CONTROL & INSTRUMENTATION

Cyber Security Procurement Language for Control Systems

Documentation number: SUT C-2

Status as of July 2019

PCC Rokita SA
ul. Sienkiewicza 4
56-120 Brzeg Dolny
kontakt@pcc.rokita.pl
www.pcc.rokita.pl

Brzeg Dolny 2019

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

Table of Contents

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

LIST OF ABBREVIATIONS

ACL list - Access control list. Network packet filtering mechanism, used during router configuration

AKP - Control and measuring instruments
AKPiA - Control and measuring instruments, and automation for the industry
AMS - Alarm Management System

APL - Advanced Process Library

BIOS - Basic Input/Output System or Basic Integrated Operating System
BMS - Building Management System

CPU - Central Processing Unit
DG - General Director
DCS - Distributed Control System

DMZ - Demilitarized zone

DNS (Domain Name System) - System which translates domain names into IP address.

EMC - Electromagnetic Compatibility

ERP - Enterprise Resource Planning
ESD - Emergency Shutdown System
EX - Explosion proof

FAT - Factory Acceptance Test

Heartbeat Signals - It is a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a computer system.

HART - Highway Addressable Remote Transducer. Communication protocol for industrial networks.

HIDS - Host Intrusion Detection System
HMI - Human-Machine Interface

IED - Intelligent Electronic Devices

IK - Critical infrastructure
MPI - Multi-Point Interface
MR - Matrix of risk

MRP - Material Requirements Planning

NIPS - Network-based Intrusion Prevention System – System for network monitoring and network accessibility, integrity and confidentiality protection

NIDS - Network Intrusion Detection System

NPOIK - National Critical Infrastructure Protection Programme

NTP - Network Time Protocol

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

OPC - OLE for process control.

OT - Operational Technology – Industrial process control
P&ID - Piping and Instrumentation Diagram
PLC - Programmable Logic Controller

RFC (Request for Comments) - The data base of information related with the Internet and computers networks

RTU - Remote Terminal Unit

SAT - Site Acceptance Test
SCADA - Supervisory Control And Data Acquisition
SIL - Safety Integrity Level

SIS - Safety Instrumented Systems

SSiN - control and supervisory system (electric power)

SDT - Standard of Technical Documentation
SUT - Standard of Technical Equipment
TCS (SSRK) - Train Control System

USB - Universal Serial Bus

VLAN (Virtual Local Area Network) - virtual local computer network isolated in another larger physical network by additional logic

VPN - Virtual Private Network

WAN - Wide Area Network

WLAN - Wireless Local Area Network
ZSZ - Integrated Management System

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

1. INTRODUCTION

A key component of protection of country critical infrastructure and key resources under the **National Programme for Critical Infrastructure Protection** (NPOIK) is IT security of OT environment control systems and it should be taken into account both in the design, modification and maintenance of industrial automation systems and production networks so to ensure an acceptable level of risk for functioning organization in this area.

As functional control systems work in order to ensure of continuity and safety work of critical infrastructure of the country, it is necessary to recognize and understand the important roles of the systems. Furthermore, interest of identifying potential vulnerabilities, consequences and challenges related to protection of the systems against cyberattacks, should increase. Due to the closed nature of the control systems using outdated IT technology, the production areas are particularly vulnerable to cyberattacks, especially when combined with ERP systems or other management information systems. The related losses (downtime, leaks of confidential information and, as a result, a decrease in the company's image, loss of trust in the brand, loss of competitiveness) have a financial dimension.

Factors contributing to the escalation of risk in OT systems
1. Control systems adopt standardized technologies with known vulnerabilities.
2. Control systems are connected to other networks, which are not safe.
3. Insecure connections exacerbate security gaps.
4. Manuals for OT systems are publicly available both for terrorists and legitimate users.

2. PURPOSE OF THE DOCUMENT

The purpose of this document is to ensure the organization of adequate operational reliability and adequate protection of OT control systems (DCS/SCADA/MES) in the field of cybersecurity. This document presents the PCC Rokita group's applicable design and/or implementation guidelines and recommendations for OT control systems, including safety requirements in the architecture and specifications of OT systems and the necessary acceptance tests (FAT/SAT) covering the verification of safety recommendations so as to ensure compliance with the company's systems security policy and good practices to ensure an acceptable level of cybersecurity for them. Using these guidelines should help to ensure security in OT control systems. The document includes information and concrete examples of text for the purchasing processes to help control systems community, both, owners and system integrators to provide sufficient security controls of control systems under contract agreements, in order to provide an acceptable level of risk.

3. DEFINITIONS

Attack – Intentional and planned operation, causing malfunction, disruption or shutdown of the industrial automation systems.

Backdoor - a security system gap, created intentionally for later use.

BIOS (Basic Input/Output System or Basic Integrated Operating System) – BIOS refers to a software code initialized by a computer during the booting process. The basic function of BIOS is to prepare hardware so as other programmes stored on various carriers (such as hard disks, floppy disks and CD) could upload, execute and take control over the computer. This is a loading process.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

Gateway – A part of networking hardware, which participates in communication between two separate computer networks.

Sensor - is a device, physical system that transforms its reaction to a physical stimulus into a measurable signal of other physical quantity in order to deliver information about the physical quantity.

Canary(-ies) – in computing, canaries are fake devices or unused Ethernet ports, used in conjunction with a detection software to warn against unauthorized network probing or surveillance. The name is an allusion to the use of canaries as warning signals in coalmines.

CPU (**Central Processing Unit)** - a digital, sequential device that executes commands based on interpreted data taken from memory.

DCS (Distributed Control System) – a control and visualization system of an industrial process, which includes a common database of control and visualization as opposed to SCADA or PLC systems.

Deny All – The most important rule of local network protection of firewall, is following: „All actions, which are not expressly allowed, are prohibited". Thanks to the strategy, only those accesses exist, which have been opened explicitly by administrators themselves.

DMZ (Demilitarized zone) – special configuration of LAN aimed at improving safety by segregating computers on each side of a firewall. It is a logically delimited part of network (limited trust) intermediate between different level of criticality of networks as for example: a delimited part of network between network of office users (untrusted zone) and production process and automation systems network (trusted zone, protected by firewall)

DoS (Denial of Service) – Disruption or deny of an authorized access to a system or system resources as well as delay or disruption of a system operation.

Emergency Shutdown System (ESD) – An interlock system to ensure safe shutdown of the production process in case of failure or emergency.

ERP (Enterprise Resource Planning) – it is a software dedicated for companies (application system), the aim of which is to integrate all processes within an organization.

FAT (Factory Acceptance Test) – the activities aimed at confirmation that a system is working correctly. FAT is carried out at a manufacturer's site before delivery to its destination site.

FUZZING – A method to test of software or find gaps that might be used for hacker attacks

Heartbeat Signals – Known as a watchdog clock. The signals inform about communication condition/status of a system.

HART (**Highway Addressable Remote Transducer) –** it is the communication protocol for industrial networks allowing change of range and diagnostics of instrumentation. One of the standard communications protocols of instrumentation in the field of industry.

HAZOP – Hazard and Operability Study

HIDS (Host-based Intrusion Detection System). A software to detected possible malicious activity on a host, such as file changes (checking file system integrity), profiles of connections of operating systems, etc.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

HMI (Human-Machine Interface). An operator panel, an electrical device allowing to control other devices, executing some processes, e.g. technological or production processes.

IED (Intelligent Electronic Devices) – it is a definition used in the electricity industry to describe microprocessor controllers of electrical power system equipment, such as switches, transformers, capacitors banks.

IK – Critical infrastructure – resources (physical and cybernetic systems) critical (necessary) for functioning of society and economy.

Security incident OT (Incident) - **an** event or series of undesirable or unexpected events, that directly threaten the security of information (threaten its confidentiality, availability or integrity) or pose significant probability of disruption of technological processes or business activities.

Client – a device or application that communicates with a server.

Access control – system protection against unauthorized logical or physical access including a process allowed to regulate and monitor access to resources of a system in accordance with an adopted policy of security.

Cryptography – A set of measures and methods aimed at protecting transmitted information against unauthorized access, e.g. by encryption.

LAN (Local Area Network) – a local computer network connecting network resources within a limited area.

Log – A register of events with information about events and actions related to the operation of an application or IT system

Malware – Malicious Software – a malicious software dangerous for the operating system and data stored in a computer

MES (Manufacturing Execution System) – dedicated to collect information about a production process directly from production areas and transfer them to a business area, as well as some supporting systems, e.g. central servers of AV signatures distributions, transfer servers, file exchange servers, servers of directory services, etc.

Micro switch – electric switch operated with a small movement of its lever.

Reference model - A structure that allows a consistent description of elements and interfaces of a system.

MPI (**Multi-Point Interface)** – the industrial network for communication between PLC controllers, programmer station, operator panels and other SIMATIC series devices manufactured by SIEMENS.

MRP (Material Requirements Planning) – The set of processes, that allows planning materials demand based on data of product structure, information about stocks, status of purchase and plan of production.

NIDS (Network Intrusion Detection System) – used to identification of unauthorized or incorrect network traffic.

NTP (Network Time Protocol) – that allow precise synchronization of time between ICT devices.

OPC – OLE for process control – open communication standard used in automation for the industry and IT systems of higher layers (business), used to connect application based on operating systems with a hardware and a software of the automation equipment.

OT (Operational Technology) – A category of *hardware and software* monitoring and controlling physical devices -

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.

PLC (**Programmable Logic Controller) –** A microprocessor device that cyclically executes a control algorithm, on the basis of which input states are transformed into appropriate output states.

Vulnerability – it is a gap of implementation, operation or management of a system that allows disrupting its work or violating an approved policy of security

Security policy – A set of rules, procedures, guidelines, standards defining how an organization protects its resources.

PROFIBUS DP – communication protocol for industrial networks created for a real-time deterministic distributed industrial network PROFIBUS. One of the standard communications protocols for automation devices in industry.

PROFInet – modern Industrial Ethernet-based standard for building integrated and concise automation systems and distributed automation systems based on a component model.

Transducer - A device that converts one quantity into another according to defined rules and with some accuracy.

Smart transducers - transducers for measurement and signal processing, ensuring communication with an external measuring or control system via digital signal, based on the standard communication protocol.

Communication protocol – set of rules and steps performed by communication devices for data transmission and exchange.

RTU (Remote Terminal Unit) – a universal device for remote monitoring and control of devices and automation systems, usually implemented in industry.

SAT (**Site Acceptance Test)** – an activity aimed to confirm that a system delivered to a customer is complete and no damage occurred during shipment and implementation.

SCADA (Supervisory Control And Data Acquisition) – it is a control system supervising production or technology processes. SCADA carry out the following functions: collection of processes data (including measurements), visualization of the collected data, process control based on the collected data and appropriate control algorithms, alarming and measurement data archiving.

SDT – Technical Documentation Standard - the internal PCC Rokita SA standards concerning technical documentation and system of process identification.

SIL (Safety Integrity Level) – level of necessary requirements, which have to be fulfilled for the safety system to be operational.

SIS (Safety Instrumented System) – an automatic system used to maintain process safety or to take a process to a safe state when predetermined conditions are violated.

Control – an action for an object in order to achieve a specific objective, related with some information in the form of a signal.

Automatic control – a control implemented by means of a dedicated device (a controller, a regulator, etc.)

Manual control – it is a control directly implemented by a worker.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

Controller – a device controlling an operation of an electrical device. It can be a computer, electrical, electronic or electromechanical device.

System – a set of interconnected hardware and software elements implementing at least one function.

Security system – a system the aim of which is supervising and monitoring an operation of both the whole OT systems, their application tools, services as well as telecommunication and tele transmission elements used by the OT systems.

Signal - a model of any measurable time variable generated by physical phenomena or systems.

Analog signal - an analogue signal is any continuous signal for which the time-varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal.

Digital signal – an electric or an optic signal, which transfer digital data by appropriate coding (i.e. digital modulation)

Measurement signal – a signal of set parameters, known to the metrologist, used to activate the measured system or instrument under test.

VLAN (Virtual Local Area Network) – is a virtual computer network, logically separated from another, larger physical network.

VPN (Virtual Private Network) – a tunnelling protocol ensuring greater efficiency or security of data transfer in an network traffic on a private network among end customers via the public Internet, in such a way that the nodes of the network are transparent for the transmitted packets of data.

End devices – the components of control system that collect information or control a process. It can be sensors, controllers, valves, processors, etc. The end devices are supplied with a regular computer software (e.g. Web, FTP, TELNET) in order to ease maintenance and configuration.

End devices, remote terminals assemblies and PLC controllers that contain microprocessors are considered as „smart" end devices. The sensors, actuators and traditional gauges have limited processing possibilities and are known as „dumb" end devices. A serial or Ethernet communication between „smart" or „dumb" end devices and control system can be captured and modified affecting a controlled process negatively.

Actuators – mechanical devices used in regulation and control systems producing an input signal to a regulation/control object based on a control signal.

Authentication – Security measures the aim of which is to confirm reliability of a connection and messages or to confirm an access of a given user to restricted resources.

Watchdog – is an electronic timer that is used to detect and recover computer malfunctions.

WLAN (Wireless Local Area Network) using microwaves/infrared waves as a transfer signal. WLAN is based on IEEE 802.11

Firewall – a dedicated device or software preventing unauthorised access on an ICT network level by filtering traffic and rejecting unauthorised connections.

Resource – physical or logical object owned by or entrusted to an organization, which have an actual or contractual value.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

Event – A malfunction or a potential cause of an incident which could cause damage to OT system.

4. BASE MATERIALS

1. Department of Homeland Security: Cyber Security Procurement Language for Control Systems - September 2009r.
2. The guideline of the Polish Government Centre for Security dated 2017: "Standards and Good Practices of Critical Infrastructure Protection – Industry Automation in the Fuel and Gas Sector. (The original title of the guideline is „Standardy i dobre praktyki ochrony infrastruktury krytycznej – Automatyka przemysłowa w sektorze ropy i gazu – Poradnik RCB z 2017r.")
3. The guideline of the Polish Government Centre for Security dated 2017: "Standards and Good Practices of Critical Infrastructure Protection – Industry Automation in the Electricity Sector. (The original title of the guideline is „Standardy i dobre praktyki ochrony infrastruktury krytycznej – Automatyka przemysłowa w sektorze elektroenergetycznym – Poradnik RCB z 2017r.")
4. Operational Guidelines for industrial Security- The guideline of Siemens AG company, dated 2013.

Related documents:

1. The Risk Matrix
2. Procedure ZSZ **PW.02.PR01 Purchase of technical products and services**
3. Procedure ZSZ **PW.C.09.PR.03 Supervision of the equipment for monitoring and measurements**
4. **Guideline ZSZ PBT.I02 Passwords policy for control systems.**
5. Technical Equipment Standard SUT E-1 Guidelines for a technical equipment in the field of electrical.
6. Technical Equipment Standard SUT M-1 Guideline for a technical equipment in the field of mechanical.

5. GENERAL REQUIREMENTS

5.1 Scope

The present document includes the general requirements for the design and selection of automation devices and control and visualization systems as well as acceptance conditions of automation equipment and control systems in the field of cybersecurity OT. Before starting to prepare technical design or select a device, all technical requirements, standards and guidelines specified in this document should be agreed.

Note: Any deviations from the technical guidelines contained herein should be agreed and accepted in writing by the Investor.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

5.2 Exclusions

The following systems are excluded from the C&I detail engineering:

1. Control and visualization systems for building automation (Building management system, BMS)
2. Control and visualization systems for railway traffic (SSRK)
3. Control and visualization systems for electricity industry (Control and supervision system - SSiN).
4. Dispatcher systems.

5.3 Standards and regulations applicable in PCC Rokita

5.3.1 The legal requirements

1. PBT.I02 Passwords policy for control systems.
2. Regulation no. 64/2011 General Director of PCC Rokita S.A. dated December 16, 2011 on the system of technical protection of property.

5.3.2 Technical regulations and specifications.

5.4 General design requirements and acceptance conditions applicable in PCC Rokita

5.4.1 Acceptance conditions of automation equipment and control systems.

1. Disable or uninstall in a network device all services or software, which are not required for a regular system operation. This action allows to avoid security gaps.
2. Scanning of ports is a regular method to ensure necessary services and eliminate unnecessary ones. Scanning should be done before FAT with representative, fully functional system configuration and once again after SAT. All input /output ports must be scanned in terms of UDP and TCP. Ports scanning should be done occasionally in production systems, because in a majority of cases scanners disturb their work.
3. The hosts should be configured with least privilege file and account access, as well as the documentation of this configuration should be delivered.
4. The necessary system services to execute at the least user privilege level possible for that service should be configured. The documentation of this configuration should be delivered.
5. It is necessary to disable, by a software or physical disconnection, all unnecessary communication ports and removable media drives, or provide engineered barriers, as well as provide documentation of the results.
6. A password of the BIOS protection against unauthorized changes should be provided, unless it is technically impossible, in that case a Vendor shall document this case and provide mitigation measures.
7. A list of all disabled or removed USB ports, CD/DVD drives and other removable media devices should be provided.
8. It is necessary to configure the network devices in order to limit access to/from specific locations, where appropriate, as well as provide documentation of the configuration.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

6. Solutions ensuring a required cybersecurity level in different layers of protection.

Figure 1. Layers of cybersecurity protection in OT systems.

6.1 Safety of installation

1. It is necessary to comply with the internal provisions of the PCC Rokita, in particular with the regulation no. 64/2011 General Director of PCC Rokita S.A. dated December 16, 2011 on the system of technical protection of property.

6.1.1 Physical access to cybernetic elements.

1. The Vendor/Contractor shall deliver a detailed plan of appropriate physical safety mechanisms.
2. The Vendor/Contractor shall provide lockable or blocking enclosures for control system components (e.g. servers, terminals and network equipment).
3. The Vendor/Contractor shall provide locking devices with at least two keys, depending on The Purchaser requirements.
4. The rooms, where the main components of a control system are located (e.g. servers, terminal computers, network equipment, engineering and operator stations) should be lockable.
5. The Vendor/Contractor shall verify and provide documentation to confirm that there are no unauthorized logging devices installed (e.g. key loggers, cameras, and microphones).
6. The Vendor/Contractor shall verify and provide (as a part of the FAT and the SAT procedures) documentation to confirm that physical security components (e.g. safety devices, locks) are tested.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

7. The Vendor/Contractor shall disable (as a part of the FAT and the SAT procedures) by hardware and software means all unused ports and input/output devices. (see subsection Błąd! Nie można odnaleźć źródła odwołania.).
8. The Vendor/Contractor shall verify and provide, as a part of the SAT procedures, documentation to confirm, that all protection components of rooms with control system equipment (e.g. servers, terminal computers, network equipment, engineering and operator stations) work correctly.

6.1.2 Physical access to the areas (perimeter security)

1. Perimeter security includes i.e. fences, walls, fully enclosed buildings, entrance gates or doors, vehicle barriers, lighting, landscaping, surveillance systems, alarm systems and shields. Physical security may also include entry and exit loggings as well as room or area logging by means of a key card access system.
2. Lack of identification of areas of perimeter security can facilitate physical intrusion. The ability to detect perimeter intrusion is key to prevent physical attack.
3. Only staff, which need access to a location shall be given the access permission. Protected areas with a critical equipment shall not have any equipment or functions that require access by many people, including Contractors.
4. Physical security monitoring (e.g., cameras, card access) should alarm the company control centre (company security). For cybersecurity reasons these alarms shall not be on the same network as control systems and technological process visualization.
5. The Vendor/Contractor shall provide a site security assessment, making special note of parameters or events that may impact physical intrusions. As a result of the site security assessment a documented physical protection plan shall be delivered to the Purchaser.
6. The Vendor/Contractor shall verify and provide documentation confirming that enclosures such as walls, buildings or fences adequately secure the perimeter against pedestrian, vehicles and projectile intrusion.
7. The Vendor/Contractor shall allow access within the perimeter only for those employees, contractors, or guests that have been verified by both Vendor/Contractor and Purchaser
8. The Vendor/Contractor shall provide no reproducible keys or key cards for all locks.
9. The Vendor/Contractor as a part of FAT procedure shall test and provide documentation confirming that all alarm systems pick up all incidents of intrusion with minimal false alarm events.
10. The Vendor/Contractor as a part of SAT procedure shall provide access control mechanisms to the Purchaser.
11. The Vendor/Contractor as a part of SAT procedure shall provide expected functionality of physical security to the Purchaser.
12. The Vendor/Contractor shall provide adequate onsite training for operators and guards prior to commissioning.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

13. The Vendor/Contractor, prior to start-up, as a part of SAT procedure shall verify and provide documentation on all remote alarm, surveillance and locking functionality.
14. The Vendor/Contractor shall provide maintain access control mechanisms in a safe configuration.
15. The Vendor/Contractor shall validate results of the perimeter security in accordance with the terms of a contract/order.
16. The Vendor/Contractor shall change all locks, locking codes, key cards, etc. in accordance with the terms of a contract/order.
17. The Vendor/Contractor shall coordinate access control changes with the Purchaser in order to update the physical security.

6.1.3 Physical access to manual controls

1. Physical access to manual controls should be heavily restricted to authorized staff only.
2. Unauthorized access to manual controls poses a risk of system damage or intrusion, therefore must be protected.
3. The Vendor/Contractor shall provide means to physically secure the manual control mechanism by lockable enclosure or locking functionality built into the mechanism.
4. The Vendor/Contractor, prior to start-up, shall verify and provide documentation on all remote alarm, surveillance and locking functionality.
5. The Vendor/Contractor shall provide maintain manual control mechanisms in a safe configuration within a by a period specified in a contract/order.
6. The Vendor/Contractor shall validate results of manual control mechanisms security.
7. The Vendor/Contractor shall change all locks, locking codes, key cards, etc. in accordance with the terms of a contract/order.

6.2 Network security

6.2.1 Perimeter protection

6.2.1.1 Firewalls

1. The Vendor/Contractor shall provide firewalls and sets of firewall rules between network zones or provide sets of firewall rules if a firewall is not provided by Vendor/Contractor.
2. After the award of the contract, the Vendor/Contractor shall provide detailed information about all communications, including protocols required by the firewall as well as identify each network device initiating communication in accordance with suitable sets of rules.
3. The Vendor/Contractor shall verify that the SAT procedures include validation and documentation of the requirements. Any usernames, passwords or other security codes configured by the Vendor/Contractor or a manufacturer must be changed at this time.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

4. It is necessary to keep valid firmware and patches of firmware.

6.2.1.2 Network Intrusion Detection System (NIDS)

1. The Vendor/Contractor shall provide traffic profiles with expected communication paths, network traffic and expected limit of use, for anomaly-based NIDS.
2. The Vendor/Contractor shall provide appropriate signatures for signature-based systems.
3. Post-contract award, the Vendor shall provide a configured NIDS and/or provide the information to configure a NIDS.
4. The Vendor/Contractor shall verify NIDS during the entire FAT procedure and periodically implement appropriate malicious software. The Vendor/Contractor shall examine the log files and check the expected results.
5. The Vendor/Contractor shall use NIDS during the entire SAT procedure and periodically implement appropriate malicious software. The Vendor/Contractor shall examine the log files and check the expected results
6. The Vendor/Contractor shall tune signatures and adjust thresholds to reduce false alarms and minimize false results.
7. The Vendor/Contractor shall update the NIDS configuration and/or documentation as needed after the changes are made.

6.2.1.3 Detection system (Canaries)

1. The „Honey pots", which analyse unauthorized connections and/or Canaries, which flag that a connection attempt has taken place, shall be provided by the Vendor/Contractor to provide passive network monitoring.
2. The Vendor/Contractor shall provide a configured canaries or information to configure them with alerting software to indicate unauthorized connection attempts.
3. The Vendor/Contractor shall verify that SAT procedures include written validation and documentation of the requirements. All default usernames, passwords or other security codes configured by the Vendor/Contractor or manufacturer must be changed at this time.
4. The Vendor/Contractor shall reconfigure Canaries as needed when network address topologies are changed.

6.2.2 Network Addressing and Name Recognition (Resolution)

1. To protect against DNS attacks, DNS servers for internal control system network should reside inside a firewall and should be separate from DNS servers on the company network. DNS servers for control system network should be authoritative only for address space of the control system network. It means that the DNS servers should contain complete information about the zone (name to IP address mappings) only for hosts on the control system network. The control system network is perfectly isolated and hosts will not

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

need to resolve external names. However, if the hosts have to resolve names for host outside the trusted control system network, queries should go to the control system DNS server, which forward the queries through a firewall to a DNS server on the corporate network.

2. Recommendations for secure DNS configuration:

   • Using dedicated servers for DNS and related services and disabling all unneeded services.

   • Using the latest software with current patches.

   • Periodically backing up and reviewing DNS configuration files as well as running integrity checks to verify the integrity of configuration files, zone data, and other DNS files.

   • Running DNS servers as a user other than a root. Enabling access controls to allow only specific individuals to create, delete, or modify DNS data.

   • Enabling prevention of cache pollution.

   • Restricting addresses that can send queries to the control system DNS servers in order to control system hosts.

   • Restricting zone transfers only to trusted hosts and authenticating them.
   • Using a static addressing scheme. If dynamic addressing is used, allow dynamic updates only from trusted hosts.

   • Configuring the firewall in order to allow communication between the control system and corporate DNS servers only on UDP and TCP 53 ports.

   • Allowing special considerations for hosts with multiple IP addresses for redundancy.

3. If an order is granted before the Contract is made the Vendor/Contractor shall provide recommended methodology of network addressing and names recognition.
4. The Vendor/Contractor shall provide means to verify the integrity of configuration files, zone data, and other DNS files (e.g., the integrity checking may be done by HIDS devices).
5. After the award of the contract the Vendor/Contractor shall provide configured DNS servers or information to configure a DNS server (servers) that meets a pre-negotiated standard of security.
6. The Vendor/Contractor shall treat addressing information as business sensitive and protect them.
7. The Vendor/Contractor shall install and run DNS servers continuously during the entire FAT process.
8. The Vendor/Contractor shall verify all domain servers and the hosts within the domain involved in testing are resolvable by all client and server systems connected to the network.
9. The Vendor/Contractor shall document both solution of forward (hostname to IP address) and vice versa, solution of reverse (IP address to hostname).
10. The Vendor/Contractor shall run DNS servers during the entire SAT process.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

11. The Vendor/Contractor shall verify all domain servers and the hosts within the domain involved in testing are identifiable by all client and server systems connected to the network.
12. The Vendor/Contractor shall document both solution of forward (hostname to IP address) and vice versa, solution of reverse (IP address to hostname).
13. The Vendor/Contractor shall provide continuous patch management process for DNS and related services such as DHCP.

6.2.3 Remote access.

6.2.3.1 TCP/IP

1. The Vendor/Contractor shall provide physical and cybersecurity functions, including authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect a device and configuration computer against unauthorized modification or use.
2. The Vendor/Contractor shall clearly identify the physical and cybersecurity functions and provide methodology of maintaining the functions, including methods of setting change which has been configured by vendor/contractor or default manufacturer conditions.
3. The Vendor/Contractor shall verify that addition of a security function has no negative impact on connectivity, delay, bandwidth and response time, including during a SAT procedure after connecting to the existing equipment.
4. The Vendor/Contractor shall remove or disable all software components, which are not required to operation and maintenance of a device prior to the FAT. The Vendor/Contractor shall provide documentation for all removed and/or disabled software components.
5. The Vendor/Contractor before the end a negotiation stage shall provide appropriate protocol stack updates and/or workarounds (bypasses) in order to mitigate all vulnerabilities related to a product and maintain the established level of system security.
6. The Vendor/contractor shall verify and provide documentation confirming that the security system (SIS) is certified after putting security devices in operation.
7. The Vendor/Contractor shall use implementation of TCP/IP protocol, which is fully compliant with current RFC documents of TCP/IP protocol.
8. The Vendor/Contractor shall provide a product which is IPv6 compatible.
9. The Vendor/Contractor shall provide possibility to monitor traffic in encryption system.
10. After the award of the contract the Vendor/Contractor shall provide an independent external security verification of the IPv6 implementations (e.g. by fuzzing techniques). The Vendor/Contractor shall provide documentation of the results of the external security verification.
11. The Vendor/Contractor shall mitigate all vulnerabilities discovered during the testing of the IPv6 implementations and provide documentation of the results.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

12. The Vendor/Contractor shall verify and provide physical and cybersecurity functions, including authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the system against unauthorized modifications or use.
13. The Vendor/Contractor shall verify and provide documentation stating that all validated security updates and patches are installed and tested at the start of a FAT procedure.
14. The Vendor/Contractor shall verify and provide documentation stating that all unused software and services are removed or disabled.
15. After FAT, the Vendor/Contractor shall create a baseline of the system communication and configuration including i.e. cybersecurity functions, software, protocols, ports and services and provide documentation describing each change.
16. The Vendor/Contractor shall verify by means of cybersecurity scans of the system and provide documentation stating that the addition of security functions has no negative impact on connectivity, delay, bandwidth and response time.
17. The Vendor/Contractor shall verify and provide documentation and changes of physical and cyber security functions, including i.e. authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the system computer against unauthorized modifications or use.
18. After SAT, the Vendor/Contractor shall create a baseline of the system communication and configuration including i.e. cyber security functions, software, protocols, ports and services and provide documentation describing each change.
19. The Vendor/Contractor shall verify and provide documentation stating that all default accounts configured by manufacturer, usernames, passwords, security settings, security codes and other methods of access are changed, disable or removed.
20. The Vendor/Contractor shall ensure maintenance of delivered system security functions.
21. The Vendor/Contractor shall provide documentation of all additions and changes to a remote access device within a warranty period.
22. The Vendor/Contractor shall verify permissions and security settings in baseline system before a delivery of updates or replacements in order to maintain the established level of system security.

6.2.3.2 VPN

1. The placement and ownership of VPN should be agreed for each VPN, which is implemented. A good practice is to place a VPN server in DMZ, separate from a control network and allow the user to connect with a control network by means of authentication process required for a user accessing locally to a network. VPNs are strongly affected by firewall rules and should be consider in a case of firewall solutions.
2. The Vendor/Contractor shall provide physical and cyber security functions including i.e. multifactor authentication (e.g. security token, known key and/or certificate), encryption, access control, event and communication logging, monitoring and alarming in order to protect a system and configuration computer against unauthorized modifications or use.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

3. The Vendor/Contractor shall clearly identify the physical and cyber security functions and provide methodology of maintaining the functions, including i.e. methods of changing settings which have been configured by vendor/contractor or default manufacturer conditions.
4. The Vendor/Contractor shall verify that addition of a security function has no negative impact on connectivity, delay, bandwidth and response time, including during at SAT procedure after being connected to the existing equipment. The Vendor/Contractor shall provide documentation of the results of the above-mentioned verification.
5. The Vendor/Contractor shall remove or disable all software components, which are not required to operation and maintenance of a device prior to FAT. The Vendor/Contractor shall provide documentation for all removed and/or disabled software components.
6. The Vendor/Contractor before the end of a negotiation stage shall provide appropriate protocol stack updates and/or workarounds (bypasses) in order to mitigate all vulnerabilities related to a product and maintain the established level of system security.
7. The Vendor/Contractor shall verify and provide documentation confirming that the security system (SIS) is certified after putting security devices in operation.
8. The Vendor/Contractor shall provide DMZ outside the control network for the VPN server to reside.
9. The Vendor/Contractor shall use different methods of authentication in order to establish access to the control network and VPN connection.
10. The Vendor/Contractor shall verify and provide documentation of physical and cyber security functions including i.e. multifactor authentication (e.g. security token, known key and/or certificate), encryption, access control, event and communication logging, monitoring and alarming in order to protect the system against unauthorized modifications or use.
11. The Vendor/Contractor shall verify and provide documentation stating that all validated security updates and patches are installed and tested at the start of the FAT procedure.
12. The Vendor/Contractor shall create a baseline of the system communication and configuration including i.e. cyber security functions, software, protocols, ports and services and provide documentation describing the functionality of each item and change.
13. The Vendor/Contractor shall verify and provide documentation stating that all unused software and services are removed or disabled.
14. The Vendor/Contractor shall verify and provide documentation stating that all default accounts configured by a manufacturer, usernames, passwords, security settings, security codes and other methods of access are changed, disable or removed.
15. The Vendor/Contractor before the end of a negotiation stage shall provide appropriate updates and patches as soon as cyber security problems are identified in order to maintain the established level of system security.
16. The Vendor/Contractor shall verify permissions and security settings in the baseline system before delivery of updates or replacements in order to maintain the established level of system security.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

17. The Vendor/Contractor shall ensure maintenance of delivered system security functions.
18. The Vendor/Contractor shall provide documentation of all additions and changes to a remote access device within the warranty period.

6.2.4 Network partitioning

6.2.4.1 Network devices.

1. The Vendor/Contractor shall provide and verify a method of managing network devices and changing addressing schemes.
2. The Vendor/Contractor shall verify and provide documentation stating that a network configuration interface is secured.
3. The Vendor/Contractor shall provide and verify ACL, port security address lists and upgraded security for ports duplication.
4. The Vendor/Contractor shall remove or disable unused network configuration and management functions on network devices.
5. The Vendor/Contractor shall provide firewall rules for inbound and outbound traffic based on set of deny all rules.
6. The Vendor/Contractor shall provide NIDS rules and log review tools that verify a firewall operation and detect atypical traffic.
7. The Vendor/Contractor shall provide NIPS architecture that will operate with a communication method.
8. The Vendor/Contractor shall provide VPN concentrators configured with filters and ports security as well as provide documentation about network devices installed with security settings.
9. The Vendor/Contractor shall scan the network ports and document traffic origination and functions for each port.
10. The Vendor/Contractor shall provide updates and patches in order to maintain the established level of system security.
11. The Vendor/Contractor shall verify permissions and security settings on the baseline system before delivery of any updates or replacements.

6.2.4.2 Network architecture

1. Simplification of a network should be the priority during designing initial architecture or rules of firewall. Variety of protocols open for data should be limited to a minimum. Data that are modified many times and retransmitted, such as database, internet and FTP, first should be moved to the DMZ, modified in DMZ and transferred from DMZ to other networks. The Contractor shall provide and verify a method of managing network devices and changing addressing schemes.
2. The Vendor/Contractor shall provide and document safe network architecture where the higher security zones communicate with the less secure zones.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

3. The Vendor/Contractor shall provide and document the design for all communication paths between networks of different security zones by means of DMZ.
4. The Vendor/Contractor shall verify and document that disconnection points are established between network partitions and provide methods to isolate subnets in order to continue limited operations.
5. The Vendor/Contractor shall provide and document adapted filtering and monitoring rules for all security zones and alarming for unexpected traffic.
6. The Vendor/Contractor shall provide and document a DMZ, which is restricted to communication, where all traffic is monitored, alarmed and filtered.
7. The Vendor/Contractor shall provide and document outbound filtering and alarms for unexpected traffic in security zones.
8. The Vendor/Contractor shall provide and document all sources and destinations with a forced initiation of communication, even during restart between security zones.
9. The Vendor/Contractor shall provide and document two DMZ architectures by means of different products performing the same functionality in parallel.
10. The Vendor/Contractor shall provide and document mechanism for patching a single DMZ architecture operating in a parallel configuration without disrupting the other DMZ also operating in parallel. .
11. The Vendor/Contractor shall assess the need and provide update and patches as soon as vulnerabilities are recognised in order to maintain the established level of system security. The Vendor/Contractor shall verify and document that the security profile of the network architecture is maintained.

6.3 System Integrity

6.3.1 System Hardening

6.3.1.1 Removal of Unnecessary Services and Software.

1. A recommended hardening activity is disabling or removing any services or software, which are not required for normal system operation, thus removing potential vulnerabilities.
2. Ports scan is the normal method to ensure required services and elimination of unneeded ones. Ports scan shall be done before FAT with a representative, fully functional system configuration. All input/output (I/O) ports have to be scanned in terms of UDP and TCP protocols. The scan should be run before FAT and again before SAT. Ports scan can be used on production systems only occasionally. In most cases, the scanners disrupt operations of production systems.
3. After the award of the contract, the Vendor/Contractor shall provide documentation describing in detail all applications, tools, system services, scripts, configuration files, database and all other required software as well as appropriate configurations, including versions and/or levels of patches for each of the computer system related with a control system.
4. The Vendor/Contractor shall provide a list of services required for any computer system with running control system applications or required for connection of control system applications. The list shall include

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

all ports and services required for normal operation, as well as any other ports and services required for emergency operation. The list shall also include an explanation or cross-reference to justify why each service is necessary for operation.

5. The Vendor/Contractor shall verify and provide documentation stating that all services are patched to the current status. Within an earlier stage of the negotiations, the Vendor/Contractor shall provide appropriate software and service updates and/or workarounds (bypasses) in order to mitigate all vulnerabilities related to the product and maintain the established level of system security. The Vendor/Contractor shall remove and/or disable all software components, which are not required for operation and maintenance of the control system prior to FAT. The Vendor/Contractor shall provide documentation for all removed and disabled software and service components. Software to be removed and/or disabled shall include, but not limited to:
   1. Games.
   2. Not delivered device drivers for network devices.
   3. Messaging services (e.g. MSN, AOL IM).
   4. Servers or clients of unused internet services.
   5. Software compilers in all user workstations and servers except for engineering workstations and servers.
   6. Software compilers for languages which are not used in the control system.
   7. Unused network and communications protocols.
   8. Unused administrative software tools, diagnostics, network management, and system management functions.
   9. Backups of files, databases, and programs used only during the system development.
   10. All unused data and configuration files.
   11. Examples of programs and scripts.
   12. Unused software tools for processing documents (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice etc.).

6. The Vendor/Contractor shall verify that the Purchaser requires results of cyber security scans (as a minimum a vulnerability and active port scan with the most current signature files) run on a control system as a primary activity of FAT. Next the assessment is compared with a list of required services, patching status and documentation to confirm this requirement. Other predicted measures include:
   1. The Vendor/Contractor shall provide for each network device or class of device (e.g. server, workstation and switch) the following documentation of configuration:
   - Network services required for operation of that device. Indicate the service name, protocol (e.g. TCP and UDP) and ports range.
   - Dependencies on basic services of the operating system
   - Dependencies in network services residing on other network devices
   - All the software configuration parameters required for correct system operation
   - Certified operating system, driver, and other software versions installed on the device
   - Results found by the vulnerability scans with mitigations affected

   2. The Vendor/Contractor shall install firmware updates available for the computer or network device certified by the system manufacturer at the time of installation as well as provide documentation.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

3. The Vendor/Contractor shall provide a summary table indicating each communication path required by the system including the following information:
a. Source device name and media access control (MAC) and/or IP address
b. Destination device name and MAC and/or IP address
c. Protocol (e.g. TCP and UDP) and port or range of ports.
4. The Vendor/Contractor shall perform network-based validation and documentation steps on each device:
Full TCP and UDP port scan on Ports 1–65535. This scanning needs to be done during a simulated "normal system operation."

7. The Vendor/Contractor shall compare the results of cyber security scans run on the system as a primary activity of the SAT with a list of the required services, patching status, and required documentation. At the conclusion of SAT and before a change or a start-up, the above cyber security scans (with the most current signature files) must be run again.

6.3.1.2 Host Intrusion Detection System (HIDS)

1. The Vendor/Contractor shall provide configured HIDS devices and/or provide the information to configure HIDS devices, including static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions sufficient for configuring the HIDS.
2. The Vendor/Contractor shall configure HIDS devices in such a manner that all system and user account connections are logged. This log shall be configured in such a way that an alarm can be displayed to the operator or security personnel if an abnormal situation occurs.
3. The Vendor/Contractor shall present a recommend HIDS configuration in a manner that does not negatively impact the operating system functions or business objectives.
4. The Vendor/Contractor shall present recommend log review and notification software tools.
5. The Vendor/Contractor shall configure devices as "append only" to prevent change of records on local storage devices.
6. The Vendor/Contractor shall manage HIDS during the entire FAT process and periodically interject applicable malware. The Vendor/Contractor shall verify log files and check the expected results. FAT procedures shall include validation and documentation of this requirement.
7. The Vendor/Contractor shall manage HIDS during the entire SAT process and periodically interject applicable malware. The Vendor/Contractor shall verify log files and check the expected results. SAT procedures shall include validation and documentation of this requirement.
8. The Vendor/Contractor shall generate a system image at the end of the SAT, which will be used later as a control baseline.

6.3.1.3 Changes in File System and Operating System Permissions.

1. The Vendor/Contractor shall configure hosts with least privilege file and account access and provide documentation of the configuration.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

2. The Vendor/Contractor shall configure the necessary system services to execute at the least user privilege level possible for that service and provide documentation of the configuration.
3. The Vendor/Contractor shall document that changing or disabling access to such files and functions has been completed.
4. The Vendor/Contractor shall provide, as a part of the FAT procedures, validation and documentation of the permissions assigned.
5. The Vendor/Contractor shall provide, as a part of the SAT procedures, validation and documentation of the permissions assigned.

6.3.1.4 Hardware Configuration

1. The Vendor/Customer shall disable, by software or physical disconnection, all unneeded communication ports and removable media drives or provide designed barriers as well as provide documentation of the results.
2. The Vendor/Contractor shall protect BIOS against unauthorized changes unless it is not technically feasible, in that case the Vendor shall document this case and provide mitigation measures
3. The Vendor/Contractor shall provide a written list of all disabled or removed USB ports, CD/DVD drives, and other removable multimedia devices.
4. The Vendor/Contractor shall configure the network devices in order to limit access to/from specific locations, where appropriate as well as provide documentation of the configuration.
5. The Vendor/Contractor shall configure the system to make it possible for the system administrator to restart devices when the devices are disabled by software and provide documentation of the configuration.
6. The Vendor/Contractor shall provide, as a part of the FAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.
7. The Vendor/Contractor shall provide, as a part of the SAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.

6.3.1.5 Heartbeat Signals

1. The Vendor/Contractor shall identify „Heartbeat" signals or protocols and recommend including the monitor in the network.
2. After the award of the contract, the Vendor/Contractor shall provide packet definitions of the "Heartbeat" signals and examples of the "Heartbeat" traffic if the signals are included in the network monitoring.
3. As a part of FAT procedures, the Vendor/Contractor shall provide documentation of the requirements.

   The Vendor/Contractor shall create a baseline of the "Heartbeat" communications traffic to take into account frequency, packet sizes and expected packet configurations.
4. The Vendor/Contractor shall provide, as a part of the SAT procedures, documentation of the requirements.
5. The Vendor/Contractor shall create a baseline of the "Heartbeat" communications traffic and check the results with respect to FAT documentation.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

6.3.1.6 Installing Operating Systems, Applications and Software Updates of Other Companies.

1. The Vendor/Contractor shall provide a patch management and update process.

   Prior to award of a contract, the Vendor shall provide detailed information about patch management and update process. Responsibility for patch installation and update shall be identified.

2. The Vendor/Contractor shall notify of known vulnerabilities having impact on delivered or required by the Vendor/Contractor components such as OS, applications and third-party software in pre-negotiated period, after a public disclosure.

3. The Vendor/Contractor shall provide notifications about patches having impact on security in pre-negotiated period identified in the patch management process. The Vendor/Contractor, before distribution shall apply, test and approve the appropriate updates and/or workarounds on a baseline reference system. Mitigation of these vulnerabilities shall occur within initial negotiation.

6.3.2 Session Management

1. The Vendor/Contractor shall not permit a transmission of user authentication data in the form of normal text.
2. The Vendor/Contractor shall provide the strongest encryption method commensurate with the technology platform and limitation of the reaction time.
3. The Vendor/Contractor shall not allow:

   - multiple simultaneous logging to keep login information between sessions

   - providing any auto-fill functionality during login

   - anonymous logging.

4. The Vendor/Contractor shall provide method of logout and timeout settings on a user account.
5. The Vendor/Contractor shall verify that SAT procedures include validation and documentation of the requirements.

6.3.3 Management and Password/Authentication Policy

1. Comply with the Instruction **Guideline ZSZ PBT.I02**
2. The Vendor/Contractor shall provide a configurable account password management system that allows selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated use of the same password.
3. The Vendor/Contractor shall not store passwords in an electronic form or in documentation supplied by a Vendor in a readable form unless the data media is physically protected.
4. The Vendor/Contractor shall control access to the configuration interface of the account management system.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

5. The Vendor/Contractor shall verify that SAT procedures include validation and documentation of the password and authentication and management rules.

6.3.4 Coding Practices

1. The Vendor/Contractor shall provide documentation of code reviews and other software development process steps used to assess software security. Software subject to these reviews shall include both applications created by Vendors/Contractors and any other source code over which the Vendor/Contractor has necessary control constituting of a part of the control system. A software of other manufacturers integrated into Vendors/Contractors products shall be assessed for security vulnerabilities. Experience shows that system integration often contributes to the overall vulnerability of the system.
2. The Vendor/Contractor shall create code in accordance with the following rules:

a. Check inputs for reasonable values.

b. Encrypt data files.

c. Take into consideration impact of operating systems and other third party's libraries on the security.

d. Make sure that operating systems and other third party's library have an update policy in place.

e. It is not allowed to overflow the buffer.

f. Verify that log files are unalterable

g. Apply comprehensive authentication and integrity checking on data communication process between processes

h. Apply design and review of code.

i. Check if there are no passwords or encryption keys entered into the code.

j. A code shall be created in such a manner that interlocks and control signals would not come from devices from an internal network of control system.

3. The Vendor/Contractor shall provide source codes of created software application.
4. The Vendor/Contractor shall provide documentation of development practices and standards applied to control system software written by a manufacturer, including firmware, used to ensure a high level of security against unauthorized access.
5. The Vendor/Contractor shall carry out the FAT procedures include validation and documentation of the software development process and/or code review.
6. The Vendor/Contractor shall carry out the SAT procedures include validation and documentation of the software development process and/or code review.
7. The Vendor/Contractor shall verify that software updates and patches are validated according to the same software development process or review plan.

6.3.5 Defects Correction

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

1. Defects correction refers to the actions which should be performed when defects are discovered in control system software, equipment and system architectures created by or under the control of the Vendor/Contractor. Guidance on corrective actions, fixes, or monitoring is needed to mitigate all security vulnerabilities. Vulnerabilities and defects are normally closely held until remediation becomes available. However, some vulnerabilities are made public before a fix has been developed and then it is necessary to mitigate these vulnerabilities.
2. Defects history and remedy steps/patches are needed to withdraw some patches.
3. The Vendor/Contractor shall provide documentation of a defect correction process.
4. The Vendor/Contractor shall provide appropriate software updates and/or methods to mitigate all vulnerabilities within a period established in a contract/order.
5. The Vendor/Contractor shall provide FAT documentation of the defect validation and remedial measures.
6. The Vendor/Contractor shall provide SAT documentation of the defect validation and remedial measures.
7. The Vendor/Contractor shall maintain for auditing purposes a main list of all defects and remedial measures for a period established in a contract/order.

6.3.6 Malware Detection and Protection

1. The Vendor/Contractor shall disclose the existence and reasons of any known or identified backdoor codes.
2. The Vendor/Contractor shall meet one of two conditions:

a. Provide a malware detection system based on a host for the control system network. The Vendor/Contractor shall check the system operation correctness in order to detect host malware, to keep suspicious files in quarantine (instead of automatic removal) and to deliver a signature update scheme. The Vendor/Contractors shall also test major updates to malware detection applications and provide performance measurement data on the impact of the malware detection use in an active system. Measurements shall include i.e. network usage, CPU usage, memory usage, and any other impact on normal communications processing.

b. If the Vendor/Contractor does not provide the actual host malware detection scheme, the Vendor/Contractor shall recommend malware detection products to be used and provide guidance on configuration of malware detection that will operate with the vendor's/contractor's products.

3. Under FAT and SAT, the Vendor/Contractor shall record system performance measurements that include the system with and without malware detection.
4. Under FAT and SAT the Vendor/Contractor shall document any known or identified backdoors.
5. The Vendor/Contractor shall retain malware detection application logs for period established in a contract/order for possible investigative and judicial purposes.
6. The Vendor/Contractor shall update malware detection software as required to be effective for the most recent malware released. As the malware variants change, new, more precise or tuned signatures need to be applied.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

7. The Vendor/Contractor shall disclose the existence and reasons for any known or identified backdoor codes.

6.4 End Devices.

6.4.1 Intelligent Electronic Devices (IED)

1. The Vendor/Contractor shall provide physical and cyber security functions including i.e. authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer against unauthorized modification or use.

2. The Vendor/Contractor shall clearly identify the physical security features and cyber security functions and provide the methodology of maintaining the functions including methods of changing settings from the manufacturer's or Vendor/Contractor's default settings.

3. The Vendor/Contractor shall verify that the addition of security function does not have a negative impact on connectivity, delay, bandwidth, response time, including during SAT when connected to existing equipment.

4. The Vendor/Contractor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to FAT. The Vendor/Contractor shall provide documentation about what is removed and/or disabled.

5. The Vendor/Contractor shall provide appropriate software and service updates to mitigate all vulnerabilities associated with the device delivered and shall maintain the established level of system security within a period established in the contract/order.

6. The Vendor/Contractor shall verify and provide documentation confirming that the safety instrumented system (SIS/ESD) will be certified after incorporating the security devices.

7. The Vendor/Contractor during FAT and SAT shall verify and document physical and cyber security including i.e. authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the device and the configuration computer against unauthorized modifications or use.

8. The Vendor/Contractor during FAT shall verify and provide documentation to confirm that all approved updates and security patches are installed and tested.

9. The Vendor/Contractor shall verify and provide documentation to confirm that all unused software and services are removed or disabled.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

10. The Vendor/Contractor during SAT shall verify and provide documentation to confirm that all default accounts, usernames, passwords, security settings, security codes and other methods of access are changed, disabled or removed.

11. During SAT, the Vendor/Contractor shall verify by means of cybersecurity scans and provide documentation confirming that an addition of security functions has no negative impact on connectivity, delay, bandwidth and response time.

12. The Vendor/Contractor shall provide updates and patches for devices as soon as cyber security problems are identified in order to maintain the established level of system security within the period established in the contract/order.

13. The Vendor/Contractor shall create a baseline of the updated system communication and configuration including i.e. cybersecurity functions, software, protocols, ports and services and provide documentation describing all changes.

14. The Vendor/Contractor shall verify permissions and security settings on the baseline system before delivery of any updates in order to maintain the established level of system security.

15. The Vendor/Contractor shall document all additions and changes on the control system during the warranty/maintenance period.

6.4.2 Remote Terminal Units (RTU)

1. The Vendor/Contractor shall provide physical and cyber security functions including i.e. authentication, encryption, access control, event and communication logging, monitoring, and alarming in order to protect the device and configuration computer against unauthorized modifications or use.
2. The Vendor/Contractor shall clearly identify the physical security features and cyber security functions and provide methodology of maintaining the functions, including methods of changing default settings configured by the Vendor/Contractor or a manufacturer.
3. The Vendor/Contractor shall verify that an addition of a security function has no negative impact on connectivity, delay, bandwidth and response time, including during the SAT procedure after connected to existing equipment.
4. The Vendor/Contractor shall remove or disable all software components, which are not required to operation and maintenance of a device prior to FAT. The Vendor/Contractor shall provide documentation for all removed and/or disabled software components.
5. The Vendor/Contractor shall provide appropriate software and service updates to mitigate all vulnerabilities associated with the device delivered and shall maintain the established level of system security within a period established in the contract/order.
6. The Vendor/Contractor shall verify and provide documentation to confirm that the safety instrumented system (SIS/ESD) will be certified after incorporating the security devices.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

7. The Vendor/Contractor during FAT and SAT shall verify and document physical and cyber security including i.e. authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the device and the configuration computer against unauthorized modifications or use.

8. The Vendor/Contractor during FAT shall verify and provide documentation to confirm that all approved updates and security patches are installed and tested.

9. The Vendor/Contractor shall verify and provide documentation to confirm that all unused software and services are removed or disabled.

10. The Vendor/Contractor during SAT shall verify and provide documentation to confirm that all default accounts, usernames, passwords, security settings, security codes and other methods of access are changed, disabled or removed.

11. During SAT, the Vendor/Contractor shall verify by means of cybersecurity scans and provide documentation confirming that an addition of security functions has no negative impact on connectivity, delay, bandwidth and response time.

12. The Vendor/Contractor shall provide updates and patches for devices as soon as identification cyber security problems in order to maintain the established level of system security within the period established in the contract/order.

13. The Vendor/Contractor shall create a baseline of the updated system communication and configuration including i.e. cybersecurity functions, software, protocols, ports and services and provide documentation describing all changes.

14. The Vendor/Contractor shall verify permissions and security settings on the baseline system before a delivery of any updates in order to maintain the established level of system security.

15. The Vendor/Contractor shall document all additions and changes on the control system during the warranty/maintenance period.

6.4.3 Programmable Logic Controllers (PLC)

1. The Vendor/Contractor shall provide physical and cyber security functions including i.e. authentication, encryption, access control, event and communication logging, monitoring, and alarming in order to protect the device and the configuration computer against unauthorized modifications or use.

2. The Vendor/Contractor shall clearly identify the physical security features and cyber security functions and provide methodology of maintaining the functions, including methods of changing default settings configured by the Vendor/Contractor or a manufacturer.

3. The Vendor/Contractor shall verify that addition of a security function has no negative impact on connectivity, delay, bandwidth and response time, including during the SAT procedure after being connected to existing equipment.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

4. The Vendor/Contractor shall remove or disable all software components, which are not required to operation and maintenance of a device prior FAT. The Vendor/Contractor shall provide documentation for all removed and/or disabled software components.
5. The Vendor/Contractor shall provide appropriate software and service updates to mitigate all vulnerabilities associated with the device delivered and shall maintain the established level of system security within a period established in a contract/order.
6. The Vendor/Contractor shall verify and provide documentation to confirm that the safety instrumented system (SIS/ESD) is certified after incorporating the security devices.
7. The Vendor/Contractor during FAT and SAT shall verify and document physical and cyber security including i.e. authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the device and the configuration computer against unauthorized modification or use.
8. The Vendor/Contractor during FAT shall verify and provide documentation to confirm that all approved updates and security patches are installed and tested.
9. The Vendor/Contractor shall verify and provide documentation to confirm that all unused software and services are removed or disabled.
10. The Vendor/Contractor during SAT shall verify and provide documentation to confirm that all default accounts, usernames, passwords, security settings, security codes and other methods of access are changed, disabled or removed.
11. The Vendor/Contractor during SAT shall verify by means of cybersecurity scans and provide documentation to confirm that an addition of security functions has no negative impact on connectivity, delay, bandwidth and response time.
12. The Vendor/Contractor shall provide updates and patches for devices as soon as identification cyber security problems in order to maintain the established level of system security within the period established in the contract/order.
13. The Vendor/Contractor shall create a baseline of the updated system communication and configuration including i.e. cybersecurity functions, software, protocols, ports and services and provide documentation describing all changes.
14. The Vendor/Contractor shall verify permissions and security settings on the baseline system before delivery of any updates in order to maintain the established level of system security.
15. The Vendor/Contractor shall document all additions and changes on the control system during the warranty/maintenance period.

6.4.4 Sensors, Actuators and Meters.

1. The Vendor/Contractor shall provide physical and cyber security functions including i.e. authentication, encryption, access control, event and communication logging, monitoring, and alarming in order to protect the device and the configuration computer against unauthorized modifications or use.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

2. The Vendor/Contractor shall clearly identify the physical security features and cyber security functions and provide methodology of maintaining the functions, including methods of changing default settings configured by the Vendor/Contractor or a manufacturer.
3. The Vendor/Contractor shall provide secure communication interfaces (serial, Ethernet and wireless) including filtering and monitoring of communication but shall not use wireless communication.
4. The Vendor/Contractor shall verify that an addition of a security function has no negative impact on connectivity, delay, bandwidth and response time, including during the SAT procedure after being connected to the existing equipment.
5. For smart devices, the Vendor/Contractor shall remove or disable all software components, which are not required to operation and maintenance of a device prior FAT. The Vendor/Contractor shall provide documentation for all removed and/or disabled software components.
6. For smart devices, The Vendor/Contractor shall provide appropriate software and service updates to mitigate all vulnerabilities associated with the device delivered and shall maintain the established level of system security within a period established in the contract/order.
7. For smart devices, The Vendor/Contractor shall verify and provide documentation to confirm that the safety instrumented system (SIS/ESD) is certified after incorporating the security devices.
8. The Vendor/Contractor during FAT and SAT shall verify and document physical and cyber security including i.e. authentication, encryption, access control, event and communication logging, monitoring and alarming in order to protect the device and the configuration computer against unauthorized modifications or use.
9. The Vendor/Contractor during FAT shall verify and provide documentation to confirm that all approved updates and security patches are installed and tested.
10. For smart devices, the Vendor/Contractor shall verify and provide documentation to confirm that all unused software and services are removed or disabled.
11. For smart devices, the Vendor/Contractor during SAT shall verify and provide documentation to confirm that all default accounts, usernames, passwords, security settings, security codes and other methods of access are changed, disabled or removed.
12. The Vendor/Contractor during SAT shall verify by means of cybersecurity scans and provide documentation to confirm that an addition of security functions has no negative impact on connectivity, delay, bandwidth and response time.
13. The Vendor/Contractor shall create a baseline of the updated system communication and configuration including i.e. cybersecurity functions, software, protocols, ports and services and provide documentation describing all changes.
14. The Vendor/Contractor shall verify permissions and security settings on the baseline system before delivery of any updates in order to maintain the established level of system security.
15. The Vendor/Contractor shall document all additions and changes on the control system during the warranty/maintenance period.

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA

7. List of Figures

This document is the property of PCC Rokita SA in Brzeg Dolny and shall not be copied or transferred to any third party without a written consent of respective authorities of PCC Rokita SA