

Confidentiality: Internal

Support Document

Cyber security requirements for vendors

Table of Contents

0	References	2
1	Introduction	2
2	Tasks	2
2.1	System criticality qualification process	2
2.2	Acquisition process.....	2
3	Description	3
3.1	Products and Services.....	3
3.2	Supplier Personnel	3
4	Supporting documents	3
5	Justification for Modification	4

0 References

Document	SAP reference
ENGIE Industrial Control System security Framework	NA
Information Security Requirements for Process Control	ZNO.10010571878
Security Requirements for Vendors IEC 62443-2-4	NA – see WWW

1 Introduction

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as skid-mounted Programmable Logic Controllers (PLC) they are present within Engie's industrial networks and critical infrastructures.

These control systems are critical to the operation of EBL's infrastructures that are often highly interconnected and mutually dependent systems.

The purpose of this document is to provide a consolidated overview of the best practice requirements for establishing secure industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing a combination of IT and control functions.

2 Tasks

2.1 System criticality qualification process

Ensures that each industrial control system included in acquisition process has a qualified criticality level, obtained through the Engie Security Risk Assessment Methodology, and thus matched to the IEC 62443-2-4 ([Formally the WIB PROCESS CONTROL DOMAIN – SECURITY REQUIREMENTS FOR VENDORS Version II](#))

compliance level requirements as defined in the table below:

System Criticality Level	Corresponding IEC 62443 compliance level
Criticality level of 9.0 or above	Gold level compliance
Criticality level of 7.0 through 8.99	Silver level compliance
Criticality level below 7.0	Bronze level compliance

2.2 Acquisition process

Verifies that contracts for process control systems include the information security requirements and that vendors complete the IEC 62443 compliancy matrix for the corresponding compliancy level of the system.

3 Description

3.1 Products and Services

A supplier's process control & automation systems will comply with the above listed set of requirements (see Supporting Documents) which provide a combined set of ethical behavior, standards and security measures that will ensure infrastructure implementation, maintenance and operations.

ICS Security Compatible solutions contribute in attaining a high degree of security but must be supplemented with additional security controls; e.g. adequate work procedures, skills & competencies of staff, remote access and general governance and management.

For obvious practical and organizational reasons, all supplier personnel, and their subcontractors, undertake to comply with the security measures and standards used by ENGIE, i.e. to only supply software that conforms to these standards and, in developing such software, to only use tools and work methods which conform to standards authorized by ENGIE.

The undisclosed use of standards that do not conform to ENGIE's standards or which contain malware shall be considered a material breach entitling ENGIE to claim compensation from the Supplier.

3.2 Supplier Personnel

Each supplier shall appoint, from amongst its Collaborators assigned to carry out an Order, a Project responsible who shall supervise the activities of, and exercise the employer's authority over his Collaborators.

When the Services are performed, in whole or in part, at the offices of ENGIE, the Supplier's Collaborator(s), and their subcontractors, appointed to perform the Services shall at all times comply with the internal regulations of ENGIE with respect to safety and well-being at work.

When the Services are performed, in whole or in part, on computers that are the property of, or leased by, ENGIE, and which may or may not be connected to ENGIE's network, the CONSULTANT's Collaborator(s), and their subcontractor(s), appointed to perform the Services shall at all times comply with ENGIE's internal security policies and ICS security requirements. The Supplier shall ensure that these documents are communicated to, and carefully respected by, its Collaborators. If the Supplier's Collaborator(s) neglect or in any way violate the rules contained in these documents, the Supplier shall be fully liable for any damage that may occur to ENGIE as a result thereof.

4 Supporting documents

Process Control Domain Security Requirements for Vendors IEC 62443. [The IEC 62443 compliance matrix excel sheet can be requested from the purchasing department and must be completed by Industrial Control Systems vendors.](#)

5 Justification for Modification

Version nr	Reason for modification	Changed pages
00	New	All
01	Modification of the document	Pages 2-3