

GENERAL SPECIFICATION

INSTRUMENTATION

GS EP INS 135

Cybersecurity Requirements for Industrial Information Systems (SII)
--

11	11/2016	Revised as per marking
10	11/2015	Revised as per marking
09	05/2015	Organisation change - January 2015
08	10/2014	Reorganised and revised as per marking
00	10/2005	First issue
Rev.	Date	Purpose of the revision

Owning entity: DSO/TEC	Managing entity: DSO/TEC/INS
Other Approving entity(ies):	

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 2 of 28

Contents

1. Scope	4
2. Reference documents	4
3. Terminology and Definitions	5
3.1 Abbreviations	5
4. Introduction	7
5. Cyber Security Risk Assessment	7
5.1 Security Profile	8
6. Architecture	9
6.1 SIE / SII Independence	9
6.2 SII Sub Networks	10
6.3 Industrial Networks	10
6.4 Network Components	11
6.5 Commercial Off-The-Shelf Software	11
6.6 Removable Media	11
6.7 Maintenance Tools	11
6.8 Restrictions	12
6.9 Communication	12
6.10 Wireless Instruments	13
7. Patch Management	13
8. Antivirus	13
9. Back-up and Restoration	14
9.1 Disaster Recovery	15
10. Access Protection	15
10.1 Physical Access	15
10.2 Logical Access Rights	17
10.3 Passwords	17
10.4 Human Machine Interface (HMI)	18

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 3 of 28

11. Process Data Server (PDS/PI)	18
11.1 PDS/PI Nodes and Gateways	18
11.2 PDS/PI Server	18
12. SIE / SII Firewall	18
12.1 SP3 SIE/SII FW Rules	19
12.2 SP2 SIE/SII FW Rules	19
12.3 SP1 SIE/SII FW Rules	20
12.4 DMZ	20
12.5 Quarantine Work Station	21
13. Remote Maintenance and Diagnostic (RMD)	21
14. Project Organization	24
15. Audits	24
16. Tests	25
17. Cyber Security Documentation	25
Bibliography	27
Appendix 1 Security Profile and Third Party Remote Access Selection Example	28

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 4 of 28

1. Scope

This specification defines the minimum cybersecurity requirements for the design, fabrication, configuration, testing, and operation of the systems and their components which are part of the Industrial Information Systems (SII) domain.

2. Reference documents

The equipment shall satisfy the requirements and regulations of the country of installation and specific standards referred to in this specification.

Where national regulations exist, their provisions and those of the standards and codes to which they refer shall apply, supplementing or amending the provisions of this document.

The reference documents listed below form an integral part of this General Specification.

External Documents

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and addendums, is the latest revision published at the effective date of this document.

Reference	Title
AGA Report No. 12	Cryptographic Protection of SCADA Communications
API STD 1164	Pipeline SCADA Security
IEC 17799	Information technology - Security techniques - Code of practice for information security management
IEC 61511 (All parts)	Functional Safety - Safety instrumented systems for the process industry sector - All parts
IEC 62443 (All parts)	Industrial communication networks - Network and system security - All parts
RFC 1918	Address Allocation for Private Internets
RFC 2246	Transport Layer Security

Total General Specifications

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and addendums, is the latest revision published.

Reference	Title
GS EP ELE 221	Electrical Control System (ECS)
GS EP EXP 131	Design and installation of Process Data Server - Creation and administration of Asset Model using Field Share method
GS EP EXP 201	Operations preparation during project - Maintainability & Inspectability criteria

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 5 of 28

Reference	Title
GS EP EXP 403	Production Availability Studies (PAS) of oil and gas facilities
GS EP EXP 407	Identification of Safety Critical Elements
GS EP INS 100	Overall Instrumentation Philosophy
GS EP INS 101	Instrumentation Design
GS EP INS 110	Instrumentation for package units
GS EP INS 134	Design and supply of integrated control and safety system
GS EP INS 140	Instrumentation for monitoring packages
GS EP SAF 041	Technological Risk Assessment Methodology
GS EP SPS 019	Subsea production control system
GS EP TEL 170	Communications Network

3. Terminology and Definitions

There are five types of statements in this specification, the “shall”, “should”, “may”, “can” and “must” statements. They are to be understood as follows:

Shall	Is to be understood as mandatory. Deviating from a “shall” statement requires derogation approved by Company.
Should	Is to be understood as strongly recommended to comply with the requirements of the specification. Alternatives shall provide a similar level of protection and this shall be documented.
May	Is to be understood as permission.
Can	Is to be understood as a physical possibility.
Must	Expresses a regulatory obligation.
Company	TOTAL E&P or any TOTAL E&P subsidiary.
Contractor	Any Party that has signed a Contract with Company for the Engineering, Procurement, Construction, and Installation in part(s) or in full of a project.
Vendor	The package Vendor sub-contracted by the Contractor or by Company.
Supplier	The Party that manufactures or supplies equipment, either individually or as a Packaged unit for the project.

3.1 Abbreviations

The following terms and abbreviations are used in this document:

AES	Advanced Encryption Standard
CPU	Central Processor Unit
CCR	Central Control Room

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 6 of 28

COTS	Commercial Off-The-Shelf
DMZ	Demilitarized Zone
DNS	Domain Name System
ECS	Electrical Control System
ESD	Emergency Shut Down
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FGS	Fire and Gas System
FW	Firewall
HIPS	High Integrity Protection System
HMI	Human Machine Interface
ICMP	Internet Control Message Protocol
ICSS	Integrated Control and Safety System
IP	Internet Protocol
OTS	Operator Training Simulator
OWS	Operator Work Station
QWS	Quarantine Work Station
PCS	Process Control System
PDS	Process Data Server
PSS	Process Shutdown System
PI	Plant Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSS	Process Safety System
RMD	Remote Maintenance and Diagnostic
SCADA	Supervisory Control and Data Acquisition
SCE	Safety Critical Element
SCE PE	Safety Critical Element Programmable Electronic
SCS	Subsea Control System
SIE	Enterprise Information System
SII	Industrial Information System
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems (PSS, ESD, FGS)

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 7 of 28

SOE	Sequence Of Events
SP	Security Profile
SSL	Secure Sockets Layer (or Transport Layer Security RFC 2246)
SSID	Service Set IDentifier
TCP	Transmission Control Protocol
UCP	Unit Control Panel
UDP	User Datagram Protocol
VDU	Visual Display Unit
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide area network
WS	Work Station

4. Introduction

Industrial Information Systems (SII) are defined as any system and its components (hardware, software, infrastructure) which contributes directly to hydrocarbon production, the integrity, the safety and the security of oil and gas installations.

The SII encompasses Process Control Systems, Safety Instrumented Systems, package Unit Control Panels (UCP), Electrical Control Systems (ECS), Telecom Industrial systems, Subsea Control Systems (SCS), Process Data Systems (PDS/PI)... with their relevant networks and components.

This specification gives the requirements to minimize cyber security risks when designing and supplying any system which is part of the SII. The objective is that SII systems shall have cyber security protection methods integrated into the design from the start and not just an “add-on” when the equipment is delivered.

Therefore this specification shall be applied in conjunction with all General Specifications for equipment within the Industrial Information System domain and specifically: [GS EP INS 134](#), [GS EP INS 110](#), [GS EP INS 140](#), [GS EP ELE 221](#), [GS EP EXP 407](#) and [GS EP SPS 019](#).

Any system determined not to be part of the Industrial Information System domain shall automatically be part of the Enterprise Information System domain (SIE). All systems must belong to one of these domains.

These minimum requirements shall be enhanced by a cyber security risk analysis.

Recommendation and requirements of the [IEC 62443](#) shall be followed.

5. Cyber Security Risk Assessment

An inventory of all systems, subsystems, networks, equipment, components which are part of the SII shall be prepared prior to the risk assessment. This inventory aims to define the SII in order to ensure that all systems are covered.

A cyber security risk assessment (see [IEC 62443-2-1](#)) shall be performed at an early stage of each project phase (e.g. basic or detail design stage) or after a modification (e.g. network, servers, systems...).

The cyber security risk assessment shall be performed with a 5-steps approach and shall be seen as an iterative and continuous process.

The following 5-steps shall be addressed:

1. Define the risk analysis methodology (e.g. architecture based)
2. Identify major items (organization, systems, subsystems, networks)
3. Identification, evaluation of the threat scenarios with their impact and likelihood
4. Reduce the risks by designing adequate countermeasures
5. Summarize the results in a Risk Register.

A cyber security risk assessment report shall be issued with the Findings, the Recommendations and the Risk Register.

This risk assessment report shall include the default SII cyber security countermeasures in line with this General Specification as well as all additional cyber security measures required to mitigate the risks identified during the Risk Assessment Study.

The cyber security risk assessment findings and recommendations shall be implemented in the Project Cyber Security Documentation.

The cyber security risk assessment can be performed using guidelines from [IEC 17799](#), API & NPRA, [GS EP SAF 041](#), [GS EP EXP 201](#) and [GS EP EXP 403](#).

5.1 Security Profile

Based on the risk assessment the systems, or sub-systems shall be assigned a security profile; SP1, SP2 or SP3, where SP3 is the most stringent. The security profile shall then determine the minimum level of cyber security protection requirements.

The Security Profile shall be determined based on the fundamental risk without taking into account any risk reduction factors or mitigation measures.

The relation between the initial Risk Level and the Security Profile is:

Figure 1 - Risk Level vs. Security Profile Relationship

Risk Level (GS EP SAF 041)	Security Profile
Level 3	SP-1
Level 2	SP-2
Level 1	SP-3

By default the following is applied:

- SIS ([GS EP INS 134](#) & [IEC 61511](#)) and Safety Critical Element with Programmable Electronic (SCE-PE) (Note 1) ([GS EP EXP 407](#)) shall be classified SP3.

General Specification		GS EP INS 135
Cybersecurity Requirements for Industrial Information Systems (SII)		
Rev.: 11	Effective date: 11/2016	Page: 9 of 28

- Monitoring systems (e.g. integrity, environment) are generally defined as P4 Packages ([GS EP INS 140](#)). Monitoring systems which are not classified as SCE-PE, which are independent and have no communications with other SII systems with different security profile (although may have hardwired interfaces) should be classified SP1.
- All other systems shall be classified SP2. SP2 generally encompasses all SII systems essential to the production (e.g. PCS as per [GS EP INS 134](#), P3 Packages as per [GS EP INS 110](#)).

Appendix 1 provides examples of SII systems with their security profile classification.

Note 1: The term Programmable Electronic (PE) comes from the [IEC 61511](#).

It is defined as an item based on computer technology which may be comprised of hardware, software, and of input and/or output units. This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector PE include:

- Smart sensors and final elements
- Programmable electronic logic solvers including:
 - Programmable controllers
 - PROGRAMMABLE logic controllers
 - Loop controllers.

6. Architecture

SII architecture is defined in [GS EP INS 100](#). Any maintenance network or cyber security countermeasures such as backup, antivirus, patch or any other maintenance tools shall not affect the architecture segmentation design or the segmentation between SII zones with different security profile.

The "network" functions (e.g. router / switch) and "security" function (i.e. firewall) shall be performed by dedicated equipment.

In the particular case of SCADA, often used for pipeline applications, the design shall be in line with [API STD 1164](#) and [AGA Report No. 12](#) statements and recommendations. Specifically the architecture shall be designed to secure the communication paths between the different units of the system.

Operator training simulators shall not be connected to the SII.

6.1 SIE / SII Independence

The SII shall be physically and functionally independent from the Enterprise Information System (SIE).

The SII shall not be connected to the SIE network unless a specific need for transferring data has been identified and is required. If it is required, then the SII shall have one (or a maximum of 2) connection point(s) to the SIE network through a dedicated security device (i.e. Firewall) whose purpose is to filter the traffic between SII and SIE network.