



# 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

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

## TABLE OF CONTENTS

1.	Scope.....	3
2.	References.....	3
3.	Terms and Definitions .....	3
4.	BASIC REQUIREMENTS.....	3

## 1. SCOPE

This Specification covers requirements for Industrial Control Systems cyber security.

## 2. REFERENCES

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

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

## 3. TERMS AND DEFINITIONS

For general terms and definitions see:

<b>OL-TR-IR-000</b>	<i>Automation and Instrumentation. General</i>
---------------------	------------------------------------------------

**ICS – Industrial Control Systems** (DCS, ESD, BMS, PLC, SCADA, monitoring) common title.

**DCS** - distributed control system

**CEG** - Electrical and Automation Department Critical Equipment Group

**Backup** – Digital data copy for quick system restore.

**PLC** – Programmable Logic Controller.

**ESD** – Emergency Shutdown System.

**IT** – Information Technology.

**BMS** - Burner Management System.

**SCADA** - Supervisory Control And Data Acquisition. System for Collect, monitoring data and the issuing of process commands.

**Contractor** – a legal entity with which the Company has concluded a contract for works related to ICS maintenance

**ICT** – Information and Communication Technology.

**OT** – Operational Technology.

**VPN** – Virtual Private Network.

**DMZ** - Demilitarized Zone.

## 4. BASIC REQUIREMENTS

**4.1** 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.

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

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

- 4.4** 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).
- 4.5** The infrastructure dedicated to cyber security must be agreed with CEG, considering that the preferred solution is a virtual environment.
- 4.6** The supplier will provide warranty support services for all implemented cyber security solutions during the warranty period – in relation to the principles of IT cyber security rules valid for OT area.
- 4.7** 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.
- 4.8** Any Remote access shall be realized only for the defined users / computers.
- 4.9** The contractor must design and implement measures to ensure the availability, integrity, confidentiality and accountability of ICS:
- 4.9.1** access control to ensure that only eligible and authorized access to the system is possible.
- 4.9.2** protection against malicious software.
- 4.9.3** keep every software, Operation Systems and firmware up-to-date according to vendors recommendations.
- 4.10** The protections system implemented by investment contractor should ensure:
- 4.10.1** Application of principles of Multilayer cybersecurity.
- 4.10.2** Hardening ICS components (servers, stations, network devices) especially:
- Any access (physical / logical) to the I/O ports (e.g. USB), floppy disc station, CD/DVD must be limited. Access to this equipment only from the administrators' accounts;
  - appropriate cyber security policies (configuration) should be defined and implemented;
  - unused applications will be uninstalled, unused services will be disabled;
  - unused ports will be closed;
  - unused networking and communication protocols must be disabled;
  - unused accounts should be blocked or removed;
  - all unused data and configuration files, sample programs and scripts must be removed.
- 4.10.3** Patch Management especially:

- the mechanism ensuring monitoring, obtaining and distributed 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;
- Patch Management system shall cover patches for operating system of servers and operators stations, 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.

**4.10.4** 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 it 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).

**4.10.5**      Compliance:

- 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/recommended by the ICS system manufacturer.

**4.10.6**      Domain Controller especially:

- Remote management of ICS computer stations and servers (including user accounts, password policies, access, etc.) can be processed by a dedicated domain controller placed inside OT zone.

**4.10.7**      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 cyber security standards (such as NIST, ISA99);

- any control systems which are not part of OT networks must be separated;

- 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.

**4.10.8**      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.

**4.10.9**      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.

**4.11**      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:

**4.11.1**      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, driver, network devices).

- 4.11.2** 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.
- 4.11.3** 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.
- 4.11.4** 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.
- 4.11.5** Antivirus system, including, among other things, its configuration broken down into individual resources.
- 4.11.6** The update process for OS systems.
- 4.11.7** 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.

**4.12** Backups:

**4.12.1** The supplier must provide a security copy with the current ICS configuration.

**4.12.2** Backups shall cover:

- operating systems;
- system software and software tools;
- application software;
- drivers;
- other software necessary for ICS operation;
- data.

**4.12.3** Contractor shall provide instructions/manual for backups and recoveries of all installed ICS software based on information regarding availability of data.

**4.12.4** ICS shall be equipped with tools for backups and recoveries execution.

**4.12.5** Backup solution of workstations and servers of ICS has to be designed, supplied 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, changes in backup policy parameters. Backup solution must support centralized management.

**4.13** Remote access to ICS:

**4.13.1** Remote access must be approved by business owners and IT Security.

**4.13.2** Remote access must be in compliance with ORLEN Lietuva IT Cyber security requirements which are implemented in local IT Cyber security directives. Signing of special NDA or VPN Agreement for remote access containing approved IT cyber security rules is necessary for granting of remote access.

**4.13.3** Remote access to ICS is only possible with the use of jump servers.

**4.13.4** Remote access shall be realized only via devices operating by ORLEN Lietuva infrastructure and controlled only via ORLEN Lietuva responsible administrators.

**4.13.5** ORLEN Lietuva IT Cyber 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 Cyber security.

**4.13.6** The final IT architecture of ICS systems also including remote access and cyber security shall be agreed according to ORLEN Lietuva IT Cyber security requirements.