

# MEASUREMENT AND AUTOMATION BRANCH

## Cyber Security Procurement Language for Control Systems

Documentation number: SUT C-2

As on: September 2022

**PCC Rokita SA**

ul. Sienkiewicza 4

56-120 Brzeg Dolny

[kontakt@pcc.rokita.pl](mailto:kontakt@pcc.rokita.pl)

[www.pcc.rokita.pl](http://www.pcc.rokita.pl)


Brzeg Dolny 2022

## Table of content

1LIST OF ACRONYMS .....	4
1. INTRODUCTION .....	6
2. DOCUMENT OBJECTIVE.....	6
3. DEFINITIONS.....	6
4. BASE MATERIALS.....	11
5. GENERAL GUIDELINES.....	12
5.1 Scope .....	12i
5.2 Exclusions .....	12i
5.3 Standards and regulations in force at PCC Rokita .....	12
5.3.1 Legal requirements .....	12
5.3.2 Standards and technical specifications .....	13
5.4 General requirements for designing and acceptance in force at PCC Rokita .....	13
5.4.1 Terms of acceptance of automation devices and systems .....	13i
6. Solutions for ensuring the requested cyber security level on different protection layers.....	14
6.1 Installation security.....	14i
6.1.1 Physical access to cybernetic elements .....	14i
6.1.2 Physical access to the areas (perimeter protection).....	15i
6.1.3 Physical access to manual override .....	16i
6.2 Network security .....	17
6.2.1 Perimeter protection .....	17
6.2.2 Network addressing and name recognition .....	18i
6.2.3 Remote access .....	19
6.2.4 Network partitioning.....	22.

6.3	System integrity .....	24
6.3.1	System "hardening" .....	24
6.3.2	Session management.....	28i
6.3.3	Management and policy of passwords/authorizations .....	29i
6.3.4	Encoding practices .....	29i
6.3.5	Fault correction .....	29i
6.3.6	Detection and protection against malware .....	30i
6.4	Terminal devices .....	31i

7. List of drawings

	Standard of technical equipment for PCC Rokita SA - Language of public procurement for ensuring cybersecurity of control systems		
	SUT C-2	Date: 9/28/2022	Page 1 of 36

	Standard of technical equipment for PCC Rokita SA - Language of public procurement for ensuring cybersecurity of control systems		
	SUT C-2	Date: 9/28/2022	Page 4 of 36

---

## LIST OF ACRONYMS

- ACL list - a mechanism of filtering of network packages used during configuration of a router**
  - AKP - Control and Measurement Instruments**
  - AKPiA - Control and Measurement Instruments and Automation**
  - AMS - (Eng. Alarm Management System)**
  - APL - (Eng. Advanced Process Library)**
  - BIOS - (Basic Input/Output System or Basic Integrated Operating System)**
  - BMS - (Eng. Building Management System)**
  - CPU - (Eng. Central Processing Unit)**
  - DG - Director General**
  - DCS - (Eng. Distributed Control System)**
  - DMZ - (Eng. Demilitarized Zone)**
  - DNS - (Eng. Domain Name System) - a system whose task is to translate domain names into IP addresses**
  - EMC - (Eng. Electromagnetic Compatibility)**
  - ERP - (Eng. Enterprise Resource Planning)**
  - ESD — (Eng. Emergency Shutdown System) — a system of interlocks in an industrial control system**
  - EX - (Eng. Explosion proof )**
  - FAT - (Eng. Factory Acceptance Tests)**
  - HART - (Eng. Highway Addressable Remote Transducer)**
  - HIDS — (Eng. Host Intrusion Detection System)**
  - HMI - (Eng. Human-Machine Interface)**
  - IED — (Eng. Intelligent Electronic Devices)**
  - IK - Critical Infrastructure**
  - MPI - (Eng. Multi-Point Interface)**
  - MRP (Eng. Material Requirements Planning)**
  - NIPS — (Eng. Network-based Intrusion Prevention System) — a system of network monitoring and protection of confidentiality, integrity and availability of networks.**
  - NIDS - (Eng. Network Intrusion Detection System)**
  - NPOIK — National Program for the Protection of Critical Infrastructure**
  - NTP — (Eng. Network Time Protocol) - A time synchronization protocol**
-

**OPC - (Eng. OLE for process control)**

**OT - (Eng. Operational Technology) - industrial control**

**P&ID - (Eng. Piping and Instrumentation Diagram) PLC - (Eng. Programmable Logic Controller)**

**RFC - (Eng. Request for Comments) - a collection of documents relating to the Internet and computer networks**

**RTU - (Eng. Remote Terminal Unit)**

**SAT - (Eng. Site Acceptance Tests)**

**SCADA - (Eng. Supervisory Control And Data Acquisition)**

**SIL — (Eng. Safety Integrity Level)**

**SIS — (Eng. Safety Instrumented System) — a system of protection automation**

**SSiN — Control and monitoring system (power engineering)**

**SDT - Standard of Technical Documentation**

**SUT - Standard of Technical Devices**

**TCS (SSRK) - (Eng. Train Control System) - Railroad traffic management system**

**USB - (Eng. Universal Serial Bus)**

**VLAN - (Eng. Virtual Local Area Network) - A virtual local computer network, logically separated within a larger physical network.**

**VPN - (Eng. Virtual Private Network)**

**WAN - (Eng. Wide Area Network)**

**WLAN - (Eng. Wireless Local Area Network) - ZSZ - Integrated Management System**

**ZSZ - Integrated Management System**

## 1. INTRODUCTION

A key element in the protection of the state critical infrastructure and key resources under the National Program for Critical Infrastructure Protection (NCIP) is the information and communications security of OT (Operational Technology) environmental control systems and it should be taken into account in the design, modification and maintenance of industrial automation systems and production networks to provide an acceptable level of risk for the organization's operations in this field.

Since functional control systems operate for the continuous and safe operation of the country's critical infrastructure, it is essential to identify and understand the important roles of these systems. Moreover, there should be increasing interest in identification of potential weaknesses, consequences and challenges associated with securing these systems against cyber-attacks. Due to the closed nature of control systems using outdated information technology, the production zone is particularly vulnerable to attacks, especially when linking them to ERP or management information systems. The losses associated with this (stoppages, leakage of confidential information and resulting loss of trust in the brand and drop of company competitiveness) can very easily be translated into the financial dimension.

The factors contributing to risk escalation in OT systems:

1. The control systems adopt standardized technologies with known vulnerabilities.
2. The control systems are connected to other networks that are not secure.
3. Uncertain connections fester the security holes.
4. Manuals concerning the use of OT systems are available publicly, both for terrorist as well as rightful users.

## 2. DOCUMENT OBJECTIVE

This document is intended to provide the organization an adequate reliability of operation and relevant protection of the OT control systems (DCS/SCADA/MES) in terms of the cyber security. This document presents design and/or execution guidelines and recommendations in force in the PCC Rokita group for the OT control systems with consideration of security requirements in the architecture and specification of the OT systems and the necessary acceptance tests (FAT / SAT) covering verification of the security recommendations so as to provide observance of the security systems policy of the company and good practices in ensuring an acceptable level of the cyber security for them.. The use of these guidelines concerning orders will help to obtain assurance of security in the control systems. This document includes information and specific examples of text in the contractual language to assist the control systems community, both owners and integrators, in establishing sufficient controls for the security of control systems within the contractual agreements to provide an acceptable level of risk.

## 3. DEFINITIONS

**Attack** — Deliberate and planned acting, resulting in erroneous functioning, disturbance of operation or deactivation of the industrial automation system.

**Backdoor** - (Pol. a rear door, wicket gate) — a hole in the security system created purposely in order to exploit it later.

**BIOS - (Eng. Basic Input/Output System or Basic Integrated Operating System).** - BIOS refers to the software code that the computer triggers when it is started up first time. The principal function of the BIOS system is to prepare a device so as the other programs stored on other media (hard drives, micro discs and CD-ROMs) could upload, execute and take over control of the computer. This process is called booting.

**Gateway** - It is an intermediary mechanism in communication of two separate computer networks.

**Sensor** - a device, physical system, which transfers its reaction to a physical stimulus into a measurable signal of other physical volume in order to provide information about the physical volume.

**Canary(ies)** — Canary data processing, a canary or canaries are false devices or unused Ethernet ports used in connection with detecting software in order to warn against unauthorized probing of the network or surveillance. The name refers to using canaries as warning devices in coal mines.

**CPU - (Eng. Central Processing Unit)** - A central unit; processor - a sequential digital device that executes commands based on interpreted data retrieved from the memory.

**DCS - (Eng. Distributed Control System)** - a system of control and visualization of an industrial process, which features a common data base for the control and visualization as distinct from the SCADA or PLC systems.

**Deny All** — The most significant rule of the local network protection in network firewalls determining that: “All activities that are not expressly authorized are prohibited!” Thanks to this strategy there exist only these accesses that were explicitly opened personally by the administrator.

**DMZ — (Eng. Demilitarized zone)** — a demilitarized zone is a special configuration of a local network objected to improve security by segregation of computers on each side of the firewall. It is a logically separated network segment (of limited trust) intermediating between networks with different levels of criticality for organization between the network of office users (untrusted zone) and production networks with industrial automation systems (trusted zones - protected by firewalls).

**DoS - (Eng. Denial of Service) — locking of services** — Disruption or prevention of an authorized access to a system or system resources or delaying or disruption of system operation.

**Emergency Shutdown System (ESD)** — an interlock system ensuring a safe process stoppage for industrial control in case of a failure.

**ERP - (Eng. Enterprise Resource Planning)** is software for businesses (a system of applications) whose objective is to integrate all the processes taking place within the organization.

**FAT — (Eng. Factory Acceptance Tests)** — an activity intended to confirm that a particular system is operating correctly. It is performed at a manufacturer before transport to a target company.

**FUZZING** — A method of testing software or finding vulnerability holes in it, useful in hacking attacks.

**Heartbeat Signals** — Also known as a watchdog clock, keeping alive and health condition. Signals inform about the communication condition of the system.

**HART — (Eng. Highway Addressable Remote Transducer)** — A communication protocol of industrial networks allowing to change the range and diagnostics of the control and measurement instruments and automation devices. One of the standard communication protocols of the Control and Measurement Instruments in industry.

**HAZOP - (Eng. Hazard and Operability Study)** - A method of risk analysis.

**HIDS — (Eng. Host-based Intrusion Detection System)** - A system of detection of host intruders. The application that detects possible malicious activity on the host from such features as file modification (integrity check of file system), operating system connection profiles, etc.

**HMI — (Eng. Human-Machine Interface)** — A control panel (operator's) - an electric device rendering possible control of other devices that execute certain processes e.g. process or production ones.

**IED — (Eng. Intelligent Electronic Devices)** - it is a term used in the power generation industry to describe microchip controllers of the power generation system devices such as switches, transformers and capacitor banks.

**IK — Critical Infrastructure** - resources (physical and cybernetic systems) featuring crucial meaning (indispensable) for functioning of the society and economy.

**OT Security incident (Incident)** - it is an event or a series of adverse or unexpected events, which directly threaten the security of information (jeopardize its confidentiality, availability or integrity) or create a substantial probability of disturbing of the technological processes or business activities.

**Client** — A device or application that communicate with a server.

**Access control** — Protection of the system against unauthorized logical or physical access comprising a process, which allows to adjust and monitor access to the system resources in compliance with the accepted security policy.

**Cryptography** — A set of means and methods objected to protect transferred information against unauthorized access e.g. by data encryption.

**LAN (Eng. Local Area Network) — A local network** — A local computer network connecting the network resources located in a small distance.

**Log** — An event registry comprising information on events and actions concerning operation of a program or information system.

**Malware (Eng. Malicious Software)** — a malicious/harmful software hazardous for the operation system and the data accumulated in a computer.

**MES - (Eng. Manufacturing Execution System)** — A production execution system used to collect information about the production process directly from the production stations and their transmitting to the business zone and also some of the supporting systems such as e.g. central AV signature distribution servers, transfer servers, file exchange servers, directory service servers, etc.

**Microswitch** — An electric switch triggered by a small movement of its lever.

**Reference model** — A structure that allows to describe elements as well as interfaces of a system in a coherent way.



**MPI - (Eng. Multi-Point Interface)** — An industrial network for communication between PLC controllers, programming station, operation panels and other devices of the SIMATIC family made by SIEMENS Company.

**MRP - (Eng. Material Requirements Planning)** - Planning of material demand - it is a collection of processes, which enables planning of the material demands on the basis of the data on the product structure, information on stock levels, status of orders in the making and production plan.

**NIDS — (Eng. Network Intrusion Detection System)** — A system of detection of cyber intrusions is used to identify unauthorized or incorrect network traffic.

**NTP — (Eng. Network Time Protocol)** - A communication protocol, which enables precise synchronization of time between ICT devices.

**OPC - (Eng. OLE for process control)** — An open standard of communication used in the industrial automation and higher levels of information systems (business), used to connect the applications based on operation systems with the hardware and application software of the industrial automation.

**OT - (Eng. Operational Technology)** — a hardware and software category for monitoring and controlling operation of physical devices - the hardware and software intended to detect or triggering changes in the physical processes by direct monitoring and/or control of physical devices such as valves, pumps, etc.

**PLC - (Eng. Programmable Logic Controller)** - A programmable logic controller is a microchip device, which performs a control algorithm in cycles, on the basis of which it processes the input states into relevant output states.

**Vulnerability** — A characteristic feature of the system, such as a hole in implementation, operation or system management, which renders possible disturbance of its operation or infringement of the accepted security policy.

**Security policy** — A set of rules, procedures, instructions, standards defining the way in which an organization protects its resources.

**PROFIBUS DP** - A communication protocol of industrial networks created for the standard of the PROFIBUS distributed real time deterministic network. One of the standard protocols of communication of the Control and Measurement Instruments and Automation in the industry.

**PROFINet** — A modern industrial standard based on the Industrial Ethernet network, for construction of integrated and coherent systems of automation and distributed systems of automation based on the component model.

**Transducer** - A device transforming a particular value to another one according to a determined dependence and with a determined preciseness.

**Smart transducers** - Transducers ensuring a measurement, signal processing and communication with an external measurement system or control system using a digital signal on the basis of a standard communication protocol.

**Communication protocol<sup>1</sup>** — A set of rules and steps executed by a communication device for the needs of transfer and exchange of the data.

**RTU - (Eng. Remote Terminal Unit)** — A universal device used for remote

monitoring and control of various devices and automation systems, implemented usually in the industrial environment.

**SAT — (Eng. Site Acceptance Testing)** — an activity objected to confirm that the system supplied to the customer is complete and features no damages that can arise during transport or implementation.

**SCADA — (Eng. Supervisory Control And Data Acquisition)** - A system of supervision and technological or production process data acquisition, which has the following functions: process data collection (including measurements), visualization of the collected data, process control on the basis of the collected data and a relevant control algorithm, alarming and measurement data archives.

**SDT** — Technical Documentation Standard - developed by PCC Rokita SA their own standards concerning technical documentation and process identification system.

**SIL — (Eng. Safety Integrity Level)** - A level of the safety integrity — It is the level of requirements, which is fulfilled in order the system ensuring security would work.

**SIS — (Eng. Safety Instrumented System)** — A system of protection automatics — A system, which operates automatically in order to keep the installation in the safe state or bring it to this state in case of occurrence of states divergent from the normal conditions.

**Control** — Reacting on the particular object in order to obtain a determined objective related with certain information in the form of a signal.

**Automatic control** — control carried on using a specially constructed device (controller, regulator)

**Manual control** — the control performed by a man.

**Controller** - A system busy with supervision of work of an electric device. It can be computer, electric, electronic or electromechanical.

**System** — A collection of mutually linked hardware and software elements, which mutually execute at least one function.

**Security system** — A system supervising or controlling correctness and continuity of operation of both complete OT systems as well as their applications, services and elements, including telecommunication and remote transmission used in the OT systems.

**Signal**<sup>1</sup> - A model of any measurable value changing over the time, generated by physical phenomena or systems.

**Analog signal** - A signal, which can assume any value from a continuous range and its values can be determined at any moment in time by a given signal mathematical function..

**Digital signal** - An electric or optic signal, which carries the digital data by relevant coding (digital modulation).

**Measurement signal** — a signal with the parameters set and known to the metrologist, used to stimulate the measured system or checked instrument.

**VLAN - (Eng. Virtual Local Area Network)** — A virtual, local computer network, separated logically within another, larger physical network.

**VPN - (Eng. Virtual Private Network)** — a communication tunnel used to provide better effectiveness or a larger security level of the transmitted data, through which the traffic goes within a private network between the end customers via the public Internet network in such a way that the nodes of this network are transparent for the packages transmitted in this way.

**End devices** — Components of a control system, which collect information or control the process. These can be sensors, controllers, valves, processors, etc. The end devices are supplied with normal computer software (e.g. Web, FTP, TELNET) in order to facilitate maintenance and configuration.

Smart end devices, remote terminal units and programmable logic controllers (OLC) include microchips and are considered “smart” end devices. Traditional sensors, actuators and measuring devices traditionally include limited possibilities of processing and are known as “dumb” end devices. Communication (serial or Ethernet) to/with “smart” or “dumb” end devices to the control system can be taken over and modified exerting an adverse impact on the controlled process.

**Devices/execution elements (Actuators)** - mechanical devices used in adjustment and control systems, working out an input signal to the adjusted/controlled object on the basis of a control signal.

**Authentication** — Safety means objected to confirm reliability of a connection, message or also confirmation of the access of the particular user to the restricted resources.

**Watchdog** - a time layout detecting erroneous operation of the system, attempting to repair it and prevent a more serious failure.

**WLAN - (Eng. Wireless Local Area Network)** — A wireless local zone computer network using microwave/infrared waves as the medium to carry signals standardized with Norm IEEE 802.11.

**Firewall** - A dedicated device or software, which protects on the level of the information and communications technology network against unauthorized access by filtering the traffic and rejection of unauthorized attempts of connection.

**Resource** — A physical or logical object possessed or entrusted to an organization, for which it has an actual or contractual value.

**Event** — A fault or potential cause of an incident that can cause damage in the OT system.

#### 4. BASE MATERIALS

1. Department of Homeland Security: Cyber Security Procurement Language for Control Systems - September 2009.
2. Standards and good practices of protection of critical infrastructure - Industrial Automatics in the crude oil and natural gas sector - RCB Handbook of 2017.
3. Standards and good practices of protection of critical infrastructure - Industrial automatics in the power generation sector - RCB Handbook of 2017.

4. Operational Guidelines for industrial Security - a handbook of Siemens AG Company of 2013.

#### Related documents:

1. ZSZ procedure **PZM.PR01 Execution of technical purchases and services**
2. ZSZ procedure **PZM.PR02 Supervision of equipment for monitoring and measurements**
3. ZSZ Instruction [PBT.I02 Password policy in control systems](#)
4. ZSZ Instruction [PBT.I03 Technical Device Standard - SUT E Electric branch](#)
5. ZSZ Instruction [PBT.I04 Technical Device Standard - SUT M Mechanical branch](#)

## 5. GENERAL GUIDELINES

### 5.1 Scope

The development includes general requirements for designing and selection of object automation devices and control and visualization systems and also the Terms of acceptance of automation devices and systems in the scope of the OT cyber security. Prior to commencement of execution of the technical design or selection of a device all the technical requirements, standards and guidelines included in this development should be agreed upon.

**Remark: All deviations from the technical guidelines included in this document should be agreed and accepted in writing by the Investor.**

### 5.2 Exclusions

The following systems are excluded from the design of the Control and Measurement Instruments and Automation branch.

1. Control and visualization systems dedicated to the building automatics (Building management systems **BMS**).
2. Control and visualization systems dedicated to the railroad traffic (e.g. Railroad traffic control system **SSRK**).
3. Control and visualization systems dedicated to the power generation (Control and supervision system **SSiN**).
4. Dispatcher systems.

### 5.3 Standards and regulations in force at the PCC Rokita Company

#### 5.3.1 Legal requirements

1. [PBT.I02 Password policy in control systems](#)
2. [ORDINANCE NO. 64/2011 OF DIRECTOR GENERAL OF the PCC Rokita SA Company dated 16 December 2011 on the system of technical protection of the property.](#)

### 5.3.2 Standards and technical specifications

## 5.4 General requirements for designing and acceptance in force at PCC Rokita

### 5.4.1 Terms of acceptance of automation devices and systems

1. Excluding or removal in a network device of any services or programs that are not required for the normal operation of the system thus removing potential security holes.
2. Scanning of ports is a normal method for ensuring the existence of required services and absence of unnecessary services. Scanning of ports should be executed before the FAT with a representative, fully functional system configuration. All the input/output ports (I/O) must be scanned in respect of the UDP and TCP The scanning should be executed before the FAT and again before the SAT. The scanning of the ports can be rarely used in the production systems. In most of the cases the scanners disturb their operation.
3. Configuration of the hosts with the least access to a file and access to the account as well as supplying of the configuration documentation.
4. Configuration of necessary system services to be executed with the lowest level of worker's authorization for these services and delivery of the configuration documentation.
5. Switching off using the software or physical disconnecting of all the unnecessary communication ports and removable drives or ensuring a design of barriers and supplying the resulting documentation.
6. Securing the BIOS against unauthorized changes, unless it is not possibly technically, in this case the Supplier will document it and provide moderating means.
7. A list of all the switched off or removed USB ports, CD/DVD drives and other removable multimedia devices.
8. Configuration of the network devices in order to limit access to/from definite locations, in relevant instances and supplying of the configuration documentation.

## 6. Solutions for ensuring the requested cyber security level on different protection layers.



Figure 1 Protection layer of cyber security in the OT systems

### 6.1 Installation security

1. The regulations in force at the PCC Rokita Company must be observed and especially ORDINANCE NO 64/2011 of the DIRECTOR GENERAL of the PCC Rokita SA dated 16 December 2011 on technical protection of the property.

#### 6.1.1 Physical access to cybernetic elements

1. The Supplier/Contractor should supply a detailed plan of relevant mechanisms of physical security.
2. The Supplier/Contractor should provide casings for the elements of the control system featuring locks with patented keys or combination padlocks with a MASTER key (e.g. for servers, terminals and network hardware).
3. The Supplier/Contractor should provide a locking device with at least two keys in case protection with a lock is necessary depending on the Ordering Party requirements.
4. The rooms, in which the main elements of the control system are located (e.g. Servers, terminal computers, network hardware, automation stations) should be locked with keys.

5. The Supplier/Contractor should verify and supply documentation confirming that unauthorized recording devices (e.g. key loggers, cameras and microphones) are not installed/mounted in.
6. The Supplier/Contractor should check and supply confirming documentation within the FAT and SAT that physical security components (e.g. protection devices, locks) have been tested.
7. The Supplier/Contractor should disconnect (deactivate) within the FAT and SAT both via the hardware as well as software all unused ports and input/output devices (see section **6.3.1**).
8. The Supplier/Contractor should provide checks and documents within the SAT procedures, which confirm that all the protection means of the rooms housing the main elements of the control system (e.g. servers, terminal computers, network hardware, automation stations) operate correctly.

#### **6.1.2 Physical access to the areas (perimeter protection)**

1. Perimeter protections comprise i.a. fencing, walls, completely locked buildings, gates or entrance doors, car barriers, lighting, relevant land shaping, surveillance systems, alarm systems and guards. The physical protection can also comprise recording of entry and exit and also recording in a room or zone, most frequently via an admission system using pass cards.
2. Failure to define the areas with the perimeter protection may render physical break-ins easier. The ability to detect violation of the zone is the key to prevent physical attacks.
3. Only the personnel that needs the access to the particular location receives permission for access. The protected areas with the critical equipment cannot include the equipment or functions, which require access of many people including Contractors.
4. Physical monitoring of the security (e.g. Cameras, card availability) should send alarms to the plant control center (Plant Securities). For the reasons of cyber security these alarms must not be located on the same network as the process control and visualization devices.
5. The Supplier/Contractor should provide the assessment of the local security with special attention paid to the parameters or events, which can influence the physical trespass of intruders. The result of this assessment should be a documented physical plan of object protection, which should be submitted to the Ordering Party.
6. Supplier/Constructor should verify and supply the documentation confirming that guards such as walls, buildings or fencing adequately protect the zone against trespassing of pedestrians, vehicles and dangerous objects.
7. The Supplier/Contractor should allow the access within the protected zone only for these workers, contractors or guests who have been verified both by the Supplier/Contractor as well as by the Ordering Party.



8. The Supplier/Contractor should provide keys, which prevent copying or coded entrance passes to all locks.
9. The Supplier/Contractor should test and provide documentation within the FAT tests, which confirm that all the alarm systems detect all the instances of trespassing the zone minimizing false alarms.
10. Within the SAT tests The Supplier/Contractor will provide mechanisms of access control by the Ordering Party.
11. The Supplier/Contractor should provide for the Ordering Party within the SAT tests the expected functionality of physical protection.
12. The Supplier/Contractor should provide relevant training at site with operators and guards (security services) before commissioning for operation.
13. The Supplier/Contractor should verify and supply the documentation concerning all functions of remote alarm, supervision and blocking within the SAT tests before starting up.
14. The Supplier/Contractor should provide keeping of the access control mechanisms in safe configuration.
15. The Supplier/Contractor should perform validation of the results in the scope of the perimeter protection in compliance with the terms defined in the agreement/order.
16. The Supplier/Contractor should replace all locks, blockade codes, entrance passes etc. in compliance with the terms defined in the agreement/order.
17. The Supplier/Contractor should coordinate changes of access control with the Ordering Party in order to update physical protection.

### 6.1.3 Physical access to manual override

1. Physical access to manual override should be strictly limited exclusively to authorized personnel.
2. Unauthorized access to manual override constitutes a risk of damage or trespassing to the system therefore it has to be protected.
3. The Supplier/Contractor should provide the means for physical protection of the manual override mechanism by locked housing or a blocking function installed into the manual override itself.
4. Prior to starting up the Supplier/Contractor should verify and supply the documentation concerning all functions of the remote alarm, supervision and blocking.
5. The Supplier/Contractor should keep the mechanisms of manual override in safe configuration during the period determined in the agreement/order.
6. The Supplier/Contractor should perform validation of the results in respect of protection of the manual override mechanisms.



7. The Supplier/Contractor should replace all locks, blocking codes, entrance passes etc. according to the principles determined in the agreement/order.

## **6.2 Network security**

### **6.2.1 Perimeter protection**

#### **6.2.1.1 Firewalls**

1. The Supplier/Contractor will provide firewalls and sets of firewall rules between the network areas or render available sets of firewall rules, if the firewall is not supplied by the Supplier/Contractor.
2. After awarding the order the Supplier/Contractor grants detailed information concerning the whole communication, including the protocols required by the firewalls and identifies each network device that initiate communication in compliance with the relevant sets of rules.
3. The Supplier/Contractor checks if the SAT procedures comprise validation and documentation of the requirements. All default names of users, passwords or other security codes configured by the Supplier/Contractor or manufacturer must be changed at this moment.
4. Make sure to continue checking for appearance of firmware updates (patches) for firewalls.

#### **6.2.1.2 System detecting break-ins to network (NIDS - Eng. Network Intrusion Detection System)**

1. The Supplier/Contractor ensures traffic profiles with expected communication pathways, network traffic, and expected limits of utilization, in case of the NIDS based on anomalies.
2. The Supplier/Contractor will provide necessary signature dot the NIDS based on signatures.
3. Upon awarding of an order the Supplier/Contractor will supply configured NIDS and/or supply information for configuration of the NIDS.
4. The Supplier/Contractor will check the NIDS during the whole FAT process and will periodically introduce relevant malware. The Supplier/Contractor will examine log files and check the expected results.
5. The Supplier/Contractor will use the NIDS during the whole FAT process and periodically introduce relevant malware. The Supplier/Contractor will examine log files and check the expected results.
6. The Supplier/Contractor adjusts signatures and adapts thresholds in order to diminish the number of false alarms and minimize false results.
7. The Supplier/Contractor will update configuration of the NIDS and/or documentation if necessary after implementation of changes.

#### **6.2.1.3 System of detection of connection attempt (Canaries)**

1. The Supplier/Contractor provides “Honey pots” analyzing unauthorized connection and/or “Canaries” (Canary), which signal that there was a connection attempt in order to provide passive monitoring of the network.

2. The Supplier/Contractor will configure or submit information for configuration of the “Canary” with the warning software in order to point out to unauthorized connection attempts.
3. The Supplier/Contractor will check if the SAT procedures include written validation and documentation of the requirements. All default user names, passwords or other security codes configured by the Supplier/Contractor or manufacturer must be changed at this moment.
4. The Supplier/Contractor will perform reconfiguration of the “Canary(-ies)” as needed, when the topologies of network addresses change.

### 6.2.2 Network addressing and name recognition

1. In order to defend against DNS attacks the DNS servers for the network of the internal control should be located inside of the firewall and should be separated from the DNS servers in the corporate network. The DNS servers for the control system should be authoritative only for the address space of the control system network . It means that the DNS servers should contain complete information about the zone ( reflection of the names onto IP addresses) only for the hosts in the control system network. It is ideally when the control system network is isolated and the hosts will not have to solve the external names. However, if the hosts have to recognize the names of hosts from outside of the trusty control systems the queries should be directed to the DNS server of the control system, which sends the queries across the firewall to the DNS server in the corporate network.
2. Recommendations concerning safe DNS configuration:
  - Use of the servers dedicated for the DNS and related services and switching off all the unnecessary services.
  - Use of the newest software versions with current updates.
  - Periodical creation of backup copies and reviewing of the DNS configuration files and performance of integrity checks in order to check the integrity of configuration files, zone data and other DNS files.
  - Starting up of the DNS servers as a user other than root. Switching on of the access control to enable only the particular persons to create remove or modify the DNS data.
  - Switching on of prevention of pollution of the cache memory.
  - Limiting of addresses, which can direct queries to the DNS servers of the control system in order to control the system hosts.
  - Limiting of zone transfers only to the trusted hosts and authentication of the zone transfers.
  - Use of a static addressing scheme. If dynamic addressing is used, allow for dynamic updating only from trusted hosts.
  - Configuration of the firewall in order to enable communication between the control system and the corporate DNS servers only in ports UDP and TCP 53.

- Permitting special remarks for hosts with many IP addresses for redundancy.
3. In case of awarding an order prior to concluding the Agreement, the Supplier/Contractor will supply recommended network addressing methodology and name recognition.
  4. The Supplier/Contractor will provide the means of verification of the configuration file integrity, particular areas and other DNS files (e.g. such integrity checking can be executed using a HIDS device).
  5. After awarding of the contract the Supplier/Contractor should supply configured DNS servers or the information for configuration of a DNS server (servers), which fulfills the initially agreed protection standard.
  6. The Supplier/Contractor should treat the address information as sensitive for business and protect it.
  7. The Supplier/Contractor will install and start up DNS servers supplied by them in continuous way during the whole FAT process.
  8. The Supplier/Contractor will verify all servers of the domains and the hosts in the domain taking part in testing can be resolved by all client and server systems connected to the network.
  9. The Supplier/Contractor should document both the resolution for passing forward (a host name into the IP address) as well as reversely (an IP address into the host name).
  10. The Supplier/Contractor will start up the DNS server during the whole SAT process.
  11. The Supplier/Contractor will check if all the domain servers and hosts in the domain taking part in testing are recognized by all the customer and server systems connected to the network.
  12. The Supplier/Contractor should document both the resolution for passing forward (a host name into the IP address) as well as reversely (an IP address into the host name).
  13. The Supplier/Contractor will provide a continuous process of correction management for the DNS system and related services such as DHCP.

### 6.2.3 Remote access

#### 6.2.3.1 TCP/IP

1. The Supplier/Contractor provides physical and cybernetic functions, including i.a. Authentication, encoding, access control, event and communication registration, monitoring and alarming in order to protect a device and configuration computer against unauthorized modification or use.
2. The Supplier/Contractor should clearly identify physical and cyber security functions and supply the methodology for preserving the functions, including changing of the setting from the ones configured by the supplier or the default conditions of the manufacturer.
3. The Supplier/Contractor checks if adding of security functions does not exert a negative impact on communication, delay, bandwidth and response time, including during the SAT after connection to the existing hardware.

4. The Supplier/Contractor removes or switches off all elements of the software, which are not required for operation and maintenance of the device before the FAT. The Supplier/Contractor will supply documentation concerning all that has been removed and/or switched off.
5. The Supplier/Contractor will provide before the expiry of the negotiations period appropriate protocol stack updates and/or workarounds in order to mitigate all the holes related to the product and maintain the determined system security level.
6. The Supplier/Contractor verifies and supplies documentation confirming that the security system (SIS) is certified after switching on the protecting devices.
7. The Supplier/Contractor will use the TCP/IP protocol implementation, which will be fully compliant with the current RFC documents of the TCP/IP protocol.
8. The Supplier/Contractor will supply the product compliant with IPv6.
9. The Supplier/Contractor will provide the possibility of traffic monitoring in the encoding system.
10. After awarding the order the Supplier/Contractor will provide independent, external verification of the implementation of IPv6 protections (e.g. using fuzzing techniques). The Supplier/Contractor will supply the documentation of the results of the independent IPv6 security verification by the third party.
11. The Supplier/Contractor should diminish all the holes discovered during testing of implementation of IPv6 and supply the documentation of results.
12. The Supplier/Contractor should verify and supply the physical and cyber functions documentation, including i.a. authentication, encoding, access control, logging of communication and events, monitoring and alarming in order to protect the system against unauthorized modifications or use.
13. The Supplier/Contractor should verify and supply documentation that all the accepted updates and security corrections are installed and tested in the beginning of FAT.
14. The Supplier/Contractor should verify and supply the documentation that all the unused software and services have been removed or switched off.
15. The Supplier/Contractor will create the base line of communication and system configuration, including i.a. cyber security functions, software, protocols, ports and services and will supply the documentation describing each item and changes.
16. The Supplier/Contractor performs verification using cyber security scans of the system and provides the documentation that addition of the safety functions does no adversely effects correct communication, delay, bandwidth and response time.
17. The Supplier/Contractor should verify and supply documentation and changes of the physical and cyber security functions, including i.a. authentication, encoding, access control, logging of events and communication, in order to protect the system computer against unauthorized modification or use.

18. After finishing the SAT, the Supplier/Contractor will create the base line of communication and system configuration, including i.a. cyber security functions, software, protocols, ports and services and will render available the documentation describing all the changes.
19. The Supplier/Contractor will check and supply the documentation that all the default accounts configured by the manufacturer, user names, passwords, security setting, security codes and other methods of access have been changed, switched off or removed.
20. The Supplier/Contractor ensures maintenance of the supplied security functions of the system.
21. The Supplier/Contractor documents all supplements and changes in the remote access device during the guarantee period.
22. The Supplier/Contractor should verify permissions and settings of protections in the base system prior to supplying updates or exchanges in order to maintain the determined security level of the system.

#### **6.2.3.2 VPN**

1. The target location of the VPN server and its ownership should be agreed for each implemented VPN. Good solution is placements of the VPN server in the DMZ zone separated from the control network and permitting the user to connect with the control network using the authentication process required for the user who gains access to the network locally. VPN are strongly dependent on the firewall rules and as such they should be taken into consideration at demand for firewall solutions.
2. The Supplier/Contractor ensures physical and cyber secure functions, including i.a. multicomponent authentication (e.g. a security token, known key and/or certificate), encoding, access control, logging of events and communication, monitoring and alarming in order to protect the system and configuration computer against unauthorized modification or use.
3. The Supplier/Contractor should clearly identify physical and cyber security functions and supply the methodology for preserving the functions, including changing of the setting from the ones configured by the supplier or the default conditions of the manufacturer.
4. The Supplier/Contractor checks if addition of a security function does not exert a negative impact on communication, delay, bandwidth and response time, also during the SAT after connection to existing hardware. Supplier Contractor documents the afore mentioned verifications.
5. The Supplier/Contractor removes or switches off all components of software, which are not required for operation and maintenance of the device before the FAT. The Supplier/Contractor will supply documentation concerning what has been removed and/or switched off.
6. The Supplier/Contractor will provide before the expiry of the negotiations period appropriate protocol stack updates and/or workarounds in order to mitigate all the holes related to the product and maintain the determined system security level.
7. The Supplier/Contractor verifies and supplies documentation confirming that the security system (SIS) is certified after switching on the protecting devices.
8. The Supplier/Contractor will provide a DMZ zone outside the control network, so as the VPN server could reside.

9. The Supplier/Contractor will use different methods of authentication in order to establish the access to the control network and VPN connection.
10. The Supplier/Contractor should verify and supply documentation for physical and cyber security functions, including i.a. multi element authentication (e.g. a security token, known key and/or certificate) encoding, access control, logging of events and communication, monitoring and alarming in order to protect the system against unauthorized modifications or use.
11. The Supplier/Contractor should verify and supply documentation that all accepted updates and security corrections are installed and tested in the beginning of the FAT.
12. The Supplier/Contractor will create a base line for communication and configuration of the system, including i.a. cyber security function, software, protocols, ports and services and will supply the documentation describing functionality of each element and change.
13. The Supplier/Contractor should verify and supply the documentation that all unused software and services have been removed or switched off.
14. The Supplier/Contractor will check and supply the documentation that all the default accounts configured by the manufacturer, user names, passwords, protection setting, security codes and other access methods are changed, switched off or removed.
15. The Supplier/Contractor will provide before the expiry of the negotiation period relevant updates and corrections in the course of identification of the problems related with the security, in order to keep the determined security level of the system.
16. The Supplier/Contractor should verify permissions and settings of the protections in the base system before delivery of updates or replacements in order to keep the determined security level of the system.
17. The Supplier/Contractor ensures maintenance of the supplied security functions of the system.
18. The Supplier/Contractor documents all completing and changes in the remote access device during the guarantee period.

## 6.2.4 Network partitioning

### 6.2.4.1 Network devices

1. The Supplier/Contractor will provide and verify the methods of management of the network devices and changing addressing diagrams.
2. The Supplier/Contractor should verify and supply the documentation that the interface of network configuration management is secured.
3. The Supplier/Contractor will provide and verify the ACL lists, port security address lists and improved security for port duplications.
4. The Supplier/Contractor should remove or deactivate unused network configuration and management functions on the network devices.

method.

5. The Supplier/Contractor will provide the principles of the firewall for the input and output traffic on the basis of refusal rules for all.
6. The Supplier/Contractor provides the NIDS principles and tool for reviewing of log books, which check operation of the firewall and detect unusual traffic.
7. The Supplier/Contractor will provide the architecture of NIPS, which will operate with a communication method.
8. The Supplier/Contractor will provide the VPN Ethernet hubs configured with filters and port protections and will supply the documentation concerning the network devices installed with the security settings.
9. The Supplier/Contractor should scan the network ports, signal formation and functionality of traffic for each port..
10. The Supplier/Contractor provides updates and corrections in order to maintain the determined security level of the system.
11. The Supplier/Contractor should verify security permissions and settings in the basic system before supplying any updates and replacements.

#### **6.2.4.2 Network architecture**

1. Network simplification of the network should be the priority during designing of the initial architecture or the rules of the firewall. The versatility of the protocols open for the data should be limited to the minimum. The data modified retransmitted repeatedly, such as the data base, Internet and FTP should be at first moved to the DMZ zone, modified in the DMZ zone and sent from the DMZ to other networks. The contractor will provide and verify a method of management of the network devices and changeable addressing diagrams.
2. The Supplier/Contractor should provide and document secure network architecture, in which the higher security zones establish communication with less secure zones.
3. The Supplier/Contractor should provide and document the design for all communication pathways between the networks of different security zones via the DMZ.
4. The Supplier/Contractor should verify and document that the unpair points as established between the network partitions and provide methods of insulation of subnets in order to continue limited operations.
5. The Supplier/Contractor should provide and document adapted rules of filtering and monitoring for all the security zones and an alarm for unexpected traffic.
6. The Supplier/Contractor should supply and document the DMZ zone, which is limited to communication, in which the whole traffic is monitored, alarmed and filtered.
7. The Supplier/Contractor should provide and document output filtering and alarms concerning unexpected traffic in the security zones.



8. The Supplier/Contractor should determine and document all sources and destinations with an enforced communication start, even during restarting between the security zones.
9. The Supplier/Contractor should supply and document two DMZ architectures using different products performing the same functionality parallelly.
10. The Supplier/Contractor should supply and document a flying mechanism of a single DMZ architecture operating in the parallel configuration without disturbing the second DMZ operating parallelly.
11. The Supplier/Contractor should assess demands and provide updates and patches within the process of identifying holes in order to maintain the determined security level of the system.. The Supplier/Contractor will check and document that the security profile of the network architecture is preserved.

## 6.3 System integrity

### 6.3.1 System “hardening”

#### 6.3.1.1 Removing of unnecessary services and programs

1. A recommended activity of hardening is switching off or removing in a network device of any services or programs, which are not required for normal operation of the system, thus removing potential holes in protections.
2. Scanning of ports is a normal method for ensuring the existence of required services and absence of unnecessary services. Scanning of ports should be performed prior to the FAT with the representative, fully functional system configuration. All the input/output ports (I/O) must be scanned in respect of the UDP and TCP. The scanning should be executed before the FAT and again before the SAT. The scanning of the ports can be rarely used in the production systems. In the majority of instances the scanner disturb their operation.
3. After awarding the order the Supplier/Contractor will supply the documentation that describes in details all applications, tools, system services, scripts, configuration files, data bases and all other required software as well as relevant configurations, including versions and/or levels of corrections for each of the computer systems related to the control system.
4. The Supplier/Contractor will supply a list of services required for any computer system with started applications of the control system or required for connection of the control system applications. The list comprises all ports and services required for normal operation and also all other ports and services required for operation in the safe mode. The list should also comprise an explanation or reference to justify why each service is necessary for operation.
5. The Supplier/Contractor will check and supply documentation that all services are patched to the current status. The Supplier/Contractor provides, within the period of previous negotiations, relevant updates of the software and services and/or workarounds to mitigate all the holes in protections related to the product and maintain the determined security level of the system.

The Supplier/Contractor removes and/or switches off all software components, which are not required.



for operation and maintenance of the control system before the FAT. The Supplier/Contractor will supply the documentation concerning what has been removed and/or switched off. The software to be removed and/or switched off comprises, but is not limited to:

1. Games,
  2. Controllers for network devices, which have not been supplied.
  3. Services of sending messages (e.g. MSN, AOL IM).
  4. Servers or clients of unused Internet services.
  5. Software compilers in all work stations of users and servers, except for programmer work stations and servers.
  6. Software compilers for languages that are not used in the control system.
  7. Unused network and communication protocols.
  8. Not utilized administration tools, diagnostics, network management and system management functions.
  9. Backup copies of files, data bases and programs used only during creation of the system.
  10. All unused data and configuration files.
  11. Illustrative programs and scripts.
  12. Unused tools for document processing (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice etc.).
6. The Supplier/Contractor will check if the Ordering Party requires the results of cyber scanning (as a minimum of the hole in securities and active scanning of a port, with most updated signature files) started in the control system as the basic activity of the FAT. This assessment is then compared with the list of the required services, state of corrections and documentation in order to confirm the requirement. Other foreseen means comprise:
1. The Supplier/Contractor provides for each network device or class of devices (e.g. server, work station and switch) the following documents concerning configuration:
    - Network services required for operation of such a device. A list of service names, protocol (e.g. TCP and UDP) and port range.
    - Dependences on the basic services of the operation system.
    - Dependences in network services residing in other network devices.
    - All the configuration parameters of the software required for correct operation of the system.
    - A certified operation system, driver and other software versions installed in the device.
    - Results found by the vulnerability scans with mitigations affected. ((The results discovered by scans vulnerable to an attack with an adverse impact).
  2. The Supplier/Contractor should install updates of the internal software available for the computer or network device certified by the system producer at the time of installation and supply the documentation.
  3. The Supplier/Contractor will supply a collective table indicating each communication path required by the system with the consideration of the following information:
    - a. The name of the source device and control of the access to the data carrier (MAC) and/or the IP address.
    - b. The name of the target device and MAC and/or the IP address.
    - c. The protocol (e.g. TCP and UDP) and the port or the range of ports.
  4. The Supplier/Contractor performs network stages of validation and documentation for each device:

Full caning of the TCP and UDP on ports 1-65535. This scanning should be performed during simulation of “normal operation of the system”.

7. The Supplier/Contractor will compare the results of the cyber security scanning started up in the system, as the basic operation of the SAT with the list of the required services, state of corrections and required documentation. After completion of the SAT and before changing or starting up, the above cyber safety scanning (with the newest signature files) must be started up again.

#### **6.3.1.2 HIDS**

1. The Supplier/Contractor provides configured HIDS devices and/or supply information for configuration of the HIDS devices including static file names, dynamic patterns of file names, system accounts and user accounts, executions of unauthorized code, using of the host and process of permission sufficient for configuration of the HIDS.
2. The Supplier/Contractor should configure the HIDS devices in the way so as to log all connections of the system accounts and user accounts. This log should be configured in such a way so as the alarm would be displayed for the operator or security employee in case of occurrence of unusual situation.
3. The Supplier/Contractor should present the recommended HIDS configuration in the way, which exerts no negative influence on the functions of the operating system or business objectives.
4. The Supplier/Contractor should present recommended tools for reviewing the logs and notices.
5. The Supplier/Contractor should configure devices as “append only”, in order to prevent changes of the records on the local memory devices.
6. The Supplier/Contractor will manage the HIDS during the whole process of the FAT and periodically input relevant malware. The Supplier/Contractor will examine log files and check the expected results. The FAT procedures should comprise validation and documentation of this requirement.
7. The Supplier/Contractor will manage the HIDS during the whole process of the SAT and periodically input relevant malware. The Supplier/Contractor will examine log files and check the expected results. The SAT procedures should comprise validation and documentation of this requirement.
8. The Supplier/Contractor should generate the picture of the system at the end of the SAT, which will be used later as the control base line.

#### **6.3.1.3 Changes to file system and operating system permissions**

1. The Supplier/Contractor should configure the hosts with the least access to the file and access to the account and supply the documentation of the configuration.
2. The Supplier/Contractor should configure necessary system services for execution with the lowest level of the user permissions for this service and supply the configuration documentation.
3. The Supplier/Contractor will document that the change or switching off the access to such files and function has been finished.

4. The Supplier/Contractor should ensure within the FAT procedures acceptance and documentation of the assigned permissions.
5. The Supplier/Contractor should ensure within the SAT procedures acceptance and documentation of the assigned permissions.

#### **6.3.1.4 Hardware configuration**

1. The Supplier/Contractor should switch off, using the software or physical disconnection, all unnecessary communication ports and data carrier removable drives or ensure designing of a barrier and supply the results in documentation.
2. The Supplier/Contractor should provide BIOS protection against unauthorized changes, unless it is technically not possible, in such instance the Supplier will document it and provide mitigating means.
3. The Supplier/Contractor should supply a written list of all switched off or removed USB ports, CD/DVD drives and other removable multimedia devices.
4. The Supplier/Contractor should configure the network devices in order to limit access to/from the particular locations, in relevant instances and supply configuration documentation.
5. The Supplier/Contractor should configure the system in order to provide the system administrators the possibility of repeated switching on of the devices, if the devices are switched off via the software and supply documentation of the configuration.
6. The Supplier/Contractor should ensure within the FAT procedures approval and documenting of a switched off or locked physical access and removed drivers.
7. The Supplier/Contractor should ensure within the SAT procedures approval and documenting of a switched off or locked physical access and removed drivers.

#### **6.3.1.5 “Heartbeat” signals**

1. The Supplier/Contractor should identify “Heartbeat” signals or protocols and recommend including the monitor into the network.
2. After awarding the order the Supplier/Contractor will supply packages of the “Heartbeat” signal definitions and examples of the “Heartbeat” traffic, if the signals are incorporated in network monitoring.
3. Within the FAT procedures the Supplier/Contractor will provide documentation of the requirements.  
The Supplier/Contractor will create the base line of the “Heartbeat” communication traffic, in order to take into consideration the frequency, package sizes and expected package configurations.
4. The Supplier/Contractor will ensure within the SAT procedures the documentation of the requirements.  
The Supplier/Contractor will create the base line of the “Heartbeat” communication traffic and check the results in respect to the FAT documentation.

#### **6.3.1.6 Installation of operation systems, applications and other firm software updates**

1. The Supplier/Contractor will run the process of management and updating of patches.

Before concluding the Agreement the Supplier submits detailed information concerning management of the patches and updating process. The responsibility for installation and updating of correction should be determined.

2. The Supplier/Contractor should notify on the known holes that have an impact on the operation system supplied or required by the Supplier, applications and software of the third parties in the period of advance negotiation after announcement to the public.
3. The Supplier/Contractor should submit notifications on the corrections that exert an impact on the security in the period of advance negotiation determined in the process of correction management. Before distribution the Supplier uses, tests and approves relevant updates and/or workarounds in the base reference system. Mitigation of these weak points will take place in the period of initial negotiations.

### 6.3.2 Session management

1. The Supplier/Contractor should not allow for submitting the data authenticating a user in the form of an ordinary text.
2. The Supplier/Contractor will provide the strongest encoding method commensurable to the technological platform and limitations of the reaction time.
3. The Supplier/Contractor must not allow for:
  - numerous, simultaneous logging in order to preserve logging information between the sessions
  - Providing a function of automatic completing during logging
  - anonymous logging.
4. The Supplier/Contractor will set the way of logging out and time limit in the user account.
5. The Supplier/Contractor checks if the SAT procedures comprise validation and documentation of requirements.

### 6.3.3 Management and policy of passwords/authorizations

1. Instruction ZSZ **PBT.I02 Password Policy in control systems must be observed.**
2. The Supplier/Contractor provides a configurable system of password management for an account, which enables selection of the password length, frequency of changes, setting of the required password complexity, number of logging attempts, no activity logging out from a session, screen blocking according to applications and refusals of reusing the same password.
3. The Supplier/Contractor should not store passwords in an electronic form or in the documentation supplied by the Supplier in a legible form, unless the data carrier is protected physically.
4. The Supplier/Contractor should control the access to the configuration interface of the account management system.
5. The Supplier/Contractor checks, if the SAT procedures cover checking of correctness and password documentation as well as the authentication principles and management.

#### 6.3.4 Encoding practices

1. The Supplier/Contractor will supply the inspection documentation for the code and other stages of software creation used to assess software security. The software subject to these inspection comprises both applications developed by the Suppliers/Contractors as well as any other source code, on which the Supplier/Contractor exercises control and which constitute necessary part of the control system. The software of other manufacturers integrated with the products of the Suppliers/Contractors should be evaluated for the holes in the protections. The experience demonstrates that the system integration often contributes to the overall vulnerability of the system to attack..
2. The Supplier/Contractor should direct themselves with the following principles at creation of the code:
  - a. The input data must be checked in respect of sensible values.
  - b. The data files should be encoded.
  - c. You should consider influence of the operation systems and other libraries of the third parties on the security.
  - d. You should make sure that the operation systems and other libraries of the third parties feature the principles of updating.
  - e. It cannot be allowed to overfill the buffer.
  - f. You should check if the log files are not changed.
  - g. You should use complex checking of authenticity and integrity in the data communication between the processes.
  - h. You should apply the design and code review.
  - i. You should check if neither passwords nor encoding keys are written in the code.
  - j. You should create a code in such a way so as the blocks and regulations were not created from the devices outside of the internal control network.
3. The Supplier/Contractor should supply the source codes of the created software.
4. The Supplier/Contractor will supply the documentation of the development practices and standards used for the software of the control system written by the manufacturer, including the firmware used to ensure a high level of protection against unauthorized access.
5. The Supplier/Contractor should perform the FAT covering validation and documentation of the software creation process and/or review of the code.
6. The Supplier/Contractor should perform the SAT covering validation and documentation of the software creation process and/or review of the code.
7. The Supplier/Contractor checks is the software updates and patches (corrections) are checked in compliance with the same software development process or the review plan.

#### 6.3.5 Fault correction

1. The fault correction refers to activities, which should be performed when faults are detected in the software of the control system, in hardware and system architectures created by or under

control of the Supplier/Contractor. Hints concerning corrective actions, repairs or monitoring are necessary in order to mitigate all the holes in the protections related to vulnerability. The vulnerabilities and faults are usually strictly maintained until the remedy means are rendered available. However, some of the holes in the protections are publicized before a correction is developed and then it is necessary to mitigate these vulnerabilities.

2. The history of faults and remedy steps/patches is necessary to be able to withdraw the particular corrections.
3. The Supplier/Contractor should supply a documented fault remedy process.
4. The Supplier/Contractor will provide relevant updates of the software and/or the methods to be applied in order to mitigate all the holes in the protections related to vulnerability for the period defined in the agreement/order.
5. The Supplier/Contractor should supply the FAT documentation concerning fault validation and remedying.
6. The Supplier/Contractor should supply the SAT documentation concerning fault validation and repairing.
7. The Supplier/Contractor will keep for the period defined in the agreement/order a principal list of all the faults and corrective measures for the purpose of an audit.

#### **6.3.6 Detection and protection against malware**

1. The Supplier/Contractor should disclose the existence and causes of all the known or identified codes of the backdoor type.
2. The Supplier/Contractor should fulfill one of the two conditions:
  - a. Providing a system of detection of malware software based on the host for the network of the control system. The Supplier/Contractor checks correctness of operation of the system in order to detect harmful software of the host, subjecting to a quarantine (instead of an automatic removal) of the suspected files and supplying a diagram of signature updating. The Supplier/Contractor tests the most important updates of applications for detection of the malware and supplies the data concerning efficiency measurement concerning influence of the use of application for detection of the malware in the active system. The measurement cover i.a. network utilization, processor utilization, memory utilization and all other influences on the normal communication processing.
  - b. If the Supplier/Contractor does not supply a real diagram of detection of the host malware, the Supplier/Contractor should propose products used to detect the malware and provide hints concerning configuration of malware detection, which will work with the products of the Supplier/Contractor.
3. The Supplier/Contractor should log the system efficiency measurements within the FAT and SAT, which include the system of malware detection and without it.
4. The Supplier/Contractor should document all the known or identified backdoors within the FAT and SAT.
5. The Supplier/Contractor should keep the logs of applications detecting the malware for the period defined in the agreement/order for potential investigations and court cases.

6. The Supplier/Contractor should update the software for malware detection in compliance with the requirements so as it would be effective in case of the newest malware. With changes of the malware variants you should apply new, more precise or readjust signatures.
7. The Supplier/Contractor should disclose existence and causes of all known or identified codes of the backdoor type.

## 6.4 Terminal devices

### 6.4.1 Intelligent Electronic Devices (IED)

1. The Supplier/Contractor should ensure physical and cyber secure functions comprising i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
2. The Supplier/Contractor should clearly identify the features of physical protection and cyber secure functions as well as supply the methodology of maintaining these functions, including the methods of changing the settings from the manufacturer or The Supplier/Contractor default settings.
3. The Supplier/Contractor should check if addition of the security function does not exert a negative impact for communication, delays, bandwidth and reaction time, also during the SAT, when connected to the existing hardware.
4. The Supplier/Contractor should remove or switch off all elements of the software that are not required for operation and maintenance of the device before the FAT. The Supplier/Contractor should supply the documentation concerning what has been removed and/or switched off.
5. The Supplier/Contractor should provide relevant updates of the software and services to mitigate all the holes in protections related to the supplied device and should keep the determined system security level in the period defined in the agreement/order.
6. The Supplier/Contractor should verify and supply the documentation confirming that the device security system (SIS/ESD) will be certified after switching on of the protective devices.
7. The Supplier/Contractor should verify and document physical and cyber security during the FAT and SAT, including i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
8. The Supplier/Contractor should verify and supply during the FAT the documentation confirming that all the accepted security updates and patches are installed and tested.



9. The Supplier/Contractor should verify and supply the documentation confirming that the whole unused software and services have been removed or switched off.
10. The Supplier/Contractor should check and supply during the SAT the documentation confirming that all the default accounts, user names, passwords, security settings, safety codes and other access methods have been changed, switched off or removed.
11. The Supplier/Contractor should verify during the SAT using cyber safety scans and supply the documentation confirming that addition of the security function does not exert a negative impact on the relevant communication, delays, bandwidth, response time and bandwidth.
12. The Supplier/Contractor should provide during the period defined in the agreement/order updates and corrections for the devices when the security questions are defined, in order to obtain the determined system security level.
13. The Supplier/Contractor should create the base line of the updated communication and system configuration, including i.a. Cyber security functions, software, protocols, ports and services and will render available the documentation describing all changes.
14. The Supplier/Contractor should verify permissions and security settings in the base system before supplying updates in order to keep the determined level of the system security.
15. The Supplier/Contractor should document all completing and changes in the control system during the guarantee/maintenance period.

#### 6.4.2 Remote Terminal Units (RTU)

1. The Supplier/Contractor should ensure physical safety and cyber security functions comprising i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming in order to protect the device and configuration computer against unauthorized modifications or use.
2. The Supplier/Contractor should clearly identify the features of the physical protection and cyber security functions and supply the methodology of maintaining these function, including the methods of changing the settings from the manufacturer or The Supplier/Contractor default ones.
3. The Supplier/Contractor should check if adding of the security functions does not exert a negative impact on communication, delays, bandwidth and reaction time, also during the SAT, when it is connected to the existing hardware.
4. The Supplier/Contractor should remove or switch off all the software components that are not required for operation and maintenance of the device before the FAT. The Supplier/Contractor should supply the documentation concerning what has been removed and/or switched off.



5. The Supplier/Contractor should ensure relevant updates of the software and services in order to mitigate all the holes in protections related to the supplied device and should keep the defined system security level in the period determined in the agreement/order.
6. The Supplier/Contractor should verify and supply the documentation confirming that the tool security system (SIS/ESD) will be certified after switching on the safety devices.
7. The Supplier/Contractor should verify and document physical and cyber security during the FAT and SAT, including i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
8. The Supplier/Contractor should verify and supply during the FAT the documentation confirming that all the accepted security updates and patches are installed and tested.
9. The Supplier/Contractor should verify and supply the documentation confirming that the all unused software and services have been removed or switched off.
10. The Supplier/Contractor should check and supply during the SAT the documentation confirming that all the default accounts, user names, passwords, security settings, security codes and other methods of access have been changed, switched off or removed.
11. The Supplier/Contractor should verify during the SAT using the cyber security scans and supply the documentation confirming that addition of the security function does not exert a negative impact on the relevant communication, delay, bandwidth, response time and bandwidth.
12. The Supplier/Contractor should provide during the period defined in the agreement/order, updates and corrections for the devices, when the security questions are identified in order to keep the determined system security level.
13. The Supplier/Contractor should create the base line of the updated communication and system configuration, including i.a. cyber security functions, software, protocols, ports and services and will render available the documentation describing all changes.
14. The Supplier/Contractor should verify permissions and security settings in the base system before supplying updates in order to keep the determined level of the system security.
15. The Supplier/Contractor should document all completing and changes in the control system in the period of guarantee/maintenance.

#### 6.4.3 PLC Controllers

1. The Supplier/Contractor should provide the physical safety and cyber security functions comprising i.a. Authentication, encoding, access control, logging of events and communication, monitoring and alarming in order to protect the device and configuration computer against unauthorized modifications or use.

2. The Supplier/Contractor should clearly identify the features of the physical protection and cyber security functions and supply the methodology of maintaining these functions, including the methods of changing the settings from the manufacturer or The Supplier/Contractor default ones.
3. The Supplier/Contractor should check if adding of the security function does not exert a negative impact on communication, delays, bandwidth and response time, also during the SAT, when it is connected to the existing equipment.
4. The Supplier/Contractor should remove or switch off all the components of the software, which are not required for operation and maintenance of the device before the FAT. The Supplier/Contractor should supply the documentation concerning what has been removed and/or switched off.
5. The Supplier/Contractor should provide relevant updates of the software and services to mitigate all the holes in protections related to the supplied device and should keep the determined system security level in the period defined in the agreement/order.
6. The Supplier/Contractor should verify and supply the documentation confirming that the instrument security system (SIS/ESD) will be certified after switching on the safety devices.
7. The Supplier/Contractor should verify and document physical and cyber security during the FAT and SAT, including i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
8. The Supplier/Contractor should verify and supply during the FAT the documentation confirming that all the accepted security updates and patches are installed and tested.
9. The Supplier/Contractor should verify and supply the documentation confirming that the all unused software and services have been removed or switched off.
10. The Supplier/Contractor should check and supply during the SAT the documentation confirming that all the default accounts, user names, passwords, security settings, security codes and other methods of access have been changed, switched off or removed.
11. The Supplier/Contractor should verify during the SAT using the cyber security scans and supply the documentation confirming that addition of the security function does not exert a negative impact on the relevant communication, delay, bandwidth, response time and bandwidth.
12. The Supplier/Contractor should provide during the period defined in the agreement/order, updates and corrections for the devices, when the security questions are identified in order to keep the determined system security level.
13. The Supplier/Contractor should create the base line of the updated communication and system configuration, including i.a. cyber security functions, software, protocols, ports and services and will render available the documentation describing all changes.
14. The Supplier/Contractor should verify permissions and security settings in the base system before supplying updates in order to keep the determined level of the system security.
15. The Supplier/Contractor should document all completing and changes in the control system in the period of guarantee/maintenance.

#### 6.4.4 Sensors, devices/actuators and measuring instruments

1. The Supplier/Contractor should ensure physical safety and cyber secure functions comprising i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
2. The Supplier/Contractor should clearly define the features of the physical protection and cyber security functions and supply the methodology for keeping these functions, including the methods of changing from the default settings of the manufacturer or The Supplier/Contractor.
3. The Supplier/Contractor should provide safe communication interfaces (serial ones, Ethernet and wireless), including the possibility of filtering and monitoring of communication. Whereby the wireless communication should not be used.
4. The Supplier/Contractor should check if adding of the security function does not exert a negative impact on communication, delays, bandwidth and response time, also during the SAT, when it is connected to the existing equipment.
5. In case of application of the “smart” devices the Supplier/Contractor should remove or switch off all element of the software, which are not required for operation and maintenance of the devices before the FAT. Supplier/Contractor should supply the documentation concerning what has been removed and/or switched off.
6. In case of application of the “smart” devices the Supplier/Contractor should provide relevant updates of the software and services in order to mitigate all the holes in protections related to the supplied device and should keep the defined level of the system security in the period determined in the agreement/order.
7. In case of application of the “smart” devices the Supplier/Contractor should verify and supply the documentation confirming that the instrument security system (SIS/ESD) will be certified after switching the protection devices on.
8. The Supplier/Contractor should verify and document physical and cyber security during the FAT and SAT, including i.a. authentication, encoding, access control, logging of events and communication, monitoring and alarming for protection of the device and configuration computer against unauthorized modifications or use.
9. The Supplier/Contractor should verify and supply during the FAT the documentation confirming that all the accepted security updates and patches are installed and tested.
10. In case of application of the “smart” devices the Supplier/Contractor should verify and supply the documentation confirming that all unused software and services have been removed or switched off.
11. In case of application of the “smart” devices the Supplier/Contractor should check and supply during the SAT the documentation confirming that all the default accounts, user names, passwords, security settings, security codes and other methods of access have been changed, switched off or removed.

12. The Supplier/Contractor should verify during the SAT using scans of cyber security and supply the documentation confirming that addition of the security function does not exert a negative impact on relevant communication, delay, bandwidth, response time and bandwidth.
13. The Supplier/Contractor should create the base line of the updated communication and system configuration, including i.a. Cyber security functions, software, protocols, ports and services and will render available the documentation describing all changes.
14. The Supplier/Contractor should verify permissions and security settings in the base system before supplying updates in order to keep the determined level of the system security.
15. The Supplier/Contractor should document all completing and changes in the control system in the period of guarantee/maintenance.

## 7. List of figures

Figure 1 Protection layers of cyber security in OT systems

14