EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE

CERN - TS Department

EDMS Nr: 473732 TS-Note-2004-021
Group reference: TS-CSE 4 May 2004

IMPROVING INDUSTRIAL PROCESS CONTROL SYSTEMS SECURITY

U. Epting, M.C. Morodo Testa

Abstract

System providers are today creating process control systems based on remote connectivity using internet technology, effectively exposing these systems to the same threats as corporate computers. It is becoming increasingly difficult and costly to patch/maintain the technical infrastructure monitoring and control systems to remove these vulnerabilities. A strategy including risk assessment, security policy issues, service level agreements between the IT department and the controls engineering groups must be defined. In addition an increased awareness of IT security in the controls system engineering domain is needed. As consequence of these new factors the control system architectures have to take into account security requirements, that often have an impact on both operational aspects as well as on the project and maintenance cost. Manufacturers of industrial control system equipment do however also propose progressively security related solutions that can be used for our active projects. The paper discusses the impact of these issues on the process control system for the air handling of the LHC tunnel and its underground areas. It describes a technical evaluation of different solutions and the associated costs.

Presented at the TS Workshop
Archamps, France, May 4 – May 6, 2004

1 INTRODUCTION

Control systems are used all over CERN and are constantly exposed to security issues. This paper describes in two parts the different security threats and gives an example on how to incorporate the illustrated guidelines in the *LHC underground areas ventilation control system* project. It should not be read as complete risk assessment study but serves as more general example for similar projects.

2 SECURITY PROBLEMS

Every computer system connected to a network is exposed to security risks. These risks need to be evaluated in order to minimize data loss, data manipulation or any malfunction of the system. At CERN a large part of the control systems are connected to the internal network (Intranet) and therefore need to be protected against all kind of risks.

2.1 Threats

Threats are usually distinguished in two main types: accidental attacks and malicious attacks. Accidental attacks may usually be solved by establishing clear procedures or easy protection schemes. Malicious attacks require more investment in terms of time and money and mostly cannot be solved to 100%.

2.1.1 Human errors

These are usually problems in case of inaccurate administration or configuration of systems, like configuring the wrong hardware or shutting off servers that are still needed by another system. This kind of problems can usually be solved by a rigorous login/password scheme, clear procedures and printed instructions close to the consoles. In case of remote access to machines, these should be configured with a unique password access that is different on each machine so that mistyping becomes unlikely.

2.1.2 Security scans

Some (usually older) systems have no or little protection against network disturbances. Sometimes simple network port scans block the access to the network and require a reboot of the server. The TS department has an agreement with the IT department, that these vulnerable machines are excluded from security scans. But as free port scan software is installed on almost every PC and may be used by every user, this causes sometimes serious problems when non qualified users run these scans on the CERN technical network.

2.1.3 Aggression

Aggression covers human attacks to a system by using stolen or guessed logins/passwords in order to disturb or stop a service. In the TS department no case of this kind of attack is known from inside CERN until now. With expanded visibility of control systems outside CERN this kind of threat will very probably increase in the future. Thus a sophisticated password mechanism is required for future control systems.

Another type of aggression is the manipulation of the hardware itself, either by switching off equipment or disconnecting it from the network. This can only be protected by putting important equipment in locked spaces or racks.

2.1.4 Viruses

Viruses or worms are automatically distributed software items that may disturb services very seriously. This kind of software is usually activated by ill reflected installation of unknown software packages or running unknown executables. Once a virus is launched, it has access to all badly protected systems running on the network. Damage may range from the manipulation of the data on a single machine up to a denial of service attack on a complete network segment. To avoid viruses and worms, recent anti-virus software has to be installed and initiated regularly.

3 HARDWARE

This chapter gives an overview of the most common hardware used at CERN for control systems in the TS department.

3.1 Servers

These machines are mainly used to serve files or applications to a variety of systems. The operating system is usually UNIX based (Solaris, HP-UX, Linux) and important services should use redundant servers. Problems with a server very often result in the loss of a complete service, like the non-availability of the alarm system or complete databases. Servers are very often the most critical part in a control system and thus need an appropriate design and protection scheme.

3.2 PCs

Local controls are often done by PCs running a windows flavour (NT, 2000, XP ...) or Linux. As Windows is widely used and the biggest parts of viruses are known for the Windows world, these systems have a big risk of being infected by viruses if not properly protected. Frequent operating systems updates and patches need to be applied in order to protect the installations effectively.

3.3 PLCs

Industrial Programmable Logic Controllers (PLCs) are used to control systems at processes level. PLCs are usually very robust and do not need a lot of maintenance once they are put in operation, but on the other hand do not have any sophisticated protection against network access. The PLC manufacturers started looking into security issues lately and first protection schemes should be available already this year. Today PLC protection is only guaranteed if used on a separated and isolated network.

3.4 I/O cards

Standard I/O cards are usually either connected directly to the PLCs or via specific hardware buses and protocols. In these cases security risks are very low. If I/O cards are connected directly to the Ethernet they are exposed to the same risks as PLCs.

4 NETWORK

This document covers only the CERN Ethernet installations. Other networks like Profibus or Modbus are considered as private (sub-) networks and thus are not really exposed to external security risks.

4.1 Ethernet

Today Ethernet is able to transport a variety of network protocols. The widest used is TCP/IP. Different protocols and applications talk to different ports on the servers. Each port is an entry point to the system and thus bears a potential security risk.

4.2 Technical vs. General Network

The networks at CERN are divided into two parts: the general services network and the technical network. The general services network provides network access to everybody and any computer on the CERN site. It is accessible from outside CERN and is frequently used for different attacks from outside. This network is used for standard applications that are not safety critical or otherwise important for CERN's controls.

Safety systems and other important systems should be connected to the technical network. This network has the same technical characteristics as the general service network, but is not visible from outside CERN and thus provides a first level of security against outside attacks. But as the technical network is currently visible by the CERN general service network, one infected machine could be enough to infect also safety critical servers.

4.3 Accessibility and Passwords

Access to all machines and services on the network is usually granted by using a login and password. Lately CERN forced the users to use encrypted mechanisms like ssh and sftp when connecting to

CERN servers to avoid sending clear passwords over the network and thus delimiting password spying mechanisms. But this method does not protect against unauthorized access if passwords are easily guessable or if group accounts with common passwords are used.

As the networks are closely connected together, all machines are somehow interconnected. In order to protect different services a separation in dedicated network segments is necessary. These segments are protected by specific entrance doors, so called firewalls. Firewalls must be configured in such a way, that only recognised machines and services may access the equipment in the network segment.

5 GUIDELINES

CERN computer users agree with their signature for the account creation request to accept some basic computing guidelines. The most global ones describe the rules for the use of the CERN computing facilities and are available in Operational Circular nº 5.

5.1 CERN Operational Circular No. 5

The use of CERN's computers, networks and related services, such as e-mail, are governed by Operational Circular nº 5. This circular describes, in somewhat legalistic language, the rules and conditions that apply to the use of CERN's computing facilities. In addition, provisions are made for computing services to indicate additional "rules of use" that are needed to maintain a level of service compatible with expectations. The document is accessible at http://cern.ch/ComputingRules/.

5.2 Security Guidelines

A dedicated web page (http://cern.ch/security/) gives an overview of the basic security issues at CERN. It covers items like:

- forbidden software
- security recommendations like passwords, ftp access, ssh access, etc. and a variety of links to other security related sites.

In principle each exposure of a system on the network bears a security risk and thus should be avoided wherever possible.

5.3 Control systems issues

Control systems are meant to be either safety critical or otherwise very important and should never be stopped in an uncontrolled manner. In order to protect these systems from the above mentioned risks, a universal strategy was proposed by a control system security specialist:

a) Review Safety Critical Systems

Any control or emergency systems should be reviewed as a high priority to understand any Health and Safety risks.

b) Awareness Campaign

Designers, users and operators of control systems at CERN need to be made aware of

- Cyber security risks
- Possible impacts of those risks
- Where to get assistance
- What to do and what not to do
- Remedial actions
- Any standard solutions that are available (e.g. AV packages, firewalls etc.)

Senior management need to be made aware of the risks issues and impacts.

All equipment groups need to be committed and made aware of the issues.

A website could be created as the one stop shop for process control security with information, contacts and resources.

c) Governance Board

- Clear governance needs to be established for process control security risks. This may be the Controls Board however this role will need to be clarified with senior management and other groups.
- Other key parties (e.g. the experiments) should name a representative as the single point of accountability for these risks and these representatives should attend the governance board meetings.
- A Process Control Security Policy should be developed in parallel with standard solutions (see below).

d) Enabling Services

Investigation should be carried out into developing some 'standard' solution packages for process control security. Examples are:

- Network Segregation
- Investigation should be carried out into methods for segregating networks. There may be many possible solutions to this (firewalls, vpns, tunnels etc.) which could form a toolkit for protecting critical systems and segregating the experiments - effectively forming different security zones.
- The effective segregation of the campus and the controls network should be a high priority.
- WTS services for remote access (Windows Terminal Server)
- Firewall information and procurement (e.g. access to personal firewall & configuration information etc.)
- Vulnerability information
- Security monitoring and intrusion detection and prevention.

e) Vendor Engagement

The key vendors should be identified and engaged. Security vulnerability information and best practice guidance should be requested. Also security clauses should be included in support and procurement contracts.

f) Project Engagement

The key projects need to be committed to ensure they are implementing an adequate security model as this is so much easier and cheaper to build in at the design stage rather than trying to bolt on security at a later date.

g) Response Capability

The existing notification mechanism should be updated and enhanced to cover all system owners and administrators.

6 STRATEGIES

In the frame of the *LHC underground areas ventilation control system* these guidelines for protection against unauthorised accesses have been evaluated as a continuous learning process and consist of the following phases:

1. Understand the Risk

Risk assessment is the starting point to whatever action oriented towards security improvements. An analysis of the particular control system, the threats that apply to it and the impacts that these threats could produce on the performances, allow understanding the system vulnerabilities.

It is only from the understanding of the system vulnerabilities that an efficient evaluation of the security improvements which should be applied can be undertaken.

2. Implement Security Improvements

Once the vulnerabilities of the system have been identified and their effects understood, it is the moment of evaluating the security improvements actions. These corrective actions can be classified in two groups, depending on the time scale in which they become effective.

In first term, there are the "*Quick Win*" improvements, which are simple actions generating an immediate effect. An example of "quick win" improvement is to eliminate the non-critical network connections in a control architecture, as a modem connection or similar.

Finally, there are the "*Long term*" improvements, which include either complex actions or the modification of the present practices and procedures. This kind of improvements, which require a longer implementation period, need to be carefully studied and planned and are at the origin of sensible long term benefits. Examples of this "long term" improvements are the formal definition and implementation of patch management and user access rights policies.

3. Establish Security Governance

Once the vulnerabilities of the critical systems have been analysed and identified, and the required security improvements are implemented, next priority is the establishment of Security Governance for the Organization. Security Governance includes full definition of Policy and Standards, which should be considered as a continuous assurance process, in a similar way than Quality or Safety. It is worthwhile to remark that no international standard exist for Security Governance of an Organization. At the time being, each organization needs to define its own Security Governance.

4. Establish Response Capability

Response Capability needs to be measured and documented, in order to trace the performances and identify deviations in relation to the targeted goals.

5. Raise Awareness and Skills

Internal communication and training, also as a continuous process, are mandatory in order to obtain and maintain the benefits in a long-term scale.

6. Manage third party risks

External communication to vendors, support organizations and industrial partners, with the purpose of involving them in the Security Improvements and obtain their engagement.

7. Engage projects early

Security aspects built-in as an essential requirement from the control systems design.

7 CASE-STUDY: LHC UNDERGROUND AREAS VENTILATION CONTROL SYSTEM

Much of the LEP underground air-handling equipment will be re-used for the LHC underground areas. These installations were commissioned in 1985 and were fully operational up to the closing of the LEP accelerator at the end of the year 2000. The associated process control and supervision equipment has become obsolete since the LEP construction period and need to be upgraded. Migration concerns a volume of 91 PLCs distributed all over the LHC site. Most of these PLCs (approx. 70%) are located in the surface buildings. The remaining PLC's are installed in different underground locations [R4].

In addition, new civil engineering structures have been excavated along the main LHC tunnel for which air conditioning units will be installed. Process control and supervision of the new installations need to be coherently integrated with the existing in a unique control system architecture. New process control equipment includes a volume of twelve PLCs and 125 micro-PLCs, all of them in LHC underground areas [R5, R6].

In this context, a global software engineering, which will provide a homogeneous approach to fulfil the functional considerations arising from the new LHC operating conditions, is unavoidable and must be considered as intrinsic to the design and execution of the hardware renewal and extension project.

Communication issues are a key factor in such a scenario, where a process characterised by a very high geographical dispersion needs to be perfectly coordinated in order to assure the requested functional performances and safety requirements. Several technical options are presented. Final assessment represents a compromise between openness to remote connectivity, which is essential for operational purposes, and engagement to the design and implementation of a *secure* control system, as in the present context and making use of the industrial technologies available in today's market. Finally, the full picture of the project definition needs to include the allocation of the project execution phase inside the global LHC schedule, constraint that is incorporated into the feasibility and risk analysis and that has an impact on the technical choices.

7.1 Technical options

Figure 1 shows the control architecture of the tunnel and underground structures ventilation in a generic LHC point.

From the communications point of view, two options are analysed. The first one consists in connecting every process controller, slave PLCs and micro-PLCs, to the CERN TCP/IP Technical Network, as well as the local supervision equipment, master PLCs and SCADA on PCs. The second one consists in using a dedicated industrial fieldbus for communication related to process control, regulation and local operation, using the CERN TCP/IP Technical Network for remote monitoring and operation only.

The first option presents the advantage of providing full remote openness and accessibility to each of the control components in the architecture. But full openness can be also its main disadvantage, since it implies that any of the 103 PLCs and 125 micro-PLCs directly performing the process control and regulation functionality is exposed to the threats described in 2.1. Consequently, the feasibility and risk analysis shows a very good evaluation on system openness, which eases system integration and future evolution, but raises the alarm in terms of functional safety, which can not be properly assured in the present context.

The second option limits the TCP/IP accessibility. The process control and regulation layer is uncoupled; all the slave-slave and master-slave dialogues use a dedicated industrial fieldbus, type Profibus DP. At any LHC point, every process control PLC or micro-PLC can be remotely accessed through the fieldbus. Therefore, this configuration maintains a degree of openness to the process control and regulation layer, but introducing some restrictions: fieldbus connection sockets are only physically accessible inside the process control cubicles or cabinets, and a computer supporting the PLC dialogue software needs to be used. Remote operation is performed through the master PLC, which at each LHC point becomes the only open door to the process control layer from the CERN TCP/IP Technical network. The feasibility and risk analysis shows this time just a good evaluation on system openness, but the functional and safety vulnerability to network security threats is strongly reduced.

In this configuration, only supervision and concentrator PLCs, which are not directly governing the local ventilation processes, are exposed. Also, impact on functional safety in the event of an attack is significantly reduced because local processes, which are uncoupled from the TCP/IP network, are designed for stand-alone operation in the event that their master PLC is lost. Furthermore, the limited number of PLCs connected to the TCP/IP network allows protecting them from unauthorised accesses, at least up to some extent. A list of authorised addresses will be configured in the TCP/IP communication processor[1] of each PLC. Connection requests from unauthorised addresses will be rejected.

[1] This feature is not available for all the SIMATIC S7 TCP communication processors (CP). The master and concentrator PLCs shall be equipped with CP supporting it.

7.2 Operational Aspects

The use of a dedicated Profibus DP fieldbus in the process control and regulation layer implies that accessing a process control PLC is not possible from the CERN TCP/IP Technical Network. In order to avoid that this limitation can become a constraint to operational features, either local or remote, the following provisions are considered.

7.2.1 Local operation

Local operation refers to manual or automatic control from the LHC ventilation control system platforms, for a given LHC point. Three human-computer interfaces (HCIs) are proposed:

1. Each process control PLC or micro-PLC is equipped with an operation panel, touch panel type for PLCs and display type for micro-PLCs. This operation panel is fitted in the front-door of the control cubicle or cabinet.
2. At each LHC point, local operation of every unit is also possible from the SCADA application platform located in the SU building.
3. Finally, local operation of every unit is possible from a laptop computer supporting the PLC dialogue software connected directly to the PLC, or through the fieldbus which links all the process PLCs at each LHC point. This option is only intended for control system troubleshooting, and maintenance operations performed by process specialists.

7.2.2 Remote operation

Remote operation refers to automatic control from the CCC remote monitoring system. In order to improve the reliability and availability of the communication and dialogue, the TIM system interfaces exclusively with the master PLCs. All data exchange through the SCADA application on PC is avoided in the design. The master PLC database is designed so that it makes available all the relevant process information to the CCC.

Several synthesis alarms are foreseen to be available as potential-free outputs at the master PLC of each LHC point. These alarms offer a hardwired path to the TIM multipurpose monitoring devices (MMDs).

The mimic diagrams available on the SCADA application are web-published for information of the operation teams, both CCC and TS/CV. No remote operation is allowed through this remote operation tool.

7.3 Assessment

The following control architecture is proposed for the LHC tunnel and underground areas ventilation control system.

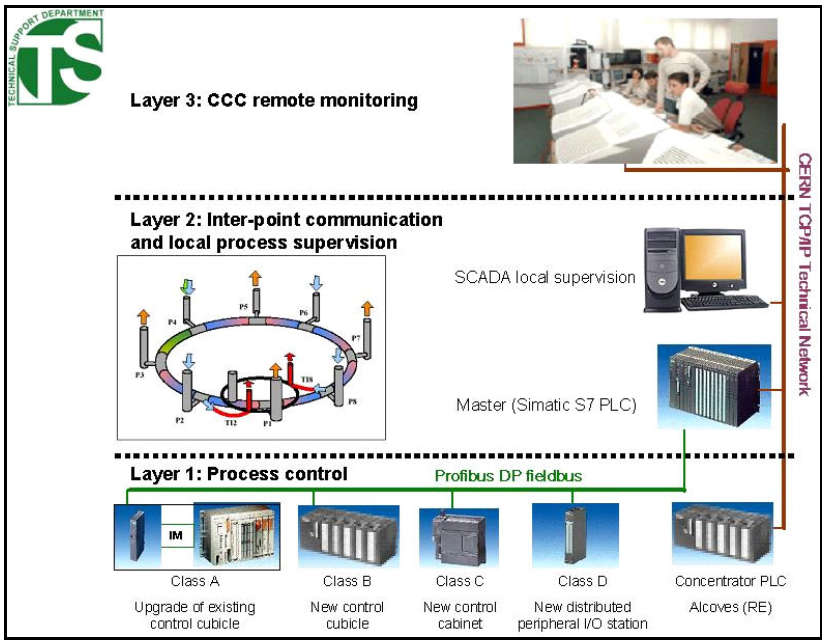

Figure 1. Control architecture of the tunnel and underground structures ventilation in a generic LHC point

Layer 1

At the process level multiple slave PLCs, (or micro-PLCs, depending on the size and complexity of the controlled installation), all of them Siemens SIMATIC S7 make, connected on a Profibus DP fieldbus, execute the start-stop control sequences, closed-loop regulation and alarm handling for the ventilation equipment that is located both in the surface and in the underground areas. Local operation HCIs are made available at each control cubicle or cabinet.

Layer 2

A master PLC, also Siemens SIMATIC S7, collects the data from all the local process PLCs. More particularly, it allows the communication with the ventilation equipment located at different LHC points, and also with the CERN Central Control Room (CCC). The master PLC is connected both on the Profibus DP fieldbus for master-slave communication and on the CERN TCP/IP Technical Network. HCI (Human Computer Interface) functionality is provided by a SCADA application on PC.

Layer 3

CCC remote monitoring system integrates all the data coming from the different systems such as cooling, air conditioning, electric power distribution, control and safety systems, etc. The technical infrastructure monitoring (TIM) system accesses the LHC tunnel and underground ventilation data directly at the master PLC, through the CERN TCP/IP Technical Network and by the means of a TIM standard software interface. SCADA applications' mimic diagrams are web-published for remote information to the operation teams.

8 CONCLUSION

Recent events show that computer security issues are becoming a serious problem also at CERN. Some guidelines seem to be obvious and can be applied straightforward for improving computer security in control system projects. Usually these "*quick win*" solutions do not require major investments but have to be considered already in the design phase.

The long-term solutions to the problems presented will require clear CERN wide guidelines and regulations for the implementation of control systems. This requires a general investment in security governance that is usually outside the scope of most control system projects. A strategy to keep the systems up-to-date in terms of security must be settled from the beginning and a continuous follow-up

is necessary to ensure secure operation and maintenance with the available and often limited resources.

REFERENCES

[1] CERN Computer Security Information - http://cern.ch/security/

[2] Operational circular No. 5

[3] Consulting on security issues by Justin Lowe, PA consulting

[4] Migration of the Process Control System for the LEP Ventilation into the LHC Configuration, Engineering Design Review, EDMS Document No. 457600

[5] Engineering Specification, Air-handling of the LHC tunnel and its underground areas, LHC-UA-ES-0001 rev. 2.0, EDMS Document No. 344211

[6] IT-2795/TS/LHC Invitation to Tender, Technical Specification for supply, installation and modification of air-handling systems for the LHC

[7] CERT® Coordination Center - http://www.cert.org/