COMPUTING AND NETWORK INFRASTRUCTURE FOR CONTROLS (CNIC)

Uwe Epting on behalf of the CNIC working group

CERN, Geneva, Switzerland

ABSTRACT

Recent events show that computer security issues are becoming a serious problem also at CERN. Control systems for the operation of the LHC, its injectors, experiments as well as the technical infrastructure rely on the application of defined management procedures, correct operating system maintenance as well as on safe network communications. A internal survey showed that significant changes would be required in these areas in order both to deal with security concerns as well as to provide clear lines of responsibility.

Also, for system support, unlike desktop services where a "one-size-fits-all" approach is appropriate, it has been determined that substantial customization is required for computers used for control systems, especially to deal with security issues. Thus, a new, CERN-wide working group, CNIC, was created with the mandate to propose and enforce that the computing and network support provided for controls applications is appropriate. CNIC defines the required policies and management structures and follows up the implementation of appropriate tools. The members of the working group jointly cover all users of computers in controls environments at CERN.

This paper shows the approach of handling security issues in control environments at CERN as well as the first results that could be obtained so far.

INTRODUCTION

Computer control systems for the operation of the LHC, its injectors, the experiments, as well as the technical infrastructure, rely on the application of defined management procedures, as well as correct operating system maintenance and safe network communications. This requires coordination and clear rules and definitions for the setup and use of control system equipment at CERN. These rules must cover the general CERN policy in matters of security, and the logical network structure. They also define what can be physically connected to the secured networks and the procedures that have to be applied to achieve this. Another important subject is the installation and maintenance of the operating systems and security patches, as well as which services are required to ensure 24/7 operation.

The document outlines the aim of the working group, overall security policy, necessary tools and services and shows the way how this working was organised.

THE CNIC MANDATE

In the initial phase of the working group it should draw up a detailed plan of work and a corresponding set of milestones. At least the following points should be covered:

- Tools for system maintenance.
- Tools for setting up and maintaining many different Controls Network domains. A domain is defined to be a collection of systems under a single management responsibility.
- Rules and policies for what can be connected to a domain and an authorization procedure. For example, this should cover wireless communications and portable computers.
- Ground rules, policies and mechanisms for inter-domain communications.
- Ground rules, policies and mechanisms for communications between controls domains and the Campus Network (and hence the Internet).
- Document all domains of use and in each case obtain from the group(s) concerned the name of the person designated to have technical responsibility, the person with hierarchical responsibility for giving the necessary authorization and their backups.
- Investigate with help from IT/CS what technical means could be provided to ensure the defined policies are complied with, and propose an implementation plan.

During Phase II the previously defined programme of work will be implemented. When complete, policy documents it defines should be circulated for review by the Controls Board and finally endorsed by the CERN Executive Board.

After the previous phases have been implemented, Phase III should cover long-term operation and review possible changes and the effectiveness of the policies and methods in real operation. The membership of the W.G. should be expanded to include the domain managers in order that their views and feedback can be taken into account.

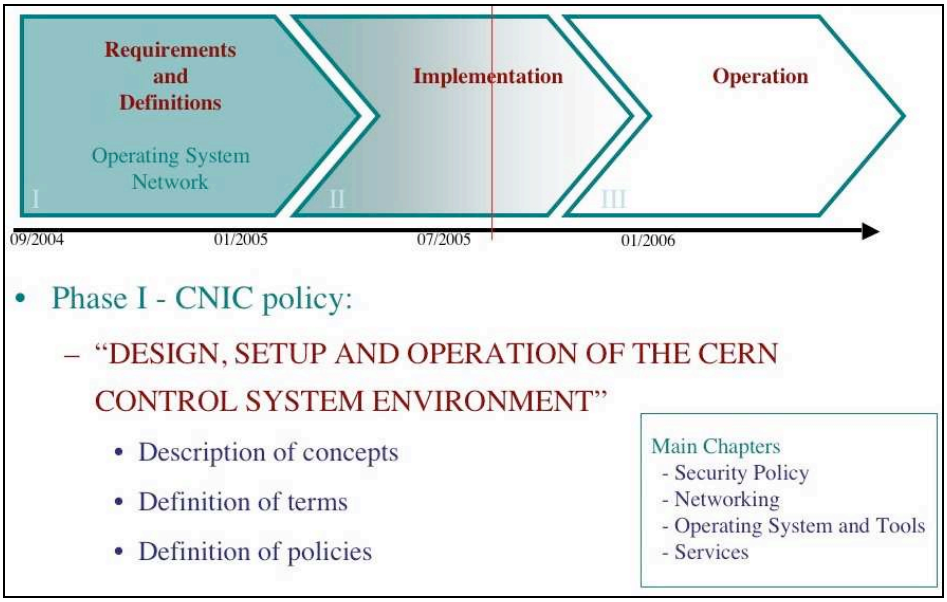

Figure 1: CNIC Phases

CNIC DEFINITIONS - SECURITY POLICY

The goal of the security policy is to establish rules and clear responsibilities for all equipment connected to the network, and to ensure that correct procedures are followed up locally by the persons responsible for the individual end systems. The security policy addresses the network infrastructure, as well as all devices actually connected to the network.

NETWORK DOMAINS

A domain is a part of the network infrastructure dedicated exclusively to a particular set of users. The following domains have been identified as being necessary for the correct operation of the LHC accelerator, its control systems, and the control systems of the experiments:

1. The Technical Network (TN)
2. At least one domain for each LHC experiment (Experiment Network EN)
3. The General Purpose Network (GPN)

The General Purpose Network is the standard CERN campus network, with access to the Internet via the CERN external firewall. This network is used for all general services such as desktop (office) computing and central servers (e.g. web servers, mail servers). The Technical Network and the Experiment Networks are reserved for control systems and are not accessible from outside CERN, but are reachable from the General Purpose Network. In addition to the above identified domains, private and isolated networks that are not maintained by a centralised CERN support team, might be installed and used. The domains will be inter-connected via dedicated interfaces which also provide controlled access. Equipment may be grouped into "Functional Sub-Domains (FSD)" by network means, e.g. for cryogenic system devices. This will allow inter-connectivity restrictions to be implemented.

All equipment connected to a domain must be registered in the network database. For each network domain at least one responsible person must be defined. These domain managers may define which services and protocols are allowed to pass the firewalls and enter the corresponding domain. Furthermore, they control the connection of all equipment to their domain.

HARDWARE DEVICES

Physical access to devices on TN and EN must be controlled. In public areas, computers and equipment must be placed in lockable racks to prevent physical tampering.

Furthermore, uncontrolled installation of software is expressly forbidden, and therefore any data transfer peripherals such as USB keys, modems, CDs, floppy disks, etc. must be disabled for equipment destined for use on the TN and EN services. Only the system administrators may be allowed the use of such devices for system maintenance activities.

OPERATING SYSTEMS AND SYSTEM FILES

Operating system software (e.g. Windows, Linux) will be provided and maintained centrally by IT Department. By default, each operating system installation must include intrusion detection software. Tools will be available to set-up "Named Sets of Computers" (NSCs) and their specific software configurations.

An upgrade and patching strategy must be defined by the persons responsible for the equipment before it is connected. Security patches and software updates will be provided by IT and need to be installed as fast as possible after release. No automatic patching is foreseen. The domain managers will be notified and will have to arrange an installation strategy as well as a time planning for their domain and their NSCs.

In certain critical situations, such as the detection of new threats exploiting known or existing vulnerabilities, an emergency procedure must be available to perform interventions on the NSCs concerned. Machines that do not conform to the required security level or cause problems for other users, can be disconnected from the network if they are a risk for other installations.

SOFTWARE

Development and deployment guidelines for software must be defined and distributed to all developers, as well as companies developing software for use at CERN. The guidelines will have to be defined by the domain managers in accordance with the specific boundary conditions of the domain.

In general the following points should be covered by the guidelines:

- development methods
- development servers and their O/S versions
- development tools
- test procedures
- test machines and their O/S versions
- acceptance procedures
- procedure for deploying software in operation
- maintenance procedures (bug fixing and patching)

Only software that passed the acceptance procedure, as defined by the domain managers, can be deployed for operation.

All software installed in a control system must allow updates to be made. Installation and upgrade policies must be in place for each project.

TESTS

Each new or modified system has to be tested before it can be connected to the TN. Software changes and patches need to be tested and validated before being deployed for operation. The systems should first be installed in a domain specific test environment and thoroughly tested.

The follow-up of the test procedures are under the responsibility of the domain managers and equipment responsible persons.

LOGINS, PASSWORDS AND AUTHORIZATIONS

Personal accounts, administered via central domain authentication services, have to be used whenever this is technically possible. Generic accounts must only have very limited authorizations (read-only), and must never be allowed to install software or alter system parameters. Whenever possible, special personal accounts with appropriate privileges should be used for system administration. It is emphasised that passwords for personal and generic accounts must follow the CERN password recommendations.

TRAINING

The level of general security awareness must be raised in the user community. Users have to understand, and must accept the security policy as defined in this document. Training material on each topic must be available for information, self-study, and training sessions. Training sessions need to be organised on a regular basis. The domain managers should also be competent to inform and train users at any moment.

SECURITY INCIDENTS AND REPORTING

Security incidents, abnormal situations and improper installations are usually detected by the computer security team and will be reported immediately to the corresponding domain and equipment responsible persons. A summary report on the incident will also be distributed to other persons responsible for a domain. Misbehaving systems will be disconnected from the network without prior notice if they pose a risk for other systems. In case the misbehaving equipment may not be individually identified , it must be possible to be cut connections at pre-defined "breakpoints" to isolate the concerned part(s) from the rest of the network.

CNIC DEFINITIONS - NETWORKING

Similar physical networking installations will be used for two differing purposes at CERN:

- Computers for desktop and general use (e.g. e-mail, WWW, office, engineering and physics applications), which do not imply any direct risks in case of equipment or hardware failure. Such machines are connected to the general purpose network (GPN).
- Computers used in operational environments that control parts of CERN's technical infrastructure, which may harm people or equipment in the case of a failure. This equipment must be connected to the technical network (TN) or experimental networks (EN).

GENERAL PURPOSE NETWORK (GPN)

The GPN offers worldwide connectivity. It can be accessed from outside CERN through application gateways. Physical connection to the CERN networks will only be possible if the MAC-address of the equipment trying to connect is known and registered in the CERN Network database.

TECHNICAL AND EXPERIMENT NETWORK (TN AND EN)

The TN and EN will have a similar infrastructure to the GPN, but with more access restrictions:

- Only tested and approved equipment can be connected.
- Authorization will be needed in order to connect equipment.
- Only a defined set of CERN users will be allowed access to the domain.
- Only limited services will be available (e.g. no mail server, no external web browsing).
- The domain should be able to run independently from centrally provided services for a limited duration.
- Optional network segregation may be instigated in order to have restricted connectivity between devices.

Only CERN registered users will be allowed to request connections to the TN. All devices being connected to this domain must be registered in a data base together with their hardware address, operating system, the purpose of the device, and a well-defined list of persons responsible for the equipment. Users who are allowed to install, maintain or configure systems must be known in advance and their data has also to be kept in a central database.

INTER DOMAIN COMMUNICATIONS

The TN domains will be linked by application gateways to the GPN . In addition to the application gateways, access to the TN domains will be granted to a restricted set of trusted central IT services. Each domain may choose which central IT services are trusted and shall be accessible from the domain.

INTRUSION DETECTION

Intrusion detection should be configured on a per domain basis. No automatic blocking of controls computers should take place. However, the network operation team must be able to disconnect machines that make denial-of-service attacks or propagate worms in the centrally managed network infrastructure. If "network breakpoints" are defined, complete network “parts” could be disconnected if required. The gateway into a network domain is by default considered to be a “network breakpoint”.

TESTING

A test environment on an independent network will be required. This environment will be used to validate hardware and software before installation in the operational environment. It must allow virus-scans and virus-attack simulation to detect infections and vulnerabilities, respectively. This functionality could be centralised in a lab (e.g. TOCSSiC) in the IT department.

CNIC DEFINITIONS - OPERATING SYSTEMS AND TOOLS

Although the implementations may not be the same, there are no obvious differences in requirements between machines running Windows or Linux. The overall goal is to manage machines by user-definable groups, to control external interventions and the application of upgrades or patches and to be able to validate changes before they are applied to the computers controlling the equipment.

It may be necessary to install and configure local firewalls, coming with Windows and Linux, to enhance the overall security. Management tools must be in place to supervise and configure the local firewalls centrally.

NAMED SET OF COMPUTERS (NSC)

A number of computers with identical functionality and, thus, a similar configuration (e.g. the Cryogenics Control Computers) will be grouped into Named Set of Computers” (NSCs). The persons responsible for a particular application must be able to define NSCs. For each NSC, regular automatic vulnerability scans must be run according to the schedule of the persons responsible for the equipment, e.g. during shut down periods. A mechanism will be required to contact the persons responsible for a NSC in the case of an emergency that requires appropriate actions to be taken.

CONFIGURATION

For each NSC, the possibility of installing a defined version of the basic operating system (Linux or Windows), and additional sets of user software that are needed to perform the corresponding control task, is required. All defined software packages must be installed from a central service.

Tools must be provided to create, distribute and install defined software to an NSC. This must also include patches to the user’s application and application configuration files. The tools must also allow a roll-back to a previous version of the configuration (e.g. previous operating system or software versions). It must be possible to audit the set of computers belonging to the NSC against a configuration baseline as defined in the configuration database and to identify non-conformities.

Additionally, it must be always possible to automatically install a new instance of a particular computer (clone), e.g. due to increasing needs, or in case of complete failure of a computer.

CNIC - IMPLEMENTATION PHASE

Planning and implementation

The CNIC working group was started in September 2004 with the aim define a policy and an implementation planning. In phase 1 the requirements and specifications for the different tools have been defined and a CERN wide awareness campaign has been started. Today we are in phase 2, the implementation phase. The required tools for installation and management have been developed and are currently being tested. A first set of Windows Terminal Servers (WTS) for controls is available and people are asked to use them to access the controls environment. Next steps will be the network filtering to start separating the campus network from the technical network. It is planned to deploy the full set of CNIC rules from 2006 onwards. Exceptions and interim solutions should be solved by Mid 2006.

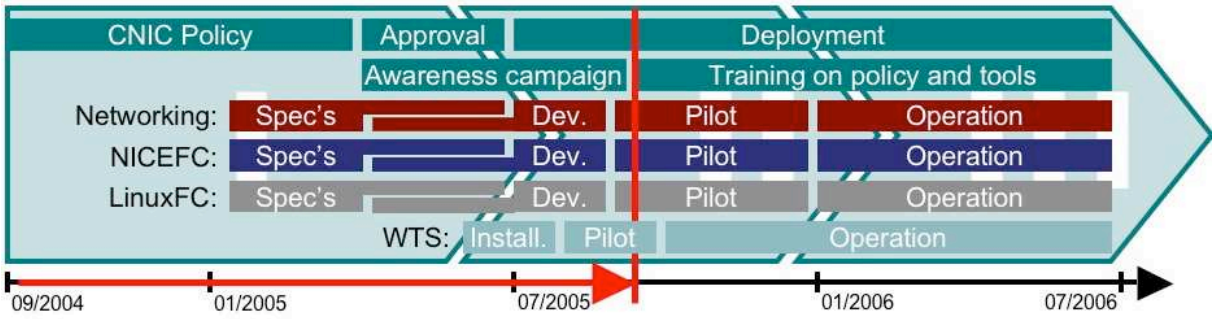

Figure 2: Implementation planning

Manpower and resources

The CNIC WG meets every fortnight with an average of 8 persons involved for the definition of the requirements and proposing technical solutions. Half of the persons represent the "clients" or "users" of the central services, the other half are the "service providers". A satisfactory level of quality requires at least one person per service (networking, Linux, Windows, application gateways). The follow-up and promoting of security policies requires at least one person per domain. Resources are also needed for the purchase of adequate equipment like network routers, Windows Terminal Servers or other dedicated equipment that is needed to meet security demands.

CONCLUSION

It was seen that awareness for security issues and acceptance for changes is very important for the success of the CNIC efforts. To obtain a common consent it is useful to show that the final advantages are higher than the investments. Manpower and resources must be available and decisions backed up by management to allow the implementation of tools and providing the required services.

Although the participants of the CNIC working group come from different CERN environments, a very constructive attitude could be established once the helpfulness of the CNIC issues was recognised. The awareness campaign raised many technical questions and reservations from the users that must now be followed up on a case per case basis. Acknowledgement by the users can only be ensured if real and practical solutions can be shown. Full acceptance is expected once the required tools are fully available and have been presented to the users.

ACKNOWLEDGEMENTS

A special thanks to the members of the CNIC-WG and colleagues all around CERN for supporting the work in such a positive way. The success of this work relies very much on the very useful and constructive input of the participants in the regular meetings, namely Nuno CERVAENS -IT/CS, Pierre CHARRUE – AB/CO, Peter CHOCHULA - PH-AIT, Lionel CONS - IT/CS, Nir DAUBE - PH-ATD, Ivan DELOOSE - IT/IS, Uwe EPTING - TS/CV, Bruce FLOCKHART - IT/CO, David FOSTER - IT/CS, Denise HEAGERTY - IT/DI, Nils HØIMYR - IT/CS, Jan IVEN - IT/ADC, Beat JOST – PH/LBC, Jean-Michel JOUANIGOT - IT/CS, Mike LAMONT - AB/OP, Patrick LIENARD - AT/MAS, Stefan LUEDERS - IT/CO, Giuseppe MORNACCHI - PH/ATD, Alberto PACE - IT/IS, Martti PIMIA - PH/CMC, Matthias SCHROEDER – IT/ADC, Søren POULSEN - TS/CV.

REFERENCES

[1] CNIC working group, DESIGN, SETUP AND OPERATION OF THE CERN CONTROL SYSTEM ENVIRONMENT (2005)
[2] CNIC on EDMS: https://edms.cern.ch/nav/CERN-0000053021
[3] OS support for Control Systems (D. Myers)
[4] Management Issues in the CERN Technical Network: https://edms.cern.ch/document/481960/1
[5] Principles governing the design, setup and operation of the technical and experimental networks (Peter Chochula, Beat Jost, Giuseppe Mornacchi, Martti Pimiä)