them, that their employees are all trustworthy, or that an attack would not have any severe consequences. Again, these assumptions may actually be true in some cases, but plant management has the responsibility to base their actions not on a subjective estimate but on an objective, thorough and documented evaluation of the risk for the plant. Such qualitative risk can be done with reasonable effort. Most automation vendors offer plant risk assessment

services to their customers.

6) Belief in security by obscurity: A variant of the lack of awareness of being affected is the belief that no attack would be possible because an attacker could not possibly understands the (legacy) protocols and systems as well as the application domain sufficiently well to mount an attack. This perception is objectively wrong [16]. Legacy control systems and protocols are used all over the world, their documentation is available to anybody with sufficient interest. INL has demonstrated that they can reverse-engineer an unknown control protocol within days to the extent that they can use it for an attack, and some attacks, e.g. attacks on availability, are independent of detailed knowledge of the system. Today, a risk analysis and security architecture for a plant should be conducted under the assumption that the attacker has full knowledge of the plant.

7) Belief in regulation: Some plant owners believe that no actions with regard to IT security are necessary until this is required by regulation, or they believe that the measures required by regulation (e.g. NERC CIP [17]) will automatically provide the right level of security for their plant. Both beliefs are dangerous: The first one disregards that not meeting regulatory requirements is just one of the potential risks that should be taken into account in the risk analysis. The second one ignores the fact that the objectives of the regulator requiring certain measures (which are ”fair” and can be objectively evaluated) and the protection requirements that the plant may have (effectively preventing violations of availability, integrity, confidentiality, access control, etc.) overlap only partially: A regulation compliant system will not necessarily be secure and a secure system may not meet the regulatory demands.

8) Belief in certification: Certain interest groups are promoting the certification of control system components with regard to security, e.g. in accordance with a standard like ISO/IEC15408 (”Common Criteria”). They argue that a similar certification requirement exists for products and plants concerning functional safety (IEC61508, IEC61511). Certification requires a large investment in terms of money, resources, and time. In addition, certification does not guarantee security - in many cases it is even counterproductive: Experience with Common Criteria certified products in other domains (e.g. operating systems, databases) has shown, that certified products still have security vulnerabilities [18]. However, a certified product has to be time-consumingly recertified after each update, therefore certified products are always several generations behind the most up-to-date system version. Specifically the Common Criteria certification has additional problems because it does not allow to reason about the security of systems composed from certified components and it does not take possible misconfigurations of the product/system into account. Plant owners/operators should be aware that security certifications will likely lead to higher product costs while not significantly improving effective security.

None of the challenges listed in this section is specific to control systems or otherwise insurmountable.

B. Lifetime challenges

A number of challenges for control system security are related to the very long life time of such systems. This not only means that system designed today will be around for a long time, but also that many of the systems in operation today and for some more years to come were originally designed, implemented, and deployed with little or no consideration for security.

1) Control system without security mechanisms: Many control systems in operation today have been designed and deployed in a time when electronic attacks on computerized systems were not yet widely spread and when those systems were protected to a large extent by the fact that there was no external connection into the control system. Physical protection of the plant thus ensured electronic security as well. At that time, neither vendors nor plant owners foresaw the evolution towards open and integrated systems. The main challenge with respect to such systems today is to realize that the original assumptions don’t hold anymore, and to react accordingly. It is today very well possible to securely operate an inherently unsecure systems encapsulated in the innermost zone of a zoned, defense-in-depth security architecture [19] that uses layers of externally arranged electronic and procedural measures to ensure that the risk of compromise of the core control systems remains neglibly small. Electronic access can be protected by multiple levels of firewalls and intrusion detection systems (IDS) with data transfer architectures that transport externally relevant data from the inside to the outside while blocking any request that originates on the outside. Communication protocols can be secured using virtual private networks (VPN) and associated authentication/authorization mechanisms at the VPN tunnel endpoints. Non-existing access controls at the console of the control system can be addressed either via replacement of frontend HMI systems or via introduction of, potentially technically supported, operational policies and procedures that ensure that only authorized humans have physical access to the control system HMI.

2) Control systems that can not be updated/patched: The control system that can not be updated or patched to remove discovered security vulnerabilities is a special case of the control system without security mechanisms. The inability to apply updates may originate from the fact that for an ”old” system component, like an outdated operating system version, updates are no longer provided by the vendor, it may be related to the fact that any change would require a time-consuming and expensive re-certification e.g. for plant environmental safety or product safety concerns, or it may be caused by the need to run the control system continuously without any interruption for modifications. Each of these reasons can be addressed. A solution for all of them is to encapsulate the unmodified/unmodifiable control system as described in the previous section. The issue of old, no longer supported components like operating systems may additionally be solved by migrating to a newer control system generation. The restriction of continuous operation can be overcome by

installing updates on a parallel system and switching over after having verified correct function of the updated system. In order to avoid regulatory re-certifications it is advisable to separate those concerns of the control system that require certification from those that are known to require frequent updates, such as intrusion detection systems, malware scanners, and security applications in general, such that the security mechanisms are decoupled and independent from the subsystems involved in the safety argument.

One can argue that the security level of the plant of course has implications for its safety posture and that thus security and safety can not easily be considered independently from each other. However, it is necessary to distinguish different levels of abstraction here: the objective and the technical realization: A safety argument following e.g. IEC61508 does not require detailed reasoning about the technicalities of the security architecture. It just requires that security has been considered such that the likelihood of safety breakdowns due to security incidents is suitably reduced.

The requirement from the safety perspective is thus that the system provides a security architecture that can guarantee certain security objectives (e.g. ”no unauthorized user can access the system”) over the life time of the system. While the security objectives remain static in the respective safety case, a dynamically evolving security architecture (new rules, new devices, new algorithms) may actually be necessary to achieve and maintain this level of protection despite a changing threat situation outside the system. A frozen security architecture would be inappropriate.

At the same time, the evolving security mechanisms must not interfere with system properties that other parts of the safety case rely on, such as CPU load, data transfer rates, interrupt times, and absence of software faults. It would, for example, not be acceptable from a safety (re-)certification point of view that the increasing number of malware signatures that have to be checked (by itself an appropriately evolving security mechanism) increases the execution time of the malware checking task on the CPU and reduces the processing time available for other safety critical tasks. Another example would involve updated software code to defend against new attacks that has unknown execution behavior and potential flaws affecting the safety functionality. Suitable decoupling is thus necessary, e.g. by using different devices for functional safety and security protection of functional safety.

3) Lifetime of COTS components: In the last decade, many control system vendors have migrated their systems from proprietary operating systems to commercial-off-the-shelf (COTS) operating systems like Microsoft Windows or a variant of Unix, because customers requested such systems due to the more comprehensive functionality, the cheaper price, and the familiarity with these operating systems in the workforce. A similar trend towards COTS components can also be observed for other elements of a control system, such as database management systems or HMIs via web browser/web server. A significant drawback of COTS system components from the consumer sector is, of course, that there the product cycles are much shorter (3-5 years) than in the automation domain. This need not necessarily lead to security vulnerabilities in the system, but it requires either to continuously migrate the system to the latest platform and set of COTS components, or to freeze the installed configuration and treat the system as unmodifiable, as described above. Recent advances in commercially available virtualization technology may make a hybrid approach approach viable, where the system is frozen on a virtual inner platform whereas this virtualization platform is hosted on an up-to-date and hardened real platform.

4) Security mechanisms with need for continuous updates: Certain security mechanisms, such as malware detectors (antivirus scanners) and intrusion detection systms (IDS) or intrusion prevention systems (IPS) rely for their function on continuous, daily, or even hourly, updates with the latest descriptions of undesirable events that they should detect, so-called signatures. The signatures are provided by the vendors of these systems, consulting companies, or the a volunteer user community. New signatures are developed as new attacks are discovered. Not updating these systems is not a viable option, because it would essentially render them useless. Also, it can not be realistically expected that any chosen product line, signature format, or signature provider will remain available, supported, and in business during the whole lifetime of the protected automation system. The security elements in the system architecture will thus, as has been explained in the previous section, have to be exchanged/renewed repeatedly during the lifetime of a plant. It is therefore necessary to decouple long-lived control and short-lived security functionality both from a technical point of view, to facilitate drop-in replacement, and from a conceptual/design point of view, to avoid dependencies of, e.g., control loops or safety arguments on certain non-commodity aspects of the security system, such as throughput or failure modes.

5) Communication protocols without security mechanisms: Like the control systems also the communication protocols used in automation systems have been designed without security mechanisms, because security was not a concern at that time. Such unsecure communication protocols can today be secured by running them inside a secure tunnel provided by a VPN. Depending on the specific requirements, the VPN provides confidentiality and/or integrity of the transmitted data and associates messages with the authenticated identity of the sender and access control rules on the side of the receiver. Support for VPNs is ideally integrated into client and server devices, but sometimes the devices, especially embedded controllers, don’t have the computational performance needed to execute computationally intensive cryptographical operations together with real-time control tasks. For this case, various vendors offer VPN devices (link encryptors) both for serial and TCP/IP/Ethernet based communication links. See Section II-C.2 for concerns regarding latency. In addition to retrofitting existing communication links with secure tunnels it is also important to ensure that newly designed automation protocols don’t make the same mistakes. Unfortunately, that is still happening - the recently introduced utility communication

standard IEC61850 [20] and the time synchronization standard IEEE1588/IEC61588 [21] were designed mostly without regard for security. A whole series of standards is currently being produced to suggest tunneling options for a number of utility communication protocols, including IEC61850 (see [22], [23]). A more positive example is OPC-UA, the next generation "unified architecture" of the well-established OPC protocol, where security has received considerable attention from the beginning [24].

C. Technical challenges

The challenges related to the human aspects and the long system lifetime are frequently encountered in a control system environment, but are not specific for this environment. This section describes a number of challenges that are more specific to the technology and the operational requirements of control systems.

1) Lack of computational power: Embedded controllers are frequently designed to use processing platforms that are tailored to the specific control task. They often do not have the performance reserves necessary to support cryptographic operations needed for authentication, message integrity protection, and encryption. This can be compensated by locating the security related functionality in dedicated security devices outside the controller. Such security devices with firewall, VPN, access control, log, IDS, and/or AV functionality are available from multiple vendors. [25], for example, describes a security gateway that is targeted towards a specific embedded controller and even implements application-level message filtering functionality that inspects incoming messages based on knowledge about the expected message semantics for the specific protected controller application. A separate security gateway has two additional advantages compared to integrating security functionality within the controller: It decouples ephemeral security functions from long-living control functions and it provides additional separation so that the effects of an attack (crashing, blocking, high CPU load) remain limited to the security gateway and don't affect real-time control functionality. As a drawback, the separation between security gateway and controller opens a hole between these two devices that an attacker with physical access to the system could exploit. For this reason, and to reduce cost despite potential security decrease through loss of separation, vendors will soon be able to offer controllers with built-in security capabilities if the market demands such devices.

2) Latency induced by cryptographic protection: Encryption and decryption of data take time, especially if data first have to be aggregated to blocks before applying an algorithm, and thus introduce latency in the message transmissions. In some automation environments such additional latency and a resulting reduction of the scan rate are critical. A working group of the American Gas Association (AGA12) has developed a low-latency encryption scheme they claim to be especially suitable for many SCADA applications [26], [27], [28]. While it was developed by an organisation associated with gas SCADA systems, this scheme is intended to be usable also in other domains, such as electric power control systems as a further alternative to the protocols in IEC62531 [22], [23]. The algorithm has been implemented as prototype in Java [29] and various vendors offer bump-in-the-wire link encryptors for retrofit to serial SCADA links using this scheme. In future work, AGA12 will also address management of cryptographic keys for protected SCADA communication links [30].

3) Intrusive vulnerability scanning: In many office IT environments all hosts on the network are regularly scanned for missing patches and known vulnerabilities. In an automation environment such procedure may not be advisable because the scanning could induce network flooding, or, depending on the aggressiveness of the scanner used, even crash one or more of the scanned hosts. This means that the host configuration monitoring tools for use in automation systems must not try to exploit a vulnerability to determine its existence. They may thus be less accurate than is possible with today's technology. Alternatively, a fully intrusive scanner could be run against a system that mirrors the live control system, such as an isolated backup, training system, or a system used to verify successful restoration of backups. In this case processes and procedures have to be in place to ensure that the mirror system is identical to the main system.

4) Preventing malware: In general, it is a good practice to run on each host one or several background scanners checking for malware like viruses, worms, Trojans, or spyware whenever a file is accessed. Guidance on using malware scanners for automation systems is given in [31]. However, running anti-malware applications may not be feasible for all hosts, or parts of the file system of a control host will have to be excluded for performance reasons. Protection against malware import may thus have to be provided by different means, e.g. by strictly controlling the paths through which malware could get into the system: All media, like CDs, DVDs, or portable memory devices and handheld computers should be scanned for malware infections on a dedicated scanning station, which is not part of the automation network, before being allowed to be inserted into the automation system. Application updates and other data to be downloaded into the control system should ideally also be digitally signed by a trusted and authorized source [32]. Hosts that are part of the automation network should not provide email clients for receiving email or web browsers for access to arbitrary web sites. For these purposes dedicated hosts can be provided in the control room, which are connected directly to the Internet or intranet, but not the automation network.

5) Preventing incoming requests: A network or network segment that allows incoming requests to servers is much more vulnerable to attacks than a pure client or network of clients. Once incoming requests are permitted it becomes much harder to differentiate between legitimate and malicious requests. An attacker my be thus be able to flood the system with traffic or otherwise spoof or manipulate permitted traffic to gain access to and compromise a server. Nevertheless, sometimes valid business reasons exist to provide a facility for clients in outside networks to request data from the control system. As far as is

possible this should be realized by a data transfer architecture in which the external client does not directly access a host inside the control network but instead only accesses a mirror server outside the automation network, which is fed regularly from within the control system. It is then possible to place a firewall between the mirror server and the control system with a rule set that blocks all requests from the outside into the control system.

6) Emergency override: Safety, and thus maintaining control over the plant, are the most important functional goals in many control systems. In many plants thus unimpeded access to controls in an emergency has to have higher priority than security/access control. A comprehensive solution will likely employ technical and non-technical means. On the technical side, biometric or token/smartcard based authentication credentials ensure that an operator can not lock himself out of the system by mistyping or forgetting his password in a critical situation. On the non-technical side there should be predefined procedures to formally declare a state of emergency, to disable parts of the access control system as necessary, and to replace technical enforcement of authorization by supervision through multiple humans. Additional procedures should be established to switch back from an emergency mode of operation to a normal, secure mode.

7) Intrusion detection in automation systems: Intrusion detection systems (IDS) are an important part of security architectures. Their role is to detect an ongoing attack and to alert a human supervisor who can then initiate an incident response. Use of intrusion detection systems inside automation systems is not yet very common, thus there is little empirical data on how useful an IDS is in this environment. One could argue that typical IDS rules do not target automation protocols and thus will not detect attacks on that level. Another concern is that IDS output will contribute to confusion and operator stress in critical situations, for example if a malfunction in the plant causes a storm of alarm messages in the automation system which then again are interpreted as unusual by the IDS, causing additional alerts from the IDS. Then again, most (untargeted) attacks will use normal IT protocols, not automation protocols, and there have been efforts to define IDS rules for automation protocols like Modbus and these have been incorporated into some commercial and open source IDS products [33]. The alarm storm problem shouldn't really occur if a signature based instead of a anomaly based IDS is used, and it is even likely that signature based IDS will perform much better (less false positives) in a control system environment with a static network, application, and dataflow topology than in a normal office environment, so that an anomaly based IDS may not be needed.

8) Controlling the client for remote access: Remote access from a central office or external service provider is a frequent requirement for automation systems, in order to reduce time delays and costs when diagnosing problems and configuring or optimizing the system. While the connection between the automation system and an external client can be secured against tampering and information disclosure using a VPN, the risk of a compromised client end-point remains. The automation system has little means of monitoring and enforcing security policies and status on remote client hosts, especially if these are under the administrative control of a different organization. An industry recommended solution for this type of scenario is to use two desktop sharing applications (e.g. PCAnywhere, MS Remote Desktop, VNC, etc.) in series. The first link connects the external remote client to a terminal server in the DMZ just outside the automation system. The second link mirrors the workplace of a control system workplace to this intermediate terminal server in the DMZ. The terminal server in the DMZ is under full control of the plant owner. As it has no special control system availability or real-time constraints, it can be updated/patched regularly by the IT department of the plant. Thus the automation system is, independently of the potentially different remote clients, only connected to one fixed outside system, the terminal server, which is in a known and controlled state. Ideally, two different desktop mirroring applications are used for the two different access links. An attacker would then have to compromise the remote client and break into the desktop mirroring connection to the terminal server, there break into a different type of desktop mirroring connection, and only then would he be able to gain access to the control system workplace. For even higher security demands, the plant-side mirrored workplace should be manned by an operator observing the remote access session who can interrupt this session in case of suspicious activity.

9) Secure wireless communications: While not yet in widespread use, wireless LANs (IEEE802.11) receive currently a lot of interest for communications on plant floors and in utility substations as is demonstrated, e.g., by the establishment of the ISA SP100 and Cigre B5.22 working groups. Over the last couple of years, significant improvements have been made with regard to security schemes in the wireless link layer. Nevertheless, it is better not to rely on the transport technology for security, but use end-to-end security mechanisms on the application layer. The issue of wireless versus wired communication becomes then largely irrelevant, with the exception of the threat of jamming, that is, drowning the communication signal in radio noise. Jamming is a type of availability attack that is particular to wireless communication systems and can not easily be prevented.

D. Financial challenges

As has been shown in the previous sections, feasible technical or procedural solutions exist for most of the challenges related to securing automation systems against electronic attacks. If this is so, then why is state-of-the-art security of SCADA systems today still regarded as such a difficult objective to realize? We argue the reason is money. Most of the security mechanisms proposed for control systems cost money, some of them, like regular updating or replacement of vulnerable or unmaintainable control system components cost even significant amounts of money during the life time of a control system, and plant owners have so far been reluctant to make these investments.

The problem is further aggravated by the fact that many good security solutions from commercial security vendors that would be technically suitable and recommendable for control systems, e.g. application level firewalls for web services, are priced towards enterprise deployments where even their high price is only a small part of the total IT investment. In contrast, such investment is difficult to justify in mostly small control system installations.

So the question is not really how to secure control systems at all, but how to secure control systems for a level of cost that is acceptable to the plant owners. That means that on the one hand we have to work to reduce cost of security - Section III provides some examples of what ABB is doing in that respect - and on the other hand the community must raise awareness for the necessity of considerable spending on security architectures and operations in order to operate today's highly interconnected automation systems securely.

Not a lot of reliable data exists on control system security incidents and existing data are not statistically significant [9]. While this is fortunate considering the possible consequences of an electronic attack on a national power grid or a chemical plant, it often makes it difficult to construct a convincing business case for SCADA security investments purely from a financial point of view. However, many utilities and industrial companies recognize that despite a low likelihood the risk related to the potential high cost of a single security incident in a critical plant justifies getting serious about implementing security measures and have started to do so. In some industries otherwise reluctant plant owners are being pushed towards investments into security through regulatory mandates, such as NERC CIP [17], though it is not clear how effective such forced security measures are in comparison to a security architecture based on a deliberate risk analysis.

III. ABB AUTOMATION SECURITY RESEARCH ACTIVITIES

In the previous section it was argued that IT security for control systems is more a cost issue than a technology issue. This section describes a number of activities and R&D projects that ABB Corporate Research together with other ABB business units undertakes in order to make security more affordable for utilities and industrial plants.

A. The plant operator as part of the security architecture

Section II-A.3 explained that continuous monitoring to detect intrusions and initiate responses is essential for the security of a system. There it was suggested to outsource monitoring to a managed security service provider, if the plant operators don't have the necessary expertise. This is feasible, but, of course, expensive. In many plants, a feasible and more cost efficient approach would be to involve the plant operator as intelligent anomaly detector and decision maker who initiates first responses and calls in qualified staff for additional help. This approach requires that the security health status of the control system can be communicated to the plant operator in a way he is used to, with paradigms like process pictures and trend curves, without requiring IT or IT security expertise. ABB is developing a security workplace as add-on to its process control system that meets these requirements [34]. Using such system, it may be possible for a plant to implement a detection/reaction strategy without having to involve expensive internal or external security analysts for around-the-clock security monitoring.

B. Scalable user access control for embedded devices

In order to provide accountability for actions taken in the system down to the individual user, it is in most cases necessary to require individual authentication to any accessed controller. This requirement is in strong contrast to the common current practice for embedded systems to share access credentials among authorized users. The current practice, though undesirable from a security point of view, is rooted in the fact that managing dozens or hundreds of individual user accounts goes beyond the capacity limits of most embedded devices, and that configuring and maintaining these user data on hundreds or thousands of devices across the plant is not cost efficiently feasible, especially when 24 hour user authorization change/revocation roll-out time limits like in NERC CIP 004-1/B/R4.2 [17] are required.

[35] proposes a novel authentication and access control scheme for embedded devices based on public key cryptography. It combines the scalability of user maintenance of centralized schemes like Kerberos with the ability to provide access to off-line devices and the storage space and engineering properties of conventional decentralized shared password schemes. The main idea is that user rights and user access credentials are managed on a single (or small set of) central servers which issue time-limited capabilities to the user which are signed with the private key of the central authorization server. Each embedded device thus only needs to know the public key of the authorization server to verify the signature and the user information and granted permissions in the capability.

C. Standards and guidance

If the plant owner has little or no security expertise in-house, then devising and implementing a security architecture or specifying security requirements for an automation system or its components requires costly employment of consultants. Several initiatives have been ongoing over the last couple of years, with significant involvement of ABB and several other automation vendors, to produce guidelines or even formal standards to communicate security essentials to automation system responsibles and to empower them to plan and specify their security needs in a way that is cost-efficient and reflects industry recommended practice [36], [37], [38], [19], [39], [40].

D. Threat modeling

Threat modeling is an essential part of any product or system design process targeting security. It is also the basis for qualitative or quantitative risk (reduction) evaluation methodologies, as have recently been proposed for the control system domain [41].

However, threat modeling today is an activity that requires considerable time and security expertise among the persons involved. Well-known threat modeling methodologies target deployed systems with known use and risk profiles, e.g. e-commerce or e-banking, but not product developments. The quality of a threat model is hard to evaluate by somebody who was not involved in its creation. This discourages peer review and independent validation of threat models. ABB recently started a research project with the University of St. Gallen, Switzerland, to address these deficits in state-of-the-art threat modeling with the goal of developing tools and methodologies or validatable threat models for products, especially for automation system components.

IV. Conclusion

This paper gave an overview over the real and perceived challenges in securing industrial and utility control systems against electronic threats. It was shown that solutions for most organizational and technical challenges exist today. The paper argues that securing control systems is not the unsurmountable challenge as which it is often portrayed, but rather a question of the willingness on the side of the plant owners to spend the necessary amounts of money and resources, as is stated in the roadmap [1]:

> "Asset owners and operators bear the chief responsibility for ensuring that systems are secure, making the appropriate investments, and implementing protective measures."

IT security in automation is not a technical problem, but a cost or cost/risk trade-off problem. Therefore, to increase the level of security in the industry, we have to both increase the willingness to pay for security, which implies to accept security as a valuable system property worth paying for, on par with safety or performance, and at the same time reduce the cost of implementing and deploying security measures. Proposals for new security mechanisms or approaches should not be evaluated from a perspective of additional cost compared to a current no security/no cost posture, but start from a fully secured system and ask whether the specific proposal can achieve the same protection objective with less initial and/or ongoing investment.

In consequence, research in the field should concentrate on making security for control systems more cost efficient. A couple of examples for such research conducted at ABB have been presented.

Unfortunately, the proliferation of control system security initiatives and forums dilutes the existing expertise and thus actually forms an obstacle to faster progress. Also, some of the current regulation-oriented approaches to security disregard the cost efficiency goal.

References

[1] J. Eisenhauer, P. Donelly, M. Ellis, and M. O'Brien, "Roadmap to secure control systems in the energy sector," http://www.controlsystemsroadmap.net/, January 2006.

[2] "IntelliGrid project home page," http://intelligrid.info/.

[3] "GridStat project home page," http://www.gridstat.net/.

[4] C. Rehtanz, T. Kostic, and M. Naedele, *Autonomous Systems and Intelligent Agents in Power System Control and Operation*. Springer, 2003, ch. Implementation of Autonomous Systems.

[5] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, June 2005.

[6] D. Walker, "Utility IT Executives Expect Breach of Critical SCADA Systems," *Pipeline and Gas Journal*, February 2006.

[7] J. Leyden, "Japanese power plant secrets leaked by virus," The Register, http://www.theregister.co.uk/2006/05/17/japan_power_plant_virus_leak/, May 2006.

[8] J. L. Shreeve, "The new breed of cyberterrorist," The Independent, online edition, http://news.independent.co.uk/world /science_technology/article622421.ece, May 2006.

[9] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in *Proc. of VDE Kongress*, October 2004.

[10] T. Datz, "Out of control," CSO Magazine, online edition, http://www.csoonline.com/read/080104/control.html, August 2004.

[11] D. Maynor and R. Graham, "SCADA security and terrorism: We're not crying wolf." Presentation at Blackhat Federal 2006, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf, January 2006.

[12] "Presentations of the 2006 SANS Process Control and SCADA Security Summit," https://portal.sans.org/scada06/.

[13] J. Weiss and J. Abshier, "Are your security practices up to IT standards?" http://www.controlglobal.com/articles/2006/051.html, 2006.

[14] W. Schwartau, *Time based Security*. Interpact Press, 1999.

[15] H. Forbes, "Survey results: Plant floor remote access," ARC Advisory Group presentation, September 2004.

[16] E. Byres, "The myth of obscurity," ISA Safety Community Update, http://www.isa.org/rd.cfm?id=1216, September 2002.

[17] NERC, "Standard CIP-002-1 to 009-1 - Cyber Security, Draft 4," January 2006.

[18] J. S. Shapiro, "Understanding the Windows EAL4 evaluation," *IEEE Computer*, vol. 36, no. 2, pp. 102–105, 2003.

[19] Eric Cosman (ed.), "Security for Industrial Automation and Control Systems, Part 1: Concepts, Terminology and Models," ISA standard S99 Draft 2, Edit 9, for ballot, April 2006.

[20] IEC, "IEC61850 communication networks and systems in substations," International Standard, IEC61850, Part 1 to 10, 2003.

[21] IEEE/IEC, "Precision clock synchronization protocol for networked measurement and control systems," International Standard IEC 61588: 2004 (1588-2002), 2004.

[22] F. Cleveland, "IEC TC57 Security Standards for the Power Systems Information Infrastructure - Beyond Simple Encryption," Oct 2005.

[23] IEC TC57/WG15, "IEC 62351: Data and Communication Security," International Standard IEC 62351, parts 1-8, various drafts, 2005.

[24] Richard Oyen (ed.), "OPC UA Part 2 - Security Model RC0.91 Specification," http://www.opcfoundation.org, April 2006.

[25] M. Naedele, "Innovative Lösungen für die Informationssicherheit in Automatisierungssystemen," in *Proc. of the VDE Kongress 2004*, October 2004.

[26] A. Wright, "Low-latency cryptographic protection for SCADA communications," in *Proc. of 2nd Int. Conf. on Applied Cryptography and Network Security*, June 2004.

[27] American Gas Association, "Cryptographic protection of SCADA communications: Background, policies and test plan," AGA Report No. 12, part 1, http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml, March 2006.

[28] ——, "Cryptographic protection of SCADA communications: Retrofit link encryption for asynchronous serial communications," AGA Report No. 12, part 2 draft, http://www.gtiservices.org/security/aga12_wkgdoc_homepg.shtml, March 2006.

[29] A. Wright, http://scadasafe.sourceforge.net/.

[30] D. Holstein and J. Diaz, "Cyber security management for utility operations," in *Proc. 39th Annual Hawaii Conference on System Science (HICSS-39)*, 2006.

[31] J. Falco, S. Hurd, and D. Teumim, "Using host-based antivirus software on industrial control systems: Integration guidance and a test methodology for assessing performance impacts, draft version 1.0," http://www.isd.mel.nist.gov/projects/processcontrol/AV_Guide_PCSF_Draft_Release_20060530.pdf, May 2006.

[32] M. Naedele and T. Koch, "Trust and tamper-proof software delivery," in *Proceedings of the 28th International Conference on Software Engineering and Co-Located Workshops, Proceedings of the Workshop on Software Engineering for Secure Systems 2006*, May 2006, pp. 51–57.
[33] "DigitalBond SCADA intrusion detection forum," http://www.digitalbond.com/support-center/.
[34] M. Naedele and O. Biderbost, "Human-assisted intrusion detection for process control systems," in *Proc. of 2nd Int. Conf. on Applied Cryptography and Network Security*, June 2004.
[35] M. Naedele, "An access control protocol for embedded devices," in *accepted for Proc. 4th Int. IEEE Conf. on Industrial Informatics (INDIN'06)*, 2006.
[36] M. Naedele and D. Oyen, "Standards for securing industrial automation systems," *ABB Review*, no. 4, pp. 69–74, 2005.
[37] ISA SP99, "Security technologies for manufacturing and control systems," Instrumentation, Systems, and Automation Society, Tech. Rep. ISA-TR99.00.01-2004, March 2004.
[38] ——, "Integrating electronic security into the manufacturing and control systems environment," Instrumentation, Systems, and Automation Society, Tech. Rep. ISA-TR99.00.02-2004, April 2004.
[39] James Gilsinn (ed.), "Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control Systems Security Program," ISA standard S99 Draft 2, Edit 9, for ballot, April 2006.
[40] M. Naedele, "Standardizing Industrial IT Security A First Look at the IEC approach," in *Proc. 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05)*, September 2005.
[41] M. McQueen, W. Boyer, M. Flynn, and G. Beitel, "Quantitative cyber risk reduction estimation methodology for a small SCADA control system," in *Proc. 39th Annual Hawaii Conference on System Science (HICSS-39)*, 2006.