

# IT Security for Automation Systems

## Motivations and Mechanisms

Martin Naedele, ABB Schweiz AG, Corporate Research

*The protection of safety-critical and infrastructure systems (such as automation systems for utilities, but also for manufacturing plants) against electronic and communication network based attacks becomes more and more important. This paper examines how such safety-critical plants and automation systems can be secured against information system and network based attacks. Based on the defense-in-depth approach, a conceptional, generic security zone model for use in analysis and synthesis of a plant security architecture is proposed, and for each of its zones a survey of the available and appropriate security mechanisms for delay, detection, and reaction is given.*

*Der Schutz von sicherheitskritischen Systemen und Infrastruktureinrichtungen (wie zum Beispiel der Automatisierungsanlagen von Versorgungsunternehmen, aber auch von Fabrikationsanlagen) gegen elektronische Angriffe über Kommunikationsnetzwerke ist ein Thema von wachsender Bedeutung. Dieser Beitrag stellt dar, wie derartige sicherheitskritische Systeme gegen Angriffe über das Informationssystem und durch das Netzwerk gesichert werden können. Unter Benutzung eines tiefengestaffelten Sicherheitsansatzes wird ein konzeptionelles und generisches Sicherheitszonenmodell für die Analyse und Synthese von Sicherheitsarchitekturen vorgestellt. Für jede der Zonen wird eine Übersicht über verfügbare und angemessene Mechanismen für die Verzögerung, Entdeckung und Beantwortung von Angriffen gegeben.*

### 1 Introduction

The protection of automation systems of manufacturing plants and utilities against electronic and communication network based attacks becomes more and more important [9][14][15]. This is mainly because of three current developments:

- There is an economic and technical trend towards interconnection and Internet connection of such systems. This makes convenient remote access to these systems available to many people, but on the other hand also enables remote attacks [17]. In many cases, legal prosecution is not a useful deterrent, e.g. because the attacker cannot be identified, or his actions are not a punishable crime in the country where he is based.

- There is a technical trend of migrating automation system and network architectures from proprietary protocols towards standardized, open protocols, applications and systems. With respect to security this has the two negative consequences that a larger number of people exists who have the knowledge necessary to attack the system, and that increased interoperability of devices prepares the ground for deliberately and incidentally malicious devices.
- The global political and economic situation makes attacks on such infrastructure systems likely:
  - "Water, electricity, [...] and other critical functions are directed by computer control [...]. The threat is that in a future crisis a criminal cartel, terrorist group, or hostile nation will seek to inflict economic damage [...] by attacking those critical networks. [...] The threat is very real." [1]*
  - "The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid." [2]*

On the economic side the competition between, for example, deregulated power utilities creates economic incentives for malicious actions:

Competition, a first for power suppliers, has created what IEEE-USA calls "financial incentives for malicious intrusion into computers and communications systems of the electric power industry and marketplace participants." [3]

In these types of applications, in contrast to commercial and administrative data processing applications, often not typical data security issues (e.g. confidentiality, integrity) as such are the most important goal, but IT security is one component of the safety and fault-tolerance strategy and architecture for the plant.

These trends have been recognized and in different industries companies have started to work together in forums like the NIST Process Control Security Requirements Forum and the recently established ISA SP99 committee to develop common and standardized strategies to defend against IT-based attacks against automation systems.

## 1.1 Previous work

While there exists a huge amount of research on security in home and office information systems - [12] gives a good introduction into the topic -, only very little has been done in the area of network security for automation systems. [8] investigates the suitability of the firewall concept for remotely accessing information systems and proposes a smartcard based infrastructure for encryption and digital signatures. In [7] security issues with regard to remote access to substation automation systems are analyzed and some security measures are proposed, with a particular emphasis on the use of passwords and proper selection of passwords. Both papers are concerned with remote access via public networks, not at all with potentially malicious devices inside the automation system.

## 1.2 Contributions

The main contributions presented in this article are the following:

A generic zone model for the design of secure automation systems is introduced as a conceptual reference model for security architecture discussions.

Security mechanisms (conventional and automation system specific) for delaying an attack, detecting an attack, and reacting on an attack are surveyed in the context of this zone model. Note however, that the zones and security mechanisms are not intended to be regarded as constituting the one and only secure automation system architecture fitting all purposes. This survey is intended as a toolbox for designers and implementors of automation systems who have to augment the automation and safety functionalities of a new or existing system with comprehensive security functionality, according to the risks, requirements, and budget of a specific system.

In addition, it is shown that making use of the specific characteristics of an automation system offers opportunities to implement security mechanisms that would not be feasible in an office computing environment.

### 1.3 Overview

This work investigates ways how safety-critical plants and automation systems can be secured against information system and network based attacks. The article is structured as follows: Section 1 has motivated the need for increased automation system security by because of recent trends, events, and reports that relate to potential threats. In Section 2 the two common defense approaches, hard perimeter, and defense-in-depth are discussed and arguments are given why defense-in-depth with multiple, staged, complementary security mechanisms is the more suitable approach. As a consequence of this reasoning, in Section 3 a conceptual, generic security zone model for use in analysis and synthesis of a plant security architecture is proposed. In Section 4, the main part of this article, for each of these three zones a survey of the available and appropriate conventional security mechanisms is given. Section 5 concludes the article.

## 2 Two approaches to securing systems

### 2.1 Hard perimeter

One of the popular philosophies for defense, be it of cities or IT systems, is the notion of the hard perimeter ("crunchy outside, chewy inside"). The idea is to have one impenetrable wall around the system and ignore all security issues inside. However, in general this does not work, for a variety of reasons:

The hard perimeter approach does not make use of reaction capabilities: At the time of detection of a successful attack, the attacker has already broken through the only wall and the whole system is open to him. In consequence, this means that the wall would need to be infinitely strong, because it needs to resist infinitely long [13].

Monoculture is dangerous: The wall is based on one (physical) principle. If that principle or fails for some reason to resist the attack, the whole defense is ineffective.

The wall must have doors to be usable; this creates technical and social engineering security risks. Once the attacker has managed to sneak inside, the system is without defense - the risk of the proverbial Trojan horse. It is also, by definition, ineffective against insider attacks.

Progressing technology gives the attacker continuously better wall-penetration capabilities.

Last, but not least, humans make mistakes: It is illusory to assume that we can design a wall that is without weak spots either in design, implementation, or operation - the Chinese Wall provides a historical example.

## 2.2 Defense-in-depth

The alternative approach, resulting from the above arguments, is defense-in-depth. Here several zones/shells are placed around the object, which is to be protected. Different types of mechanisms are used concurrently around and inside each zone to defend it. The outer zones contain less valuable targets, the most precious goods, in this case the safety critical automation system, are in the innermost zone. In addition to defense mechanisms we also have detection mechanisms, which allow the automation system operators to detect attacks, and reactive mechanisms and processes to actively defend against them. Each zone also buys time to detect and fend off the attacker. In the spirit of Schwartz's time-based security [13] this allows to live with the fact of imperfect protection mechanisms, as only a wall strength of  $P \geq D+R$  has to be achieved, where  $P$  is the time during which the protection offered by the wall resists the attacker,  $D$  is the delay until the ongoing attack is detected, and  $R$  is the time until a defensive reaction on the attack has been completed.

In summary: There are two basic approaches for securing systems in general use today, but only one, defense-in-depth, will, if properly implemented, actually result in a secure system.

## 3 Generic security zone model

As a consequence of this reasoning, a conceptual, generic security zone model for use in analysis and synthesis of a defense-in-depth plant security architecture is proposed, consisting of:

- *Remote access zone*, which contains all remote users and remotely connected information systems - either via dial-up telephone lines or via Internet/intranet,
- *Station zone*, which covers the workstations of the plant operators. These are assumed to be LAN-networked general purpose PCs. In many ways this zone is similar to a normal office computing environment: human users, interactive user operations, unpredictable data flows, complex, as well as commercial operating systems and applications. Specific for the system in the station zone of an automation system as compared to a normal office or lab computing environment, and relevant from the IT security perspective is that the software installations on the system are not determined by and under control of the user, but are centrally selected, installed, administrated and monitored, and that certain applications (e.g. IRC, email, web servers, etc) will in many cases not at all be run on operator workstations.

- *Automation system zone*, which contains the safety critical automation and control devices. These are typically embedded devices communicating in a predictable way. This means, that the configuration of the system is relatively static and that all involved devices and their normal, legitimate communication patterns (regarding communication partners, frequency, message size, message interaction patterns, etc) are known at configuration time, so that protection and detection mechanisms can be tailored to the system. Also, additional non-networked (out-of-band) safety and fault-tolerance mechanisms may be available to cover the failure of one or multiple components of the automation system.

Figure 1 shows a defense zone model for automation systems. Of course, in a practical implementation, additional subdivisions of these zones to create multiple, smaller compartments would further increase security. However, for each of these compartments in a zone the same set of security mechanism types would be applicable as are described here on the level of the zone. Thus the generic model in the following will for simplicity only use the three different types of zones.

Note that this is a conceptual model for discussing the security properties of system architectures and for selecting appropriate mechanisms. A specific automation system consisting, e.g. of a PC running an HMI application and a soft-PLC, which is connected to the Internet via modem, realizes all three conceptual zones within one host. Depending on the controlled process and the security mechanisms per zone implemented on this host it may or may not be a reasonably secure architecture – it probably isn't, though.

**Figure 1: Generic defense zone model for automation system security planning and analysis**

## 4 Zones and mechanisms

In each of the defense zones each security mechanism can be classified as belonging to one or multiple of the following categories:

- *Deterrence*: Pointing out to the potential attacker that his personal pain in case of getting caught does not make the attack worthwhile. However, in most threat scenarios for safety-critical and infrastructure systems the deterrence component, especially the counter-threat of legal action, is ineffective. Deterrence mechanisms are non-technical and will thus not be discussed in the following.
- *Connection authorization*: Is the other host at all permitted to talk to the system under consideration?
- *User authorization*: Is the user (or the application) on the other host at all permitted to talk to the protected application? What are his privileges?
- *Action authorization*: Is the user (or the application) on the other host allowed to execute the actions he wants to initiate? In this sequence?
- *Intrusion detection*: Has any attacker managed to get past a wall, e.g. by means of a Trojan? Most intrusion detection systems are based on monitoring and detecting whether anything "unusual" is going on in the system.

- *Response*: How to throw the attacker out of the system? How to remove any damage done by the attack? How to protect the environment against negative consequences of the attack? How to avoid a repetition of the same type of attack or from the same attacker?
- *Mechanism protection*: To make the above mechanisms effective, they must themselves be protected against subversion. This refers, for example, to not sending passwords in clear text over public networks, fixing well-known bugs and vulnerabilities in operating systems and applications etc.

## 4.1 Conventional IT security mechanisms

### 4.1.1 Remote access zone (Figure 2)

#### **Connection authorization:**

- dial-back modem: After authentication via dial-in modem the system dials back to a preconfigured telephone number for this authenticated user. This prevents an attacker to masquerade as an authorized user from anywhere in the world, even if he managed to obtain this user's credentials, because the attacker would also need to obtain physical access the authorized user's phone line.
- firewall: A firewall passes or blocks network connection requests based on parameters such as source/destination IP addresses, source/destination TCP/UDP ports (services), protocol flags etc. Depending on the criteria the specific firewall product uses and how clearly defined the permitted traffic on the network is, a firewall (or, more often, dual-firewall architecture) can be anything from a highly effective filter to a fig leaf.

#### **User authorization:**

- Remote Access Dial In User Service (RADIUS): A protocol for dial-in user authentication [10].
- secure passwords: Most authentication schemes rely on passwords ("something you know") to establish that the user is who he claims to be. This makes the selection of suitable passwords, as well as their management and storage one of the most important aspects, and potential weaknesses, of each system [7][16]. Related schemes use, instead of a fixed password, a one-time password generated just-in-time by individualized devices (tokens, smartcards) that are given to all authorized users, thus replacing or augmenting the "something you know" principle by "something you have".

#### **Intrusion detection:**

- failure alerts: The operators are alerted whenever one of the authentication mechanisms fails, which could indicate an unsuccessful attempt to attack the system.
- log analysis: All actions of the authentications devices are logged, and these logs are manually or automatically screened for unusual occurrences or patterns (e.g. an authorized user is suddenly accessing the system outside his normal work hours).

#### **Response:**

- collect and secure evidence: Gathering, copying, and storing at a secure location of all logs and media (e.g. hard disks) that contain evidence of the malicious activity. This evidence can be used to identify the attack and thus the system weaknesses in detail, to locate and estimate the amount of damage done by the attack, and also to support legal prosecution of the attacker. In this case the correct handling of evidence is especially important.
- trace back: This refers to activities that aim at discovering the source of the attack, both as part of the evidence collection process (see above) and to enable stronger defense mechanisms for identified sources of attacks (e.g. blocking). Due to various possibilities for faking packet data (such as the originating address) this is technically not easy. [4] discusses the various technical options for trace back and their obstacles.
- active counterattack: An active counter attack has as aim to selectively disable the attacker's computer to prevent further attacks and to "punish" the attacker. Due to the fact that a unambiguous trace back is difficult (see above), that often "innocent" systems are used as intermediary stages for staging an attack, and that the legality of a counterattack is dubious in most situations and localities, a counterattack response is normally not recommended.
- information sharing: Early sharing of information about ongoing attacks, especially novel types of attacks, with the IT community represents good "Internet citizenship" because it gives more defenders a chance to increase alertness and to remove weaknesses. Many types of attacks, such as distributed denial of service and viruses, rely on the fact that the same weakness can be exploited on a large number of systems, which then are used to launch further attacks. Therefore, reducing the number of systems vulnerable to an attack is in every defender's interest. On the other hand, many companies might be concerned about the effects of making the facts and circumstances of attacks known to competitors and the public. For this purpose several institutions exist which receive and distribute information about attacks without disclosing the sources of the information. Examples are the SEI CERT (<http://www.cert.org>) and various industry branch (IT; banking, oil & gas) specific Information Sharing and Analysis Centers (ISACs), e.g. <https://www.it-isac.org>, <http://www.energyisac.com>.
- selective blocking: If the origin of the attack and the location of entrance into the system can be identified, blocking rules of firewalls, routers, and access servers, perhaps already at the Internet Service Provider, can be temporarily or permanently modified to close the inroads of the attack.
- switching to backup IT infrastructure (production hosts, access servers, firewalls, IDS hosts) preconfigured with different passwords, different network addresses, and, even better, also software diversity (see explanation below) with respect to the primary systems.
- automated, periodic reinstallation of applications, operational data, and configurations: The SW applications of the automation system, as well as static operational data and configurations, especially of the security components, are periodically and on detection of an attack reinstalled from a known-good read-only storage device (e.g. CD). This replaces applications with backdoors (Trojans) or modified system files (e.g. password files), which an attacker has installed, even if the attack was not picked up by the IDS.

- new passwords: The automatic or manual reinstallation of system configurations in case of attack should also change the passwords used, in particular those for the security components, to avoid that an attacker can immediately re-enter the system with a compromised set of credentials.

***Mechanism protection:***

- dedicated lines: Instead of connecting the dial-in modems to telephone lines, which are accessible to anybody from anywhere in the world, dedicated telephone cables are used which connect only secure, authorized systems. Among other things this protects the information flowing between the protected system and the remote user, in particular its credentials such as passwords during the authentication process, from eavesdropping.
- virtual private network (VPN): A VPN uses encryption and digital signatures to achieve the effect of a physical dedicated line over a shared medium such as a normal telephone connection or the Internet.
- disable remote reprogramming of dial-in/dial-back modems: The dial-back mechanism is only effective, if the remote attacker can not redirect the dial-back call to his own telephone.
- network address translation (NAT): With NAT the system uses internally different IP addresses than those shown in the externally visible messages. A border device, e.g. the firewall, is responsible for on-the-fly translation of addresses in both directions. NAT makes remote probing of the internal network topology for interesting or vulnerable targets much more difficult and prevents certain attacks that bypass the firewall.
- Diversity: System diversity, e.g. by using different operating systems like Windows and Unix/Linux for the production systems and the intrusion detection systems or other security mechanisms, or by selecting different brands of firewalls for different zones and sub-zones increases security, as an attacker can not rely on a single vulnerability in one product to break through all defenses. It also offers a bit more resilience in the time between publication of an exploit for a vulnerability and the design and installation of corresponding patches in the system.

**Figure 2: Conventional IT security mechanisms for the remote access zone.**

#### ***4.1.2 Station zone (Figure 3)***

***Connection authorization:***

- firewall: see above
- switched Ethernet: There are two issues with standard Ethernet: (1) All hosts on a network segment can see all traffic, even that which is not addressed to them, and (2) multiple hosts sending at the same time can lead to non-deterministic delays. The first issue is directly security relevant, the second one indirectly (denial-of-service attacks). Using switches to give each host its own network segment and to directly forward each message only to the intended receiver remedies both issues.
- personal firewall: A personal firewall monitors and controls on each host which applications are allowed to initiate and accept connection requests from the network. A personal firewall does not control a network segment, but only the host on which it is running itself.

***User authorization:***

- secure password: see above

**Action authorization:**

- role-based access control in applications: In most cases, not all authorized users are in the same way permitted to execute all types of activities on the system, therefore the network log-on alone does not offer a sufficient granularity of access control. With role-based access control each authorized user has one or multiple roles, which correspond to sets of actions he can execute in the application. Role-based access control needs to be designed into each application, as it can normally not be provided by external add-on devices or applications.

**Intrusion detection:**

- network-based intrusion detection system (IDS): A network-based IDS tries to discover attacks based on known attack profiles and/or unusual system behavior from information seen on a network segment. A network-based IDS obtains its information from the traffic on the network segment (type, content, frequency, path of the transmitted messages).
- host-based intrusion detection system (IDS): A host-based IDS tries to discover attacks based on known attack profiles and/or unusual system behavior from information seen locally on the host on which it is running. A host-based IDS obtains its information for example from file system-integrity checkers, which monitor whether important system files change without operational reason, from personal firewall logs, from application logs, e.g. for application-level role-based access control. At least the most important and security-relevant hosts such as firewalls and network-based IDS servers should be secured by a host-based IDS.
- honeypot: A honeypot (<http://www.honeynet.org>) is a subsystem that looks particularly attractive to an attacker, e.g. from the naming of the host or files on it, or by simulating certain weaknesses in the installation. It is, however, a dedicated and isolated system without importance for the functioning of the automation system, which is especially instrumented with intrusion detection systems. The idea is that an attacker who successfully breaches the first line of defense will be attracted to the honeypot host first, and thus is at the same time delayed, kept away from the really sensitive areas, and detected by the intrusion detection systems.

**Response:**

- collect and secure evidence: see above
- selective blocking: see above
- system isolation: see above
- switching to backup IT infrastructure: see above
- automated, periodic reinstallation: see above
- new passwords: see above

**Mechanism protection:**

- switched Ethernet: as described above; serves also to protect passwords etc flowing on the network
- role-based access control: Role-based access control is also important for the security functionality itself, to ensure that only security administrators and not all inside users can change security settings and read/edit logs. This is the basis of all security precautions against insider attacks and also creates an additional hurdle for attackers that have broken into the account of one authorized user against taking complete control over the system.

- hardened host: Mechanisms like role-based access control, logging, IDS rely on the basic functions of the operating system on the host not having been corrupted by the attacker. Today's applications, operating systems, and system configurations are often so complex and complicated that they have many security holes through mis-configuration or through applications with security relevant bugs which are installed as part of the operating system, but which are not really necessary for the automation system functionality. Hardening a system means to remove all unnecessary applications and services, to fix known bugs, to replace critical applications with more trustworthy ones of the same functionality, and to set all system configuration parameters to secure values. Guidelines for the hardening of various common operating systems and applications are available from multiple sources, e.g. SANS ([www.sans.org](http://www.sans.org)).
- diversity: see above

**Figure 3: Conventional IT security mechanisms for the station zone.**

### 4.1.3 Automation system zone (Figure 4)

**Connection authorization:**

- switched Ethernet: see above
- firewall: see above

**User authorization:**

- secure passwords: see above

**Intrusion detection:**

- network-based IDS: see above

**Response:**

- switching to backup IT infrastructure: see above
- automated, periodic reinstallation: see above

**Mechanism protection:**

- switched Ethernet: see above

**Figure 4: Conventional IT security mechanisms for the automation system zone.**

## 4.2 Automation system specific IT security mechanisms

### 4.2.1 The automation system environment

Automation systems allow for specific security mechanisms (Figure 5) and thus a higher level of IT system security than normal lab or office computing environments, due to a number of reasons – though, of course, not all of these may apply to all automation systems:

The configuration of the automation system is static. The number and types of devices in the system are well-known and basically constant over time. During operation, the configuration only changes in the context of major maintenance or modification work. This justifies the effort of e.g. statically setting up tables with communication partners/addresses in all devices involved at the time of installation.

Many communications occur automatically and directly between applications acting on their own behalf with no involvement of a human user.

There are often no confidential data on the automation system network inside the plant.

Permanent Internet connectivity may often not be needed.

The devices in the automation system zone are not used for general purpose computing. Often, they are even specialized embedded devices dedicated to the automation functionality, such as power line protection in substation automation.

All appropriate technical and administrative means are taken to ensure that only authorized and trustworthy personnel has physical access to the automation equipment.

Automation system personnel is accustomed to a higher level of care and inconvenience when operating computer systems, than office staff. This increases the acceptance and likeliness of correct execution of security relevant operating procedures which are not absolutely straightforward and convenient.

**Figure 5: Automation system specific IT security mechanisms (Shown for all zones in one diagram).**

#### *4.2.2 Remote access zone*

**Connection authorization:**

- access time windows: If the remote connection is not necessary for operation, but only to upload configuration changes and download measurement values, which are not urgent and irregular in timing, the remote access can be restricted to certain time windows. Outside these time windows no access is allowed, enforced e.g. by electrically switching off the modem or router device.

**Action authorization:**

- data exchange system architecture: If the remote access functionality is not necessary for interactive operation and examination of the automation system, but only for upload and download of pre-configured parameters and data, the system can be architected so that direct remote access to the automation device, which is source or target of the data, is not required. Instead, the remote access occurs only to a less valuable FTP or web server, which acts as cache and communicates over a series of time-shifted, content-screening data forwarding operations with the actual data source or target.

**Response:**

- system isolation: The connections between the compromised system and other, more important parts of the automation system, are closed to avoid further spreading of the attack. Depending on system/remote access functionality and importance, on whether delaying the attacker and collection of further evidence, or quick restoration of operation is of higher importance, it is an option to shut-down all remote connections, both for the affected and the not-yet affected systems, until the effects of the attack are removed. Like for electric power grids, the automation system should already be architected and designed such that it can be partitioned into zones, which can be isolated while keeping disruption of the remaining parts to a minimum.

#### *4.2.3 Station zone*

**Action authorization:**

- managed application installation: Through centralized administration and monitoring it is enforced that only the authorized and necessary applications and services are running on station level PCs, and that configurations are not changed by the users. The PCs do not carry user specific data or configurations and thus can be reinstalled from a known-good source at regular, frequent intervals to remove any unauthorized modification in the system, even if the modification was never detected.

**Response:**

- system isolation: see above

#### 4.2.4 Automation system zone

**Connection authorization:**

- intelligent connection switch/monitor: As the information and message flows between the individual devices and applications in, for example, a substation automation system are deterministic and well defined at system configuration time, this information can be used by a special, intelligent connection monitoring device to determine the legitimacy of a certain message not just based on the general parameters conventional firewalls use, but also using additional criteria such as message size, frequency, and correctness of complex interaction sequences. Non-conforming messages can, in collaboration with a switch, be suppressed, in which case the device is acting as a connection authorization device, or an alert can be raised, in which case the device is acting as an automation system level IDS.
- mutual device authentication: As all communication partners (automation devices and applications) and message flows are known at configuration time, it is possible to require mutual authentication of each communication relationship at run-time, provided that the available computing power of the automation devices tolerates the execution of the necessary protocols. This prevents the installation of rogue devices in the system.

**Action authorization:**

- application level firewall: The process level network to which the automation equipment is connected should interface with the higher level (e.g. station level) network only at a small number of locations. As the purpose, the software applications, and the topology/configuration of the automation system are well-known, this interface can be implemented by an application level firewall which prevents direct interactive access ("log-in") to the automation devices and screens messages passing the interface for validity based on domain-specific criteria, such as predefined interaction sequences. Illegitimate or invalid messages can be suppressed and alerts can be raised.

**Intrusion detection:**

- intelligent connection switch/monitor: see above
- application level firewall: see above

- malicious activity detection/suppression protocol: As is shown in [5], network-based electronic attacks originating from malicious devices in an automation system like a substation automation system can be categorized as either message injection, message modification, or message suppression. Using a suitable communication protocol for detection of invalid messages, one can reduce these three categories to message suppression, which can in many cases be regarded as a system failure that conventional fault-tolerance and fault-response mechanisms such as redundant devices and emergency shutdown sequences can handle.

**Response:**

- system isolation: see above
- activation of safety mechanisms: If the attack endangers the safety of the plant, standard safety mechanisms such as reverting to manual operation or emergency shutdown are activated to protect plant equipment and environment.

## 5 Conclusion

Nowadays, realistic scenarios for network-based attacks on automation systems (referring to both infrastructure/utility automation systems and manufacturing/plant automation systems), with respect to both motivation and technical feasibility exist. These attack scenarios differ significantly from attacks in the office environment: Confidentiality is not the prime issue, and damage might not be restricted to the IT system and contained data, but involve bodily harm to the general public.

In this article, arguments have been presented why a defense-in-depths approach with a variety of layered defense mechanisms is a more appropriate strategy for securing automation systems than the often-used approach of placing a "wall" (e.g. firewall, dial-in authentication) around the system and leaving the inside unchanged.

As a reference model for security architecture discussions a generic three layer defense zone model with a remote access zone, a station zone, and an automation system zone has been proposed, and the conventional arsenal of security mechanisms has been surveyed and mapped to these zones. A lot of information on detailed issues of applying these mechanisms can for example be found at <http://rr.sans.org> and <http://www.giac.org/cert.php>.

In addition, a number of additional security mechanism have been proposed which are made possible by the specific boundary conditions (environment, operation, function) that many automation systems share.

## References

- [1] US Critical Infrastructure Assurance Office: Practices for securing critical information assets (CIAO technical report 2000).
- [2] Dick, R.: FBI National Infrastructure Protection - industry security briefing, 2002
- [3] IEEE-USA: Legislative agenda for the 107th congress (2000).  
<http://www.ieeeusa.org/forum/AGENDA/index.html>
- [4] Lee, S and Shields, C.: Technical, Legal and Societal Challenges to Automated Attack Traceback. IEEE IT Professional, May/June 2002, pp. 12-18.  
<http://www.computer.org/itpro/it2002/pdf/f3012.pdf>

- [5] *Naedele, M., Dzung, D. and Stanimirov, M.*: Network Security for Substation Automation Systems. In Computer Safety, Reliability and Security (Proceedings Safecomp 2001), LNCS 2187. Springer, 2001.
- [6] National Security Telecommunications Advisory Committee, Information Assurance Task Force: Electric Power Risk Assessment, March 1997.  
[http://www.ncs.gov/n5\\_hp/reports/EPRA/electric.htm](http://www.ncs.gov/n5_hp/reports/EPRA/electric.htm)
- [7] *Oman, P., Schweitzer, E. and Frincke, D.*: Concerns about intrusions into remotely accessible substation controllers and scada systems. Technical report, Schweitzer Engineering Laboratories, 2000.
- [8] *Palensky, P. and Sauter, T.*: Security considerations for FAN Internet connections. IEEE International Workshop on Factory Communication Systems, 2000.
- [9] *Pospisil, R.*: The next Y2K? Utilities IT, Jan/Feb 2000.
- [10] *Rigney, C., Willens, S., Rubens, A., Simpson, W.*: Remote Authentication Dial In User Service (RADIUS). RFC2865, June 2000.  
<http://www.ietf.org/rfc/rfc2865.txt?number=2865>
- [11] *Schneier, B.*: Applied Cryptography, Wiley, 1996
- [12] *Schneier, B.*: Secrets and Lies - Digital Security in a Networked World. Wiley, 2000.
- [13] *Schwartz, W.*: Time based Security. Interpact Press, 1999.
- [14] *Sherman, E.*: Terror's next target? - Networks - Critical U.S. information systems are full of holes that could be exploited by attackers living half a world away. Newsweek, 15 Oct 2001.
- [15] *Smith, T.*: Hacker jailed for revenge sewage attacks. The Register, 31 Oct 2001.  
<http://www.theregister.co.uk/content/4/22579.html>
- [16] *Spafford, G., Garfinkel, S.*: Practical Unix and Internet security, Reilly, 1996
- [17] *Waterbury, B.*: Let them in (Control Magazine, Oct 2001).  
[http://www.controlmagazine.com/Web\\_First/ct.nsf/Article1D/PSTR-52VL9L](http://www.controlmagazine.com/Web_First/ct.nsf/Article1D/PSTR-52VL9L)

## **Vita**

Dr. sc. techn. Martin Naedele arbeitet seit drei Jahren als Wissenschaftler und Projektleiter in der Abteilung für Informationstechnologie des ABB Forschungszentrums in der Schweiz. Seine Hauptarbeitsgebiete sind neue Softwaretechnologien und Softwarearchitekturen für industrielle Automatisierungssysteme. Sein besonderes Interesse gilt dabei dem Aspekt der Informationssicherheit derartiger Systeme. Dr. Naedele ist SANS/GIAC zertifizierter Auditor für die Sicherheit von IT Systemen und Netzwerken (GSNA).

Kontakt:  
ABB Schweiz AG, Corporate Research, Segelhof, CH-5405  
Baden, Schweiz  
Tel. +41 585868339,  
martin.naedele@ch.abb.com