TECHNICAL REQUIREMENTS

AUTOMATION AND INSTRUMENTATION

Document No. **OL-TR-IR-000**

TECHNOLOGICAL PROCESS AUTOMATIC CONTROL SYSTEM CYBERSECURITY INSTALLATION RULES

Document No. **OL-TR-IR-021**

Rev.	Revision description	Date	Prep. by	Check. by	Appr. by
05					
04					
03					
02					
01	Updated revision	5-Apr-24	ORLEN Lietuva	ORLEN Lietuva	ORLEN Lietuva
00	Final Issue	15-Mar-19	ORLEN Lietuva	ORLEN Lietuva	ORLEN Lietuva

TABLE OF CONTENTS

1. SCOPE 3
2. REFERENCES 3
3. TERMS AND DEFINITIONS 3
4. GENERAL REQUIREMENTS 4
5. TECHNICAL REQUIREMENTS 5

1. SCOPE

This Specification covers requirements for Industrial Control Systems cybersecurity.

2. REFERENCES

The latest editions of the following publications are to be used with this Specification as applicable:

OL-TR-GR-000	*General Requirements*
OL-TR-IR-000	*Automation and Instrumentation. General*
ISA99	*Industrial Automation and Control Systems Security*
ISO/IEC 27001, 27002	*Information security standard*
ISO 15408	*Information security standard. Common criteria for Information Technology Security Evaluation*

3. TERMS AND DEFINITIONS

For general terms and definitions see:

OL-TR-IR-000 *Automation and Instrumentation. General*

AD – Active Directory is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.
Backup – Digital data copy for quick system restore.
BMS – Burner Management System.
CEG – Electrical and Automation Department Critical Equipment Group.
Contractor – a legal entity with witch the Company has concluded a contract for works related to ICS maintenance.
DCS – distributed control system.
DMZ – Demilitarized Zone.
ESD – Emergency Shutdown System.
Event Viewer – A component of the Microsoft Windows operating system that allows you to view the event log locally or remotely.
GPO – Group Policy Object controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.
ICS – Industrial Control Systems (DCS, ESD, BMS, PLC, SCADA, monitoring) common title.
ICT – Information and Communication Technology.
IT – Information Technology.
LOG – record of events taking place in systems and networks in the organization.
Log Management – The process of generating, transmitting, storing and analyzing log data.

Log Parsing – Extracting data from the log so that the parsed values can be used as input to another system.
NSC – On 19 December 2017 adopted The National Law on Cyber Security, which consolidated the security of information resources, and the functions of the national electronic communications networks, also information security incident investigation, a coherent and coordinated implementation of information policy security policies, a clear and consistent regulation of cyber security.
OT – Operational Technology.
PKI – Public Key Infrastructure used to manage digital certificates and encryption keys for people, programs and systems.
PLC – Programmable Logic Controller.
Rsyslog – An open source utility used on UNIX-like computer systems and similar to forwarding a log over an IP network.
SCADA – Supervisory Control And Data Acquisition. System for collecting, monitoring data and issuing process commands.
SIEM – Security Information and Event Management Software - A program that is used to collect, monitor and analyze data related to security. It provides correlation of information from multiple sources.
Syslog – A protocol that specifies the general format of a log entry and the transport mechanism.
TLS – Transport Layer Security protocol based on asymmetric encryption ensuring confidentiality and integrity of data transmission.
VPN – Virtual Private Network.
WEC – Windows Event Collector service that manages event subscriptions from remote sources that support the WS Management protocol.
Windows Security Log – Microsoft Windows security log containing records of security events defined by system audit policies.
WinRM – Windows Remote Management is a Microsoft implementation of WS-Management on Windows that allows the system to access or exchange management information over a common network.
Workgroup – a logical group of computers linked together by a network.

4. GENERAL REQUIREMENTS

4.1 The contractor must design and implement measures to ensure the availability, integrity and confidentiality of ICS:

- access control to ensure that only eligible and authorized access to the ICS system is possible,
- protection for malicious software,
- Software Updates for Operating Systems and implemented software according to system Vendor recommendations.

4.2 During design phase all, ICS solutions must be agreed with the ORLEN Lietuva IT Security.

4.3 The architecture of the solution should provide design to avoid single point of failure, in particular infrastructure and applications at the level required by business and approved by the IT Security of the Ordering Party (for example: operator stations, servers, networks devices).

4.4 The infrastructure dedicated to cybersecurity must be agreed with IT Department and accepted by IT Security of the Ordering Party, considering that the preferred solution is a virtual environment.

4.5 The supplier will provide warranty support services for all implemented cybernetic solutions during the warranty period - in relation to the principles of ORLEN Lietuva Cybersecurity ex. performing periodic inspections, at least once a quarter, as part of which the Contractor will update the solution, remove any irregularities in the functioning of the solution (in terms of Hardware, software), maintenance of the equipment and consultancy in the scope of the delivered configuration. The contractor will provide access to updates recommended/approved by the ICS manufacturer. Minimal Cybersecurity Requirements for ICS – OT systems.

4.6 At the bidding stage, the potential Contractor should provide a document presenting the life cycle of the solutions provided, taking into account the planned period of provided support and the planned period of ending the sale.

4.7 As part of the delivery of the solution, the Contractor will provide a complete set of necessary licenses ensuring its proper functioning.

4.8 The ORLEN Lietuva IT Security is entitled to review the cybersecurity of solutions implemented by the Contractor among others:

- vulnerability scanning,
- verification of network traffic,
- verification of the configuration,
- verification of installed solutions.

4.9 The Contractor is obliged to remove detected non-conformities and threats detected during the security review.

5. TECHNICAL REQUIREMENTS

5.1 The investment contractor must prepare an independent documentation covering all aspects of cybersecurity and architecture of ICS in compliance with the rules and regulations applicable in the Lithuania (law XII-1428 ANSI/ISA 62443) and with the guidelines of ORLEN Lietuva Cybersecurity Level within this scope.

5.2 The independent documentation covering all aspects of cybersecurity and architecture of ICS must be discussed with, settled and positively approved by the CEG.

5.3 During design phase all ICT (Information and Communication Technology) solutions must be agreed with the CEG of the Ordering Party.

5.4 The architecture of the solution should provide design to avoid single point of failure, in particular infrastructure and applications at the level required by business and positively approved by the CEG (for example: on the level operator stations, servers, Ethernet networks, power supply). Also, the solution must meet typical OT architecture requirements Appendix 1.

5.5 The infrastructure dedicated to cybersecurity must be agreed with CEG, considering that the preferred solution is a virtual environment.

5.6 The supplier will provide warranty support services for all implemented cybersecurity solutions during the warranty period – in relation to the principles of IT security rules valid for OT area.

5.7 Direct access (from external or internal network) to the Operation Technology Network (hereafter OT) zone of ICS is forbidden. External access from public networks to the OT for vendors can be granted only by IT infrastructure. IT Security is going to specify additional requirements for such access like access via VPN. Local networks, in which ICS operate, must be separated from the general field networks with use of dedicated separating firewalls.

5.8 Any Remote access shall be realized only for the defined users / computers.

5.9 The contractor must design and implement measures to ensure the availability, integrity, confidentiality and accountability of ICS:

- Access control to ensure that only eligible and authorized access to the system is possible.
- Protection against malicious software.
- Keep every software, Operation Systems and firmware up-to-date according to vendors recommendations.

5.10 The protections system implemented by investment contractor should ensure:

- Application of principles of Multilayer cybersecurity.
- Hardening ICS components (servers, stations, network devices), especially:
  - Any access (physical / logical) to the I/O ports (e.g. USB), CD/DVD must be limited. Access to this equipment only from the administrators' accounts, other users cannot have access to the specified ports;
  - Appropriate cybersecurity polices (configuration) should be defined and implemented;
  - Firewalls available from the operating system (e.g. Windows firewall) should be activated and configured so that only the services and ports that are used during the operation of ICS/Cyber Security system are enabled.
  - Unused applications must be uninstalled, unused services will be disabled;
  - Unused ports must be closed;
  - Unused services, network cards and communication protocols must be disabled;
  - Shared network recourses;
  - BIOS/UEFI settings (security password settings, USB boot disable options);
  - Disabling / deactivating protocols that transmits logon data (eg login, passwords) in an unencrypted form (eg Telnet, FTP, HTTP);
  - Unused accounts should be blocked or removed;
  - All unused data and configuration files, sample programs and scripts must be removed.

5.11 Operating system patch management, especially:

- The mechanism ensuring monitoring, obtaining and distributing patches of the operating system and ICS software recommended by the ICS system manufacturer must be delivered, installed and productively launched;

- Providing access to the latest operating system and ICS software patches validated (preferred solution)/recommended by the ICS manufacturer during the warranty period;
- Providing secure automatic mechanism to obtain updates / patches to the operating system recommended by the ICS manufacturer;
- Providing mechanisms for automatic distribution of available patches of the operating system recommended by the ICS manufacturer. Every update process shall be confirmed and performed by responsible OT administrators (i.e. CED);
- Providing, installing and implementing a central management console that monitors patches over all computer stations and servers of ICS;
- Central management console must be installed on the Awarding Entity's infrastructure (provided by the Awarding Entity or supplied by the Contractor).
- Patch Management system shall cover patches for operating system of servers, operators' stations and monitoring stations;
- Patch Management system must be in conformity with complete ICS manufacturer recommendations;
- Instructions for Patch Management system of ICS;
- Providing access to the latest ICS firmware patches validated (preferred solution)/recommended by the ICS manufacturer during the warranty period.

5.12 Antivirus system protection with self-updating database (validated signatures), especially:

- Antivirus system (preferred the Symantec, but it can be subject of negotiations in tender/design phase) must be delivered, installed and productively launched on all computer stations and servers ICS with the latest recommended/validated signatures by the ICS manufacturer;
- Providing access to the latest antivirus signatures recommended by the manufacturer of the ICS for a period of warranty;
- Providing automatic mechanism for obtaining antivirus signatures recommended by the ICS manufacturer;
- Providing mechanisms for the automatic distribution of available antivirus signatures recommended by the ICS manufacturer;
- If possible, all the computer stations (operator, engineering etc.) must have installed the same antivirus software;
- Antivirus software shall have the possibility of auto (e.g. scheduling) and manual scan options with scan results report generation. Auto scanning of external connected storage devices (e.g. via USB) is required before their usage;
- Installed software shall have possibility of remote configuration;
- Provided, installed and implemented a central console that manages antivirus software on all computer stations or servers ICS;
- Centralized management from one places (i.e. automatic changes in configuration/update spread for all others operating stations);
- Disabling, uninstalling or changing the antivirus system configuration for ICS should be possible only by the ICS system administrator after acceptance of the ORLEN Lietuva IT security.

5.13 Antimalware system protection, especially:

- The antimalware system (preferred the FireEye Hx, but it can be subject of negotiations in tender/design phase) should be installed on all components of the ICS or supporting systems in D.C. - where technically feasible;

- The antimalware system should be installed on all components in the DMZ layer - where technically possible;
- The antimalware system should be installed on ICS components implemented in the control / monitoring / protection layer of the automation (e.g. on the site), where its installation does not have a negative impact on the operation of the ICS system;
- If possible, all computer stations (operator, engineering, etc.) and servers must have the same anti-malware software implemented;
- Installed software should be able to be remotely configured;
- Delivery, installation and implementation of a central anti-malware management console on all computer stations or ICS servers;
- The server for the software's central console must be installed on the infrastructure of the Ordering Party;
- Central management from one place (ie Automatic configuration changes / updates for all other operating stations);
- Disabling, uninstalling or changing the configuration of the antimalware system for ICS should be possible only by the ICS system administrator after acceptance of the Orlen Lietuva IT Security Area.

5.14 Compliance, especially:

- A solution that provides the ability to visualize the current status of installed operating system updates and applications in relation to the patches validated/recommended by the ICS system manufacturer on all ICS components and the current status of antivirus signatures installed in relation to the ICS system recommended by the ICS system manufacturer.

5.15 Jump Server, especially:

- Jump Server must be installed on the Ordering Party's infrastructure;
- Access to the Jump Server may be made after the acceptance of the business area and the IT Security Area in accordance with the ORLEN Lietuva 2015-11-27 No. TV1(1.2-1)-343 order RULES FOR MANAGEMENT OF ACCESS TO INFORMATION RESOURCES.

5.16 Authorization and authentication, especially:

- Remote management of ICS computer stations and servers (including user accounts, password policies, access, etc.) should be performed by dedicated domain controllers located in the OT zone;
- Only the accounts necessary for the correct operation of ICS must be implemented in the ICS system (unnecessary accounts should be deleted or disabled);
- Default operating system accounts must be deleted or locked;
- ICS administrators only need to have personal accounts defined.
- Local accounts should not be used in domain-controlled ICS components;
- Remote access to ICS components can only be granted for individual access accounts – no group accounts access is allowed. In the case of configured remote access capability for individual non-privileged (standard) users, user accounts are subject to the password complexity requirements described below and the need to be changed at least once every 180 days (not apply to Operators and Administrators).

- Default login credentials must be changed prior to production state of the system.
- The implemented password management policy should be constructed taking into account the following requirements:
  - At least 8 characters long for a standard User account.
  - At least 12 characters long for a privileged account.
  - Use at least 3 out of 4 groups of characters, i.e. lowercase letter (a-z), uppercase letter (A-Z), number (0-9), special character (e.g.%, #, @, &, <, ^).
  - Password History: 6.

5.17 System for collecting logs from ICS components and sending logs to the central SIEM class solution, especially:

- The solution must ensure the collection of logs from computer stations, servers, network devices, anti-virus software, disk arrays, ICS virtual environment, backup software.
- The solution must enable the transfer of logs from ICS system components through a solution (e.g. a log server) located in the DMZ OT zone to the central instance of the SIEM class system. In addition, this solution must provide the ability to identify the source from which the logs come. The standard type of logs that are collected in the ORLEN Lietuva are:
  - Syslog source. The Logging Protocol system facilitates the transfer of information from many different types of devices and applications to a central server, known as a log server in a specific message format. This logging protocol is a key part of infrastructure monitoring (network devices, applications) and allows you to track the overall health of devices through simplified management of log messages. In Appendix 1 is an example of the network architecture used in the ORLEN Lietuva to collect syslog event.
  - Windows Event Log sources. The Windows Event Log is a detailed record of system, security, and application-related events stored in the Windows operating system. In Appendix 1 is an example of the network architecture used in the ORLEN Lietuva for collecting Windows Event Log events.
- Along with the implemented solution, proposals and good practices related to correlation rules, alerting and visualization, and implementing sources should be provided.
- The solution must cooperate / integrate with SIEM class solutions of leading and recognized manufacturers.

5.18 Infrastructure, especially:

- The Contractor must permanently label the ICS cabling on both ends in accordance with the terminology used;
- It is recommended that Mains power should be supplied from two independent sources.

5.19 Networking, especially:

- Complete protection of the designated electronic border between IT zone, OT DMZ zone and OT zone;
- Design and implementation of ICS networks separation and segmentation appropriate to the cybersecurity standards (such se NIST, ISA99);

- Access to the OT network may only be performed in accordance with the rules specified by the IT Security;
- ICS ICT networks must be separated from other networks (including corporate networks) by means of dedicated firewalls provided by the Ordering Party;
- any control systems which are not part of OT networks must be separated;
- Unnecessary traffic generated by ICS must be removed at the source of this traffic (including: Internet traffic, unused traffic, unnecessary traffic between subnets and unnecessary traffic within a subnetwork);
- All network switches (used to connect computer stations, servers, disk arrays) delivered to ICS must have all ports with a capacity of min. 1 GB (from layer L2 upwards);
- All switches supplied to ICS must be configurable, for example to disable unused ports or block unused accounts;
- Switch Port Analyzer functionality (SPAN) also called the mirror port (allowing to dump the network traffic from all other ports to one port) must be configured on switch of the ICS. SPAN/Mirror ports are to operate without affecting the performance and correct operation of the ICS;
- All switches delivered to ICS must be configured in accordance with cybersecurity rules, including disabling unused ports, disabling unused protocols, disabling unused accounts, configuring switches only via encrypted protocols;
- The network switches should be delivered, implemented and production run in the latest stable version and with the latest bug/security fixes recommended by the manufacturer of the ICS system.

5.20 Security credentials, especially:

- All access passwords with logins shall be provided together with handing over of the complete system to the ORLEN Lietuva authorized persons (including administrator, required for service works and all others necessary for ICS operation);
- Substantive credentials for ICS should be placed without undue delay in ORLEN Lietuva management system;
- All default passwords shall be changed before placing system into operation.

5.21 Data exchange with external systems, especially:

- Data exchange with external systems should take place using the OPC standard and a dedicated server installed in the OT DMZ zone.

5.22 The contractor must develop and submit to the OT Security the technical documentation for industrial automation systems necessary for the operation of the ICS, including:

- Architecture of connections between individual system components and external systems, including addressing and used port numbers and protocols (including, among others: servers, computer stations, controllers, drivers and network devices).
- Configuration of computer stations, including but not limited to:
  - operating system settings;
  - user accounts and permissions;
  - partitioning disk with configuration;
  - network adapter settings;

- firewall rules that will be implemented on firewalls in individual computer resources;
- software that will be installed / launched on individual resources;
- the services that will be started into individual applications for individual resources along with their configuration;
- ports that will be opened for individual applications on individual resources;
- configuring the antivirus software;
- settings of USB ports and CD / DVD drives on the OS system (normally disabled with the possibility of unlocking by the administrator);
- BIOS settings (including password setting, USB lock option);
- configure the security local policies and GPO policies in the OS;
- the method and policy of back-up.

- Configuration of controllers, PLC device and etc:
  - configuration of communication cards;
  - used protocols and communication channels (eg with computer stations);
  - success settings from external devices;
  - used firmware and update policy;
  - users accounts and permissions.
- Backup system, including configuration of the backup system, configuration of backup policies and their allocation to particular resources, expected maximum network load, expected backup average time.
- Antivirus system, including, among other things, its configuration broken down into individual resources.
- The update process for OS systems.
- Procedures including, among others:
  - backup procedures and manuals;
  - the procedure for updating the antivirus (database of antivirus signatures, applications);
  - operating system upgrade procedure;
  - change management procedure;
  - access management procedures.

5.23 Backups:

- The contractor must provide a security copy with the current ICS configuration.
- Backups shall cover:
  - operating systems;
  - system software and software tools;
  - application software;
  - drivers;
  - other software necessary for ICS operation;
  - data.
- Contractor shall provide instructions/manual for backups and recoveries of all installed ICS software based on information regarding availability of data.
- ICS shall be equipped with tools for backups and recoveries execution.
- Backup solution of workstations and servers of ICS has to be designed, suppled and implemented to be performed automatically. The backup system must enable: automatically in accordance with the introduced plan to make backup copies on dedicated place, automatically restored and backed up, verification of the correctness of backup copying and transfer of information to the administrator, verification of planned backup policies and changes in backup policy parameters. Backup solution must support centralized management.

5.24 Remote access to ICS:

- Remote access must be approved by business owners and IT Security.
- Remote access must be in compliance with ORLEN Lietuva IT security requirements which are implemented in local IT security directives. Signing of special NDA or VPN Agreement for remote access containing approved IT cybersecurity rules is necessary for granting of remote access.
- Remote access to ICS is only possible with the use of jump servers.
- Remote access shall be realized only via devices operating by ORLEN Lietuva infrastructure and controlled only via ORLEN Lietuva responsible administrators.
- ORLEN Lietuva IT security are allowed to make an IT security review of solutions implemented by Contractor. The Contractor is obliged to remove the findings from IT security review in the way and scope previously agreed with ORLEN Lietuva IT Security.
- The final IT architecture of ICS systems also including remote access and cybersecurity shall be agreed according to ORLEN Lietuva IT security requirements.

5.25 Procedures, including:

- Backup / restore procedures.
- Procedure for updating the database of anti-virus vaccines and anti-virus software.
- Firmware, Operating system update procedure with a detailed description of the steps to be performed to perform the update.
- Guidelines / recommendations regarding cybersecurity events that should be monitored by the Employer.

Appendix 1

Typical OT architecture

