Chapter 3

SECURITY ASSESSMENT OF A TURBO-GAS POWER PLANT

Marcelo Masera, Igor Nai Fovino and Rafal Leszczyna

Abstract Critical infrastructures are exposed to new threats due to the large number of vulnerabilities and architectural weaknesses introduced by the extensive use of information and communication technologies. This paper presents the results of an exhaustive security assessment for a turbo-gas power plant.

Keywords: Turbo-gas power plant, security assessment

1. Introduction

Enterprise systems that employ information and communication technologies (ICT) are prone to vulnerabilities that can be exploited by malicious software and agents. Considering the massive use of ICT in national critical infrastructures, it is imperative to perform comprehensive risk assessments that evaluate the main threats and the effectiveness of countermeasures.

Several approaches have been proposed for conducting risk assessments of ICT infrastructures (see, e.g., [1, 4]). The InSAW methodology [4–9] is specifically tailored to analyzing the impact of ICT threats on critical infrastructure assets. Dondossola and colleagues [2] presented the first practical test of the InSAW methodology. They applied an embryonic version of InSAW to analyze the vulnerabilities of a simple, albeit not actually deployed, remote control station.

This paper discusses the results of an exhaustive InSAW security assessment of the ICT infrastructure of a turbo-gas power plant. It also presents a set of ICT attack scenarios that have been successfully implemented in a laboratory environment. This environment, which was developed in collaboration with a major energy company, reproduces the networks, SCADA systems and electromechanical devices used in the turbo-gas power plant.

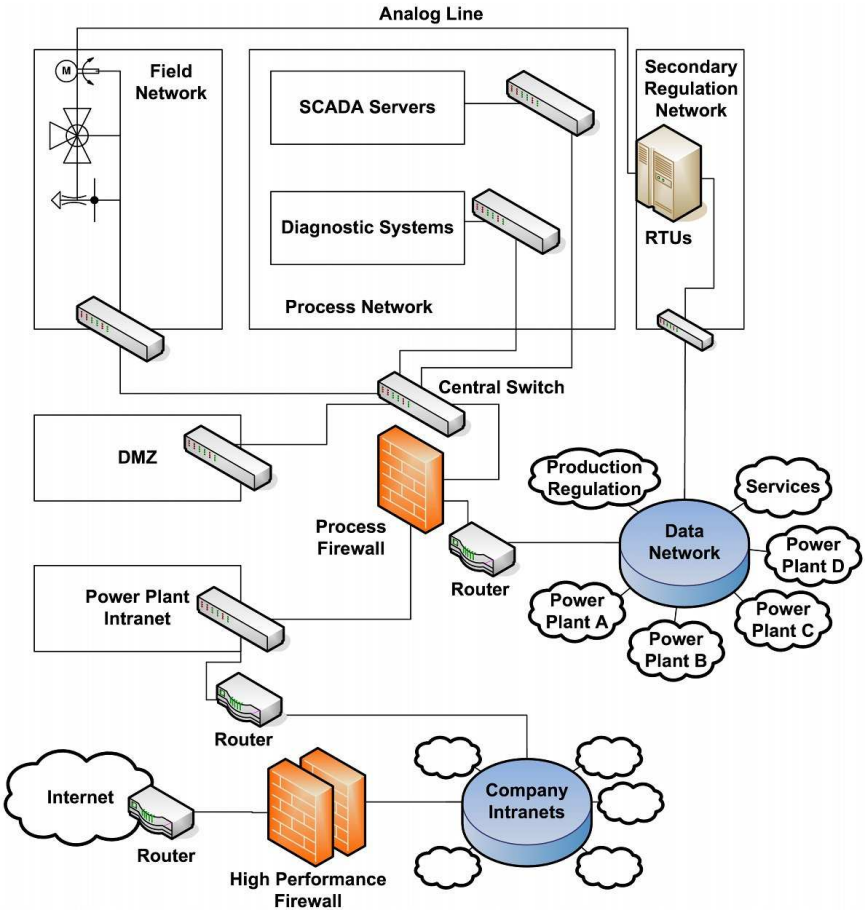

Figure 1. Power plant schematic.

2. System Description

In order to conduct a security assessment, it is necessary to model a complex system in terms of functional blocks. Since the focus is on threats derived from the use of ICT in a turbo-gas power plant, we focus on the networking aspects of the power plant architecture.

2.1 Network Architecture

Figure 1 presents the high-level architecture of the turbo-gas power plant. Several major subsystems are relevant from the networking perspective:

- **Power Plant Backbone:** This subsystem contains all the network devices that allow the various power plant subnets to communicate. The

principal devices include: (i) layer switches that manage traffic; (ii) process firewalls that separate and filter the traffic between the field network, process network and external entities; (iii) routers that interconnect various power plant subnets and the corporate intranet; and (iv) Internet firewalls that separate power plant company networks from the Internet.

- **Field Network:** This network interconnects the sensors and actuators that directly interact with power plant electromechanical devices.
- **Process Network:** This network hosts the SCADA systems used by operators to control power plant processes.
- **Demilitarized Zone (DMZ):** This area hosts data exchange servers that receive data from the process network and make it available to operators via the power plant intranet.
- **Secondary Regulation Network:** This network hosts remote terminal units (RTUs) that implement the secondary regulation protocol.
- **Power Plant Intranet:** This branch of the company network provides intranet services to plant operators. It is used for routine office activities as well as for remote plant control by providing access to the process network via a VPN through the DMZ.
- **Company Intranet:** This generic network, which typically uses Windows platforms, is used for all corporate activities. Note that "company" refers to the entity that owns and operates the power plant.
- **Data Network:** This high availability network is used to directly interconnect all company assets; it provides services such as DNS and antivirus software updates.
- **Internet:** This consists of all external computing assets.

2.2 Operational Flows and Dependencies

When analyzing a complex system, it is important to consider the operational flows generated by operator interactions with the system as well as the dependencies between the various subsystems. Due to a lack of space, it is not possible to discuss these in detail. Therefore, this section presents the operational flows and dependencies that are most relevant to the power plant attack scenarios considered in our work.

Field Network: The field network hosts all the devices (sensors and actuators) that are connected directly to the power plant hardware (e.g., gas turbine and steam system). The data flow uses dedicated communications protocols such as Modbus and Profibus. The field network devices are located on the "frontlines" of the ICT system; as such, they are vital to all power plant control operations. Thus, the device measurements and actions must be communicated to the higher control level (i.e., SCADA systems).

Process Network: The process network hosts the SCADA servers that interact with the field network. They analyze data received from the field network and present plant operators with summarized information about the state of the power plant. The operators use diagnostic systems, which exchange data with the SCADA servers, to investigate any anomalies that are observed. Based on the results of the analysis, an operator issues commands using the SCADA servers to devices in the field network to effect the appropriate changes to the state of the power plant.

Demilitarized Zone: The DMZ usually hosts a data exchange server. This server receives plant status data from the SCADA servers. Operators connected to the power plant intranet query the server to obtain high-level information about plant operations without having to access the process network. Remote access to the DMZ and to the process network is regulated by a properly-configured firewall, which also operates a point-to-point VPN (over Radius). Thus, only authorized operators can remotely access the DMZ and process network. Note, however, that traffic flow between the various servers is generally not authenticated.

Remote Terminal Unit Network: The RTU network receives power production data from the data network. The RTUs communicate directly with devices in the field network using a dedicated analog channel. Note that no mutual authentication is implemented between the RTUs and field network devices.

Intranet: The power plant intranet is typically a part of the company intranet. In our case study, the intranet uses Windows platforms with a strong set of security and access control policies. Operators connected to the intranet can establish VPN connections with the process firewall in order to access the process servers and DMZ servers. The operators can also access the Internet via the intranet.

Data Network: The data network connects all the power plant's process networks to facilitate fast data transfer over a private network. It also provides services such as DNS. Several flows exist between the process and data networks. The data network is also used by operators to send commands to the RTU network required for production operations and secondary regulation.

Internet: The Internet represents the external world, i.e., everything outside the company network. However, in our case study, public communication channels are used by remote operators to connect to power plant assets (e.g., for maintenance purposes). This uses Radius authentication over a site-to-site VPN network. Thus, remote operators appear virtually as "internal operators." Data flows between the intranet and Internet materialize whenever an internal operator conducts Internet-related activities. Note that Internet access policies

are role-dependent: some operators are allowed to directly access the Internet while others have to pass through a set of proxy servers.

3. Vulnerability Analysis

Based on our security assessment methodology [8], we attempted to identify all relevant vulnerabilities before postulating attack scenarios. Our analysis identified several vulnerabilities, which we have organized into three classes:

- **Architectural Vulnerabilities:** These vulnerabilities directly derive from weaknesses in the network architecture. Example vulnerabilities include weak separation between the process and field networks; lack of authentication between active components (actuators and SCADA servers, actuators and RTUs, SCADA servers and data exchange servers, etc.); and the process firewall itself, which is a single point of failure.
- **Security Policy Vulnerabilities:** These vulnerabilities arise from weak security policies, especially related to users who remotely connect to the intranet (e.g., the machines used by remote users may not have the latest security patches and anti-virus protection). Other vulnerabilities are due to ambiguous traceability and access policies.
- **Software Vulnerabilities:** Several operating systems are used in the power plant: Linux, SCO Unix, Windows NT, Windows 2000 Server, Windows XP and Windows 2003 Server. Most of these systems did not have the latest patches and some unauthorized applications were installed. In all, we identified 240 software vulnerabilities that affected computers, servers, switches and routers. At least 100 of these vulnerabilities could be used to seize partial or complete control of the targeted machines. Moreover, more than 70 vulnerabilities could be exploited to block machines.

The results of the vulnerability analysis are not as dramatic as expected. In fact, very few of the identified vulnerabilities could be exploited to launch serious attacks. Nevertheless, the presence of these vulnerabilities highlights how the extensive use of ICT has significantly increased the number of possible "failure" scenarios.

4. Threat Analysis

The threat analysis component of the power plant study identified the potential threats starting from a list of typical hazards. The threats that were deemed to be the most effective were examined in greater detail. The results were then synthesized and the corresponding threat profiles and exposure indices developed. The following three phases were involved in the threat analysis:

- **Threat Hypothesis:** The threats are characterized according to their type (internal/external), agent (person/object), motivation (intentional,

accidental, etc.), expertise and resources (required to manifest the threat), perceived value, plausibility and severity.

- **Threat Verification:** The identified threats are screened according to the risks they might pose to the system.

- **Threat Value:** The plausibility and severity values are qualitatively estimated for each threat.

Note that the "plausibility" of a threat is the likelihood of the existence of the menace that targets a certain vulnerability to produce damage to the system. The "severity" of a threat is the capacity to produce damage by exploiting a certain vulnerability.

No generally accepted definition of a threat exists. From the legal point of view, a threat by an agent is an unwanted (deliberate or accidental) expression of intent to execute an action that may result in harm to an asset. Therefore, a threat is the potential occurrence of a negative action, not its actual realization. The following is a generic list of threat agents that can jeopardize critical infrastructure assets [10]:

- **Crackers, Malicious Hackers, Script Kiddies:** These individuals, who have varying levels of technical expertise, break into systems by subverting security mechanisms. They may launch attacks for the challenge or thrill of doing so, or for bragging rights in their communities.

- **Insider Threat:** The disgruntled insider is a major threat. An insider may not have a great deal of knowledge about computer intrusions, but his knowledge of and access to the targeted system enables him to cause considerable damage.

- **Malware Writers:** Malicious code writers produce software (viruses, worms or Trojan horses) designed specifically to damage or disrupt systems. This so-called malware can be specific (i.e., it targets particular systems or organizations) or it can be generic.

- **Criminal Groups:** Criminal groups frequently attack systems for monetary gain. They may attempt to steal sensitive information for re-sale or for purposes of blackmail, extort money by threatening to attack computing assets, and commit various types of fraud (e.g., attempting to influence stocks) or forgery (e.g., changing payment information in invoices).

- **Hacktivists:** Hacktivism refers to politically-motivated attacks on computing assets. Hacktivists may overload e-mail servers or hack into web sites to send political messages. Their actions against infrastructure assets are usually motivated by environmental, safety or nationalistic reasons.

Table 1. Principal threats.

Threat	Expertise	Resources	Value	Plausibility	Severity
Insider	Minimum	Limited	High	Medium	High
Int. Malware	Medium	Limited	Minimum	High	Low
Ext. Malware	High	High	Maximum	Low	Low
Hackers	Medium	Limited	Maximum	Medium	High
Criminals	High	Very High	Maximum	Medium	High

- **Terrorist Groups:** Terrorism is the unlawful use of force or violence against persons or property in order to intimidate or coerce a government or civilian population to further certain political or social objectives.

- **Information Warfare:** Several nations are aggressively developing information warfare doctrines, programs and capabilities. These capabilities can be used to disrupt the supply chain and inflict considerable damage to the various infrastructure sectors, ultimately affecting the economy and the residents of the targeted region or country.

The threats we have identified are presented in Table 1. The plausibility and severity values assigned to the threats were based on detailed analyses of power plant systems and on interviews conducted with plant operators and managers. For example, under normal conditions, the severity of an insider threat (disgruntled employee) is very high if the individual has direct access to the process network and to the SCADA systems. On the other hand, even if the plausibility of a malware infection is high, its impact on the power plant "core" (i.e., field network) is low. This is because the computing systems in the field network are less vulnerable to traditional viruses – they run dedicated services and use proprietary protocols; even if the systems are compromised, it is possible to bypass them and control the power plant manually. Of course, the evaluation scenario has to be modified if advanced viruses that specifically target power plant systems are introduced. Likewise, the severity of a hacking attack is high because a hacker (hypothetically) can seize control of critical systems. The same argument holds in the case of attacks launched by criminal groups.

5. Attack Scenarios

This section presents a high-level description of the attack scenarios that we identified and implemented. The purpose is to give an idea of the level of exposure faced by a typical power plant.

5.1 Radius Server Denial of Service

Denial-of-service attacks limit or block access to specific resources, making them, and possibly a larger system, unusable. In this scenario an attacker attempts to consume the bandwidth of a Radius server that is connected to the Internet.

The first step is to perform system fingerprinting, where information is collected about a target system. Since the Radius server is connected to the Internet, it is relatively easy to obtain information about it by analyzing the results of network scans, ICMP packet content, etc. Information about the targeted system can also be obtained using social engineering techniques on employees and other individuals familiar with the system and its configuration.

Bandwidth consumption is a simple task: an attacker directs large volumes of traffic to the targeted server. This is accomplished by compromising a sufficient number of machines connected to the network and using them to generate attack traffic. Our scenario involves a dedicated Trojan horse that propagates itself on networks and compromises machines, installing a backdoor in every compromised machine. The attacker uses the backdoors to seize control of the machines and proceeds to establish a "zombie network" for launching distributed denial-of-service attacks. Using the zombie network and the information gleaned from system fingerprinting and social engineering, the attacker blocks all external access to the company intranet and, thus, external access to the power plant network.

5.2 Intranet Virus Infection

In the virus infection scenario, the attacker gains control of a computer in the corporate intranet in order to impersonate a legitimate user. The infected computer is directed to perform malicious actions on critical plant networks, such as launching denial-of-service attacks on the process firewall or data exchange server, or corrupting diagnostic systems or SCADA subnets. Virus infections potentially affect all systems that are connected to an open network. Anti-virus software is the primary defensive mechanism, but even systems with the latest software are vulnerable to attack in the interval between the release of a new virus and the time the next patch is released.

The first step of the attack is to collect information about the target system (e.g., using system fingerprinting). Next, the attacker obtains a new virus that is tailored to the targeted system. It is assumed that the attacker has the expertise to write such a virus or is able to obtain the virus from the hacker community.

If the attacker has already gained access to the targeted machine, the virus can be directly installed on the machine. Alternatively, the attacker exploits a vulnerable service at an open port on the firewall or uses social engineering to convince a legitimate user to install software containing the virus.

If the virus has been designed with a backdoor, the attacker can gain control of the infected machine and impersonate a legitimate user, performing

authorized actions as well as illegal actions that may be permitted by deficient security policies. Note that control of the compromised machine is easily maintained if the attacker is an insider. However, an external attacker would have to penetrate the firewall to reach the infected machine and perform the malicious actions. This poses an obstacle, but it is possible to create a virus that performs the malicious actions autonomously.

The virus attack can be used to cause damage to the data exchange server and the SCADA servers. Also, it could be used to steal credentials (user names and passwords) or deny service to the power plant firewall and other computing assets. Note that the virus infection scenario is developed for the intranet environment. A similar scenario may be devised for the data network, DMZ or process network. For example, if the infected machine is in the data network, which connects all power plant assets, it is possible to conduct a denial-of-service attack on the RTU network and disrupt the secondary regulation protocol.

5.3 Phishing Attack

In the phishing attack scenario, the attacker steals the credentials of an authorized user in order to target the power plant network. A phishing attack may send a fake e-mail message, display a seemingly legitimate link that actually connects to a malicious website, or poison the DNS server to make the victim connect to a malicious server.

In our scenario, the attacker has to replicate at least a portion of the system interfaces and infrastructure, e.g., by creating a fake domain and a data exchange server for data distribution. Information required to create the fake site that replicates system interfaces and infrastructure can be obtained via system fingerprinting. Once this is done, the attacker collects information on users and systems, including DNS data. This enables him to implement a DNS poisoning attack that re-routes users to the fake website instead of the data exchange server. The fake website provides false information about the state of the power plant and also captures their credentials, making it possible for the attacker to connect to the real data exchange server.

6. Conclusions

The security assessment of the operational power plant clearly demonstrates that ICT introduces a large number of vulnerabilities. Our experiments involving a laboratory testbed that reproduces much of the ICT infrastructure of the power plant verify that the ICT attack scenarios are feasible and can be very damaging. In particular, our use of a malware simulation framework [3] has enabled us to investigate the serious impact of virus infections on power plant safety and security.

Sophisticated analytic tools are required to identify and address the myriad security problems. Our use of the InSAW methodology in the analysis process has facilitated the identification of failure-prone relationships in power plant

subsystems; this has helped discover weaknesses, create realistic attack scenarios and understand the potential cascading effects of failures. Still, our work is merely the first step in a systematic campaign to address the impact of ICT vulnerabilities on critical infrastructures. Our future research will investigate vulnerabilities in SCADA communication protocols and architectures with the goal of articulating effective security policies and countermeasures.

References

[1] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE (SM) Approach*, Addison-Wesley, Boston, Massachusetts, 2002.

[2] G. Dondossola, J. Szanto, M. Masera and I. Nai Fovino, Effects of intentional threats to power substation control systems, *International Journal of Critical Infrastructures*, vol. 4(1/2), pp. 129–143, 2008.

[3] R. Leszczyna, I. Nai Fovino and M. Masera, MalSim – Mobile agent malware simulator, *Proceedings of the First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, 2008.

[4] M. Masera and I. Nai Fovino, A framework for the security assessment of remote control applications of critical infrastructures, *Proceedings of the Twenty-Ninth ESReDA Seminar*, 2005.

[5] M. Masera and I. Nai Fovino, Emergent disservices in interdependent systems and systems-of-systems, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 1, pp. 590–595, 2006.

[6] M. Masera and I. Nai Fovino, Models for security assessment and management, *Proceedings of the International Workshop on Complex Network and Infrastructure Protection*, 2006.

[7] M. Masera and I. Nai Fovino, Through the description of attacks: A multidimensional view, *Proceedings of the Twenty-Fifth International Conference on Computer Safety, Reliability and Security*, pp. 15–28, 2006.

[8] I. Nai Fovino and M. Masera, A service-oriented approach for assessing infrastructure security, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 367–379, 2007.

[9] I. Nai Fovino, M. Masera and A. Decian, Integrating cyber attack within fault trees, *Proceedings of the European Safety and Reliability Conference*, 2007.

[10] United States General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report GAO-04-354, Washington, DC (www.gao.gov/new.items/d04354.pdf), 2004.