CERN
CH-1211 Geneva 23
Switzerland

Document
Security Baseline for Ind. Embedded Devices

CERN Div./Group or Supplier/Contractor Document No.
Computer Security Officer

EDMS Document No.
1139163

APRIL 04TH, 2011

SECURITY BASELINE FOR INDUSTRIAL EMBEDDED DEVICES

ABSTRACT A “Security Baseline” defines a set of basic security objectives which must be met by any given service or system. The objectives are chosen to be pragmatic and complete, and do not impose any specific implementation. Therefore, details on how these security objectives are fulfilled by a particular service/system must be documented in a separate “Security Implementation Document” [1]. These details depend on the operational environment a service/system is deployed into, and might, thus, creatively use and apply any relevant security measure. Derogations from the baseline are possible and expected, and must be explicitly marked.

At CERN, for each service/system used in production, such a Security Implementation Document must be produced by its system/service owner, and be accepted and approved by the Computer Security Officer. All systems/services must be implemented and deployed in compliance with their corresponding Security Implementation Document. Non-compliance will ultimately lead to reduced network connectivity for the affected services and systems (i.e. closure of CERN firewall openings, access blocked to other network domains, and/or disconnection from the CERN network).

This document describes the Security Baseline for embedded systems used in the CERN production environment.

Prepared by:	***Checked by:***	***Approved by:***
Filippo Tilaro Brice Copy Computer Security Team	IT Security Contacts Department Security Contacts Experiment Security Contacts	Computer Security Officer IT Group Leaders IT SRM Members
Distribution:	Unrestricted	

History of Changes

Rev. No.	***Date***	***Reference***	***Description of Changes***
0.1	2010/12/14		First draft
0.9	2011/04/04		Draft for comments

1. SECURITY BASELINE REQUIREMENTS

This document contains recommendations and security configurations for embedded devices which are part of a Process Control System (PCS) connected with enterprise networks. These specifications represent a reference point for both network administrators and operators. Moreover the cooperation between network administrators managing general CERN networks (GPN) and technical networks (TN) must be considered one of the most critical aspects. Unfortunately not all security concepts from the IT world can be implemented in process automation: it is well-known that an IT system focuses mainly on global accessibility and best-effort security. On the contrary, the most important factor for process automation is the functionality and availability of the plant. Any deviations from these security concept specifications can result in security vulnerabilities.

The objectives of the Security Baselines below apply to any embedded device, PLC, industrial module which can be considered part of a PCS. If a service/system consists of multiple devices/modules, the baseline applies to each of them. All of the following requirements should be considered mandatory, and in case of unfeasibility, other alternative solutions must be taken into account so as not to compromise the entire system security level. The terminology follows RFC2119 [2]. The words “least”, “minimize”, “restrict” and “small” refer to the operative minimum before rendering the service/system useless.

1.1 ACCESS CONTROL

Ref.	Requirement	Comment
ED-AC-1	Restrict privileged device accesses to a small, controlled group of users.	“Rule of least privilege”
ED-AC-2	Deploy a conservative RBAC strategy to grant only the necessary access rights to each account.	RBAC: Role-based access control
ED-AC-3	Do not leave any default passwords or services. When it is feasible activate the device built-in security systems.	(e.g. PLCs’ ACL)
ED-AC-4	Change the default passwords of all users on all deployed devices. User accounts that are no longer needed must be removed.	
ED-AC-5	Create a central record of assigned device names and IP addresses and keep it up-to-date.	In order to have complete visibility and control over the entire system.
ED-AC-6	Restrict remote access to few privileged accounts and secure them through additional security mechanisms.	Avoid external dial-up connections.
ED-AC-7	Record privileged operations occurring on individual devices.	For any required future error analysis (forensics).

1.2 INDUSTRIAL DEVICES NETWORK CONFIGURATION

Ref.	Requirement	Comment
ED-NC-1	Isolate the individual devices from the office network through Firewalls, VLAN, DMZ or air-gap.	
ED-NC-2	Connect the device into a segmented network (known as “security cell”) and make sure it has been isolated from the rest of the site.	Alternative solution only in very specific working scenarios.
ED-NC-3	Connect all devices belonging to one segment and involved in its operation directly and not through leased lines (for example modems, GSM …).	
ED-NC-4	Restrict remote access to an industrial device from outside its	

	parent control cell through a secure access point, if required.	
ED-NC-5	Control and regulate the traffic load of each device in order to guarantee that it can be handled both during normal working conditions and exceptional ones (alarms, high rate of I/O triggers).	The approved and necessary data traffic must be known and identified in advance.
ED-NC-6	Establish policies to limit or prohibit media connections (even indirect) to individual devices (for example USB keys or CDs).	The main attack vector for the “Stuxnet” was using USB keys.
ED-NC-7	Do not install network management services (such as DNS, WINS, DHCP, domain controllers, etc…) on an industrial device, but only on specific servers which have been specifically configured for this purpose.	
ED-NC-8	Apply the same policy to all devices of the site in order to guarantee the uniformity of network settings, configurations, security policies, users and passwords handling.	The entire site operation can be jeopardized by a single incorrectly configured device.
ED-NC-9	Make sure that the device is time-synchronized with the rest of the site in order to reduce the risk of Jitter and time discrepancies.	

1.3 MONITORING AND LOGGING

Ref.	Requirement	Comment
ED-ML-1	Setup a monitoring system to check device status, its configuration and running software.	
ED-ML-2	Monitor all the entities which are communicating with each embedded device and ensure they are allowed to do so.	
ED-ML-3	Deploy an intrusion detection system (IDS) for the industrial traffic ensuring that it does not impact expected functionalities.	
ED-ML-4	Deploy a logging system to store the main events, operations and actions in order to reconstruct the sequence of events and changes in case of faults.	
ED-ML-5	Define recovery functions and procedures to restore a device to working conditions after any fault.	

1.4 PROCEDURES

Ref.	Requirement	Comment
ED-PR-1	Divide precisely the spheres of responsibility between the IT department and the PCS personnel to avoid any administration interference.	Configure independently from IT requirements.

1.5 ROBUSTNESS TESTING AND DEPLOYMENT

Ref.	Requirement	Comment
ED-RD-1	Scan the device interfaces (for example open ports, services running) which can be used as potential vectors of attack and make sure there are no hidden vulnerabilities.	
ED-RD-2	Check the effectiveness of the built-in device security systems (e.g. ACL, firewall, password checking etc…).	
ED-RD-3	Verify that the device’s network protocols implementation does not expose inherent vulnerabilities.	
ED-RD-4	Disable unwanted and unnecessary services.	

ED-RD-5	Make sure that the device can be accessed only from within the security cell or the access point.	
ED-RD-6	Perform appropriate integration tests before deploying a new device in the system.	
ED-RD-7	During the deployment phase, choose the device which provides the essential functionalities but no extraneous services, unless they can be deactivated as required.	
ED-RD-8	Deploy only fail-safe mode devices taking care that their fail configuration is consistent for the plant process.	“Fail-safe device” means that the device is also secure when it fails.
ED-RD-9	Make sure that the developed software is safe and does not make use of improper functions or vulnerable operations.	E.g.: programmed opening connections, timer reset, …

1.6 SOFTWARE & APPLICATIONS

Ref.	Requirement	Comment
ED-SW-1	Apply security patches to the operating system and all applications in a timely manner. The meaning of “timely” must be explicitly defined.	A centralized patching strategy is suggested.
ED-SW-2	Put in place an appropriate patching strategy that avoids (or at least minimizes) downtime.	
ED-SW-3	Test security updates prior to deployment. Deploy an appropriate redundancy device installation scheme to avoid downtime during updates.	
ED-SW-4	Perform manual and automatic reviews of the configuration of each device in order to ensure it is still security compliant.	This activity is part of the periodic risk assessment.
ED-SW-5	Install only absolutely necessary software. Do not leave any unused generic system/user functions, data blocks, functional blocks, or any other functions which can be used maliciously.	

1.7 ADDITIONAL SECURITY BASELINES

Ref.	Requirement	Comment
PCS-ADD-1	Implement the requirements defined in the most recent “Security Baseline for Servers” [3] for all devices being part of the PCS.	

2. REFERENCES

[1] The CERN Security Team, “Security Implementation (Template)”, EDMS 1062504
[2] Network Working Group, RFC2119, http://www.ietf.org/rfc/rfc2119.txt
[3] The CERN Security Team, “Security Baseline for Servers”, EDMS 1062500