

GENERAL SPECIFICATION

INSTRUMENTATION

GS EP INS 135

**Cyber Security requirements for design and supply
of ICSS and Package Systems**

07	11/2012	Revised as per marking
06	01/2012	Revised as per marking
05	01/2011	Revised as per marking
04	10/2009	Revised as per marking
00	10/2005	First issue
Rev.	Date	Purpose of the revision

Owning entity: DEV/TEC

Managing entity: DEV/TEC/INS

General Specification		GS EP INS 135
Cyber Security requirements for design and supply of ICSS and Package Systems		
Rev.: 07	Effective date: 11/2012	Page: 2 of 24

Contents

1. Scope	4
2. Reference documents.....	4
3. Glossary.....	5
4. Introduction	6
5. Risk Assessment	7
6. Architecture	8
7. Communication	8
7.1 Wireless	8
8. Commercial Off-The-Shelf Software.....	9
8.1 Configuration	9
8.2 ICSS and Package P3 Peripherals.....	9
8.3 Antivirus Software	10
9. Industrial Networks	10
9.1 Network Components.....	11
10. Access Protection	11
10.1 Physical Access	11
10.2 Logical Access Rights	12
11. Human Machine Interface (HMI).....	13
12. Process Data Server (PDS/PI)	13
12.1 PDS/PI Nodes and Gateways	14
12.2 PDS/PI Server.....	14
12.3 PDS/PI Study	14
13. Firewall.....	14
13.1 DMZ.....	15
14. Maintenance	16
14.1 Remote Maintenance and Diagnostic (RMD)	16

General Specification		GS EP INS 135
Cyber Security requirements for design and supply of ICSS and Package Systems		
Rev.: 07	Effective date: 11/2012	Page: 3 of 24

14.2	Maintenance Tools.....	18
15.	Project Organisation	19
16.	Audits	19
17.	Tests.....	20
18.	Documentation - Cyber Security Dossier.....	20
Appendix 1	SII Functions Sensitivity Example.....	22
Appendix 2	Third Party Remote Access.....	23

1. Scope

This specification defines the minimum cyber security requirements for the design, fabrication, configuration, testing, and operation of Integrated Control & Safety Systems (ICSS), package Unit Control Panels (UCP) and associated instrumented industrial systems.

This specification applies to all programmable electronic systems, networks and human machine interfaces, like the ones used for wells, process, machineries, monitoring systems, Sub Sea and electrical automatic control. These systems are part of the Industrial Information System (SII).

2. Reference documents

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 supplements, is the latest revision published at the effective date of this document.

Reference	Title
AGA 12	Cryptographic Protection of SCADA communication
API 1164	Pipeline SCADA security
IEC 17799	Information Technology- Security techniques - Code of practice for information security management
IEC 62443 (All parts)	Security for industrial process measurement and control - Network and system security - All parts
ISA 99 (All parts)	Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program - 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 supplements, is the latest revision published in the applicable yearly collection.

Reference	Title
GS EP ELE 221	Electrical Control System (ECS)
GS EP EXP 131	Design and installation of Process Data Server
GS EP EXP 201	Operations preparation during project - Maintainability & Inspectability criteria

Reference	Title
GS EP EXP 403	Production Availability Studies of Oil and Gas Facilities
GS EP INS 110	Instrumentation for package units
GS EP INS 111	Design and supply of liquid custody transfer metering units
GS EP INS 112	Design and supply of gas custody transfer metering units
GS EP INS 134	Design and supply of integrated control and safety system
GS EP INS 150	Design method for system configuration - Standards functions
GS EP SAF 041	Technological risk assessment methodology
GS EP SPS 019	Subsea production control system
GS EP TEL 170	Design and installation of Communications Network

3. Glossary

AES	Advanced Encryption Standard
CPU	Central Processor Unit
CCR	Central Control Room
COTS	Commercial Off-The-Shelf
DMZ	Demilitarized Zone
ESD	Emergency Shut Down
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FGS	Fire and Gas System
ICMP	Internet Control Message Protocol
ICSS	Integrated Control and Safety System
IP	Internet Protocol
HIPS	High Integrity Protection System
HMI	Human Machine Interface
HIPS	High Integrated Protection System
PCS	Process Control System
PDCS	Power Distribution Control System
PDS	Process Data Server
PSS	Process Shutdown System
PI	Plant Information

General Specification		GS EP INS 135
Cyber Security requirements for design and supply of ICSS and Package Systems		
Rev.: 07	Effective date: 11/2012	Page: 6 of 24

PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSS	Process Safety System
RMD	Remote Maintenance and Diagnostic
SCADA	Supervisory Control and Data Acquisition
SIE	Enterprise Information System
SII	Industrial Information System
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems (PSS, ESD, FGS)
SSL	Secure Sockets Layer (or Transport Layer Security RFC 2246)
SSID	Service Set Identifier
TCP	Transmission Control Protocol
OWS	Operator Work Station
UCP	Unit Control Panel
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
SSL	Secure Sockets Layer
WAN	Wide area network

4. Introduction

Process Control System (PCS), Safety Instrumented Systems (SIS), Supervisory Controls and Data Acquisition System (SCADA), Programmable logic Controller (PLC), Package P3 Unit Control Panel (UCP) and Package P4 Systems referred to in this document are part of the Industrial Information System (SII).

In the recent years, they have increasingly relied on commercial information technologies such as "Ethernet", "TCP/IP" and "MS Windows™" for both critical and non critical computing and communications.

The use of these commercial protocols and operating systems has made the interfacing of control equipment much easier, but there is now significantly less isolation from the outside world. Network security issues and vulnerabilities found on the world and in the Enterprise Information System (SIE) can now be passed to process control networks and operating systems.

This specification gives the requirements to minimise the risks when designing and supplying an ICSS & package control and monitoring systems part of the SII. Package control system designates all systems controlling process equipment, machineries, electrical networks, subsea equipment, metering system and others. Therefore this specification shall be applied in

General Specification		GS EP INS 135
Cyber Security requirements for design and supply of ICSS and Package Systems		
Rev.: 07	Effective date: 11/2012	Page: 7 of 24

conjunction with [GS EP INS 134](#), [GS EP INS 110](#), [GS EP INS 111](#), [GS EP INS 112](#), [GS EP ELE 221](#) and [GS EP SPS 019](#).

These minimum requirements shall be enhanced by a risk analysis.

Recommendation and prescription of the [IEC 62443](#) and [ISA 99](#) shall be followed.

5. 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.

The Risk Assessment shall be initially performed at an early stage (i.e. During the Basic Engineering Phase or FEED).

The Risk Assessment Study 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: quantitative vs. qualitative, metrics, steps dedicated to a Project
2. Identify major items (organization, systems, subsystems, networks) and their security impacts in term of availability, integrity, confidentiality and proof (Note 1)
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 Risk Assessment Report shall be issued with the Findings, the Recommendations and the Risk Register.

This Risk Assessment with its relevant Inventory shall be reviewed during each Project Phase (i.e. Basic and Detail or after major modification) and during the Operation Phase every five years or after major modification.

The Risk Assessment Report shall include the default SII cyber security measures 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.

This Risk Assessment Report shall be classified CONFIDENTIAL.

The Risk Assessment Findings and Recommendations shall be implemented in a particular Project Cyber Security Specification.

The Risk Assessment Study can be performed using guidelines from [IEC 17799](#), API & NPRA, [GS EP SAF 041](#), [GS EP EXP 201](#) and [GS EP EXP 403](#).

Note 1: An example of the sensitivity table of major SII functions is given in Appendix 1. This table gives an impact rating at site level resulting in a loss of availability, integrity, confidentiality and proof (or traceability) of the main functions of the SII.

General Specification		GS EP INS 135
Cyber Security requirements for design and supply of ICSS and Package Systems		
Rev.: 07	Effective date: 11/2012	Page: 8 of 24

6. Architecture

The SII (see the general architecture in the [GS EP INS 134](#)) 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.

The SII shall have one connection point to the SIE network through a dedicated security device (i.e. Firewall) whose purpose is to filter the traffic between SII and SIE network.

The architecture of this connection shall be designed to allow for the physical disconnection from the SIE network at any time in case of high cyber risk. However, the SII systems shall not be impacted by disconnecting the SIE / SII link.

The architecture shall be designed in such a way that all functions shall be implemented on the appropriate equipment, in accordance with the reliability/safety and cyber security levels. As an example, Operator workstations shall not be used for production management, and control functions shall not be performed from PDS/PI HMI.

In some cases an "industrial" firewall may be implemented within the SII network to logically separate and control different SII sub-networks.

In the particular case of SCADA, often used for pipeline applications, the design shall be in line with [API 1164](#) and [AGA 12](#) statements and recommendations. Specifically the architecture shall be designed to secure the communication paths between the different units of the system.

7. Communication

In case of remote control through radio communication (e.g. satellite platform), a specific Cyber Security Communication Study shall be made in co-ordination with Telecom specialists in order to define the need to implement VPN (Virtual private Network) tunneling. This is the case when a shared media like public telephone lines or radio links supporting other functions (voice/ SIE data) is used in order to connect two separate industrial networks. This should also be implemented when using non secured media.

7.1 Wireless

Connection of any wireless equipment directly on an intra sites SII network is not allowed. In case this technology is proposed a specific study is required. The study and the decision shall be validated by Company during the Pre-project phase.

Wireless used for inter-sites connections between SII sub networks is allowed. This wireless interconnection shall comply with the minimum rules as follows:

- Non disclosure of the SSID
- Use of available free frequencies after spectral analysis and validation by the regulatory authority (recommended whether applicable)
- Alarm detection in case of signal intrusion
- Encryption of the radio segment (between the radio units)