

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)

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: 9 of 24

- Access to the wireless devices with strong authentication
- Implementation of a VPN tunnel (e.g. IPSec) between the SII sub networks of the interconnected sites.

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

An availability study shall be performed to verify the wireless communication compatibility with the operating philosophy e.g. Redundancy links/equipments, loss of service scenario...

The compatibility of the solution (bandwidth, latency, jitter, redundancy, etc) with the data transmission requirements shall also be studied.

8. Commercial Off-The-Shelf Software

8.1 Configuration

Commercial Off-The-Shelf (COTS) Software including the Operating System (OS) of any equipment shall be properly configured to minimise cyber risks.

This shall be achieved by disabling all services not used for the dedicated control or safety software.

Administrator/user accounts shall be defined. Administrator account shall be dedicated to COTS management only (with administrative privileges). All ICSS or package system applications shall run under user account with restricted rights (no administrative privilege).

Configuration of the operating system shall be described in a dedicated document.

COTS software configuration shall be audited during specific testing.

File system permission shall be described.

Back-up and restoration procedures (after crash) of COTS configuration shall be written and tested (including back-up tools).

Vendors shall design the system in order to permit safe update of the Operating System (patches) described in dedicated procedures.

COTS software configuration of any equipment within the SII shall not be accessible to Operator or maintenance team, but only to the assigned SII administrator with specific access rights and authentication. This shall also be the case at power-up.

System audit log shall be configured to allow security auditing. Time synchronization of all equipment on the SII network shall be implemented.

8.2 ICSS and Package P3 Peripherals

External mass storage devices (Floppy, CD-ROM, tape drive, etc.), interfaces ports (serial interface, USB ports, etc.), printers, routers, switches, central processing units, more generally all SII devices shall not be functionally and/or physically accessible. This can be achieved for example by BIOS configuration and/or by physical protection (USB locks, locked enclosure or cabinets) or by physical removal of subject interfaces, ports, or devices.

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: 10 of 24

8.3 Antivirus Software

Antivirus software shall be installed on all workstations (i.e. Engineering, Maintenance, Operator) and servers.

Configuration of the antivirus software is the responsibility of Vendor, in order not to impair the behavior of the device (specifically the Operator workstations).

The Vendor will specify which directory/files not to scan (with justification), the scanning periodicity and sequence for several workstations, automatic action to be taken after detection, etc.

Company may specify the preferred antivirus brand to be used for the project; in this case the Vendor shall validate the specified software.

An AntiVirus server (for example the maintenance/engineering workstation) within the SII shall allow for regular & automatic updates of all workstations after downloading the server with the AntiVirus file/directory data base. This file/directory shall be downloaded on the AV server either manually or automatically from the DMZ (for example using an "FTP get" command.). Logging of events shall be configured in order to report any detection on the Antivirus server.

The antivirus policy shall ensure that the antivirus updates are verified prior to installation. The system shall allow for the updates to be staged in order to allow the update to be verified on a single station prior to updating on all.

Safety Instrumented Systems (PSS, ESD, FGS), as well as any HIPS workstations, shall be individually updated manually. Stand alone Packages such as P3 or P4 not connected by a network with the AV Server may be updated manually and individually.

Tools and procedure for updating the antivirus knowledge base shall be provided and tested for all systems within the SII.

9. Industrial Networks

Industrial networks belonging to SII shall be properly configured to minimise cyber risks. This shall be achieved by disabling all network services not used for the dedicated control or safety operation. This includes all networks specific equipments such as switches & routers.

Network design shall comply with **GS EP TEL 170**.

Administration of the industrial network belonging to SII shall be performed within the SII domain (no administration from the SIE domain or office network). Administration protocols shall comply with **GS EP TEL 170** and their implementation shall be a secure version (e.g. SNMP v3).

IP addressing plan shall be defined at the beginning of the project, and approved by Company. If not otherwise specified, for SII equipments, non routable IP addresses ranges as per **RFC 1918**: from 172.16.0.0 to 172.31.255.255 shall be used.

IP address plan being confidential, IP address shall not be written on the equipment.

Connection of equipment on a spare physical connection port of the network shall not be possible (either physically or logically) without an administrator level intervention and control and with specific provided tools.

SII network configuration (all equipment) shall be described in a dedicated document.

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: 11 of 24

Back-up and restoration procedures (after crash) of network configurations (all network equipments like routers, switches, firewall, etc.) shall be written and tested (including back-up tools). Independent dedicated media / servers for back-up shall be provided.

Network configurations shall be audited during specific testing.

9.1 Network Components

All network components (hubs, switches, routers, etc.) shall be of industrial type: either rack or DIN mounted with redundant power supplies.

They shall not downgrade the whole reliability.

They shall be validated and fully supported by ICSS Supplier or P3/P4 Package Supplier.

10. Access Protection

To maintain cybersecurity during operation of vital/critical functions with respect to the four criteria of Appendix 1, protection from undue access, either physical or logical, shall be implemented.

Risk assessment shall be the basic tool to identify the specific measures to be implemented on each piece of equipment.

10.1 Physical Access

Care shall be taken in the physical location of sensitive devices in Control Room and Technical Rooms. A specific assessment shall be performed.

When the sensitivity level in one category is greater or equal to 2 (Appendix 1), the information or equipment contributing to the associated function is considered as sensitive.

There are four different types of areas, presented here in increasing order of security:

- WHITE areas, where no measures are required. They do not contain any sensitive information or equipment
- YELLOW areas, which contain sensitive equipment, but which are easy to protect or where the risk is low
- ORANGE areas, which contain very sensitive equipment or information and/or in which staff may work, where the risk can be high and in which security is therefore reinforced (case of networks room, rooms containing firewalls, servers, maintenance tools)
- RED areas, which contain particularly security - sensitive information or equipment (not relevant in SII).

Instrument technical rooms and control rooms will be generally classified as either yellow or orange area.

Depending upon classification, associated risks and operation constraints then specific technical measures can be applied to each room, ranking from simple to more sophisticated solutions:

- Proximity detectors to control door status (open/close) and presence detectors connected to ICSS I/O's

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: 12 of 24

- Rooms locked with a security key. A register of the holders of means of access shall be kept up to date
- Access controlled by a card reader or biometric authentication device, and the opening of doors (and sometimes windows) permanently controlled and recorded.

Yellow area should have an access control system by security key.

Orange area should have an access control system by card reader or equivalent.

A specific room with restricted access to protect specific sensitive systems shall be designed ("computer room"). It shall be classified as ORANGE area, with a restrictive and controlled physical access.

These specific sensitive systems are, but not limited to:

- Engineering Work Stations
- configuration data bases
- Historical data base
- Network management tools
- Network devices and security devices.

Operator Work Stations of specific systems such as, but not limited to, condition machine monitoring system, Multiphase meter system, Overall Flow metering System will not be installed in such Computer room.

The physical access requirements (access to mass storage/interface ports, etc.) are not applicable for the sensitive equipments located in the orange access restricted "computer room".

Equipment dedicated to control or safety such as Operator Work Station Central Units, firewalls, Network devices, etc. shall be installed in closed enclosures fitted with locks.

10.2 Logical Access Rights

Typically 5 access levels may be implemented in an ICSS or package system (GS EP INS 134 & GS EP INS 150):

- Visitor (or read only): No action possible on Process. For Work Stations used for information only and for initial start-up of the Work Station
- Operator (or operation): control of the unit or the part of unit the Operator is in charge of
- Maintenance: adjustment and maintenance (modification of PID tuning parameters alarm limits modification, bypasses setting, etc.)
- Method: process parameter modifications, limited application software modification
- Engineer: all application software modifications, system administration.

The last three levels correspond to different tasks of maintenance or system administration. Sometimes the method level is not implemented.

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: 13 of 24

Functional access location may be:

- Locally on the equipment itself
- On site but remote from the equipment location
- Remote from site but in the affiliate either within the SII domain or within the SIE domain, remote from E&P location outside the affiliate.

For each access location, and each level or more accurately each task or job, an authentication level shall be assigned with the list of authorized personnel taking in account the sensitivity of the accessed system. The access authorizations must be assigned by name.

Authentication levels may be:

- Group Identification only (generic password per group)
- Authentication (individual account: identifier + password)
- Strong authentication (smart card + pin code or fingerprint reader).

Using of generic password shall be avoided and justified.

In the case of use of password, the system shall allow and request for regular changes. Passwords shall have a minimum of seven characters of three types (letters, numbers, special).

From these considerations and following the risk analysis, the strategy for defining logical access rights shall be written and implemented. However strong authentication shall be implemented for remote access.

The ICSS or package system shall be provided with the tools to implement and manage the access right strategy.

11. Human Machine Interface (HMI)

A specific access assessment study shall be performed with the HMI design to define in details the access levels.

The Operator workstations shall not be used as Operator interface for functions not directly related to control. Similarly, control HMI should not be implemented on other functions' dedicated equipment (for example PDS/PI consoles/office workstations, etc.).

All mass storage and interface devices should not be accessible to Operator.

At power-up the Operator workstation shall be initialized in the "visitor access" mode with no access to operating system commands. For workstation installed in a remote non-permanently manned technical room, after a time out the workstation shall automatically switch back to the "visitor access" mode or power off.

12. Process Data Server (PDS/PI)

Process Data Server / Plant Information (**GS EP EXP 131**) shall be used for interfacing the ICSS, P3/P4 Packages, subsea control systems and associated systems which need to be monitored from the SIE.

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: 14 of 24

12.1 PDS/PI Nodes and Gateways

Dedicated PDS/PI nodes and gateways for the ICSS shall be installed in the SII.

Dedicated PDS/PI node(s) and gateway(s) for the P3 Packages shall be installed in the SII.

A dedicated PDS/PI node and gateway for the P4 packages should be installed in the SII. However, where few P4 packages exist this function may be combined in the P3 package node.

Means to back-up, protect, restore and configure the PDS/PI (system/network/software and application) shall be implemented.

12.2 PDS/PI Server

The PDS/PI server shall be installed in the SIE.

12.3 PDS/PI Study

A specific study shall be performed during the Basic Engineering and/or when starting the EPC and shall contain as a minimum:

- The Packages which have to be monitored from the SIE
- The ICSS requirements
- The PDS/PI related architecture
- The PDS/PI node/gateways/servers/client hardware and software quantity and capacity
- The equipment location (offshore/onshore)
- The relevant telecom requirements
- A table describing the traffics (IP address source and destination, protocol, ports number, service description) between the SII and the SIE domains
- The firewall rules
- The testing requirements...

This study shall minimize the traffic for protecting the SII.

This study shall be validated by Company.

13. Firewall

Firewall shall be installed between the SII and the SIE domains. There shall be a maximum of 2 firewalls:

- 1 firewall between SII/SIE for traffic related to ICSS, P3 packages and subsea control system
- 1 firewall between SII/SIE for traffic related to P4 packages.

This is in order to avoid propagation of any incident and ensuring no uncontrolled traffic between functionally independent systems (refer also to risk analysis).

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: 15 of 24

The following rules shall be applied for firewall configuration:

- The base rule set shall be DENY ALL, PERMIT NONE.

Ports and services between the SII, the SIE and the DMZ shall be enabled and permission granted on a specific case by case basis. The authorized traffic shall be approved by Company.

The firewall shall follow the following rules:

- All "permit" rules shall be IP address, TCP/UDP, service and port specific
- All rules shall restrict traffic to specific IP addresses
- Any non-IP protocol shall also be filtered
- Any inbound traffic from SIE to SII is not allowed
- Any permanent inbound traffic from DMZ to SII is not allowed
- Non-permanent inbound traffic from DMZ to the SII may be allowed (note)
- All outbound traffic from SII shall terminate in the DMZ
- Direct traffic from SII to SIE is allowed only for the port 5450 (PDS/PI)
- To improve isolation, any protocol/services allowed between the SII network and DMZ should not be explicitly allowed between DMZ and SIE office LAN (and vice-versa)
- Source and destination shall be restricted by service / port and shall be stated in the firewall rules.

Firewall brand shall be specified by Company. The configuration shall be performed by a specialist personnel designated and approved by Company. Firewall configuration is confidential and shall only be disclosed to an agreed restricted list of persons.

Note: For RMD application, non-permanent inbound traffic from the DMZ to the SII may be allowed (e.g. "browsing", "polling" used for data packets transfer). The relevant targeted network(s) shall be independent from any other SII networks and all the Ports and Services shall be identified. Modification and/or control of the targeted network equipment shall not be possible. This type of application shall be documented in the RMD Technical Design Dossier, tested and subject to Company Approval. For details refer to section 14.

13.1 DMZ

DMZ ([ISA 99](#) & [IEC 62443](#)) may be used for Antivirus Servers, Patch Management Servers and Remote Maintenance and Diagnostic Servers.

The equipment located in the DMZ may be supported by several hardware/software servers.

All applications involving communication with the SIE e.g. Antivirus, OS patch, Vibration analysis system, or for a remote connection shall be addressed.

A specific Remote Maintenance Study shall be performed at an early stage of the project for defining in detail the architecture around the DMZ.

This study shall describe all the detailed mechanisms for communications through the firewall (software/hardware, source, destination and service or TCP/IP ports allowed with purpose).

This study shall minimise the traffic in order to protect 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: 16 of 24

This study shall result in a hardware and software architecture drawing and a table describing the traffics (IP address source and destination, protocol, ports number, service description) between the SII, the DMZ and the SIE domains.

This study shall be validated by Company.

14. Maintenance

14.1 Remote Maintenance and Diagnostic (RMD)

According to project specific requirements, vendors may require to have access to data from the SII domain, remotely, from outside the Company SIE network for maintenance or diagnostic purposes. All remote access shall require a specific study which shall be subject to approval by Company RSSC.

There are 2 types of Remote Maintenance and Diagnostic access:

- **Type 1**

Remote Maintenance by monitoring of specific plant data for supervision and analysis purposes (permanent connection and read only)

- **Type 2**

Remote Diagnostic for troubleshooting, diagnostic or administrative purpose (Antivirus Patch, COTS update...). This access shall be limited in time (non permanent connection read/write function).

Remote Access cyber security protection means shall be provided with the minimum following requirements:

- **Proof** Strong Authentication - Each Vendor that connects shall be authenticated with a PKI certificate issued by Company
- **Confidentiality** All flows crossing public networks (e.g. Internet) shall be encrypted
- **Integrity** Vendor PC conformity to Company requirements (to connect to Company security gateway, the Vendor PC shall have a supported antivirus program running, with virus signatures no older than 60 days).

The general principle is that direct connections between the systems within the SII domain and the outside world via Internet for any purpose through the use of modems etc are forbidden

The remote vendor shall gain access to Company SIE network only via Company DMZ (i.e. Total Connect).

The remote vendor shall not have direct access to SII but access via intermediary servers.

Any form of remote maintenance or diagnostics on Safety Instrumented Systems (PSS, ESD, FGS, HIPS) is forbidden.

- **Type 1** access is split into 2 sub-types

- **Type 1a** access shall be carried out using the PDS/PI. Data will be made available to PDS/PI server on SIE. Remote access will therefore collect data from the PDS/PI server.

- **Type 1b** access shall be used in cases where PDS/PI cannot be used. For this sub-type a specific remote access server shall be installed in SII/SIE DMZ. This RMD server will receive data from the system within SII domain. Remote access vendor will then be able to communicate with the RMD server through an SSL connection via Company DMZ (Total Connect).
- **Type 2** access shall only be given to Vendor with specific means and procedure. These means and procedure shall allow site personnel to have a permanent and full control of the remote access operation, initiation and stop. Logging of all operations shall be performed.

A specific remote access server shall be installed in SII/SIE DMZ. This RMD server will receive/transmit data from/to system within SII domain. Remote access vendor will then be able to communicate with the RMD server through an SSL connection via Company DMZ (Total Connect).

Appendix 2 gives the Remote Access Requirements for P3 and P4 Packages Historical Data systems, and ICSS. An example of a remote access architecture is also shown.

14.1.1 Remote Maintenance and Diagnostic Study

Each Remote access shall be subject to a Specific Study generally split into 6 parts. The study shall require to be approved by Company RSSC.

1. Needs Definition

It shall define, as a minimum:

- The objective of why a remote access is required (maintenance contract requirement, specialist expertise)
- Define what data is required to be accessed
- Define whether access is Type 1 or Type 2
- Confirm for a Type1 access whether use of PDS/PI is possible
- Define which system/equipment within SII is to be accessed
- Define roles and Responsibilities for the implementation and maintenance
- Define the schedule
- Provide an initial Risk Analysis.

2. Project Execution Plan

It shall detail, as a minimum:

- Detailed roles and responsibilities of the different parties involved
- Detailed organigramme
- Detailed schedule
- Contract execution
- Technical principles of the remote access.

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: 18 of 24

3. A RMD Technical Design Dossier

It shall include as a minimum:

- Interconnection Study including detailed infrastructure requirement such as additional devices, Strong Authentication/PKI management, Encryption Management, Antivirus Management for all parts of the access chain
- Obsolescence study for the proposed equipment
- Detailed Risk analysis identifying the risks, their impacts and likelihood and the related mitigations
- Wide area network (WAN) Interconnection Study (Networks flow: volume/necessary bandwidth /data types)
- Virtual Local Area Network (VLAN) Study (Inventory of the local connectivity: switches/routers, the wiring diagrams, the IP addresses, the Network Address Translation (NAT) part of the SIE, the DMZ and the SII)
- Firewall Management (Firewall ports, Firewall Rules)
- Deployment requirements (Company DMZ, WAN and VLAN including the Firewall).

4. Procedures for Vendor/Supplier/Contractor Connection

5. A Test Plan

It shall encompass the “end to end” RMD connection from data source in SII up to the Vendor/ post via the overall infrastructure.

6. The Hand-Over Dossier

It shall include, as a minimum:

- Deliverables from 1 to 5
- A completion certificate.

14.2 Maintenance Tools

The SII subsystems (ICSS mainly) shall be supplied with access management tools allowing for ID/password control and management with logging of access requests.

SII internal networks shall be monitored by dedicated management tools. They shall be provided by system Vendor as part of the EWS. They shall comply with the Company Standard (GS EP TEL 170). They shall enable configuration, diagnostic of all networks equipment (Hub/Switches/ routers/industrial firewalls, etc.) within SII battery limits.

System and network alarms shall be integrated in the alarm management system.

Antivirus detection alarms shall also be integrated in the system alarm management and diagnosis tool.

All security related events shall be logged.

Backup tools shall be part of the standard maintenance tool package provided with the EWS and it shall provide capability for a full backup (system/network/application & data) and quick recovery.

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: 19 of 24

15. Project Organisation

The cyber security of the Industrial Information systems shall be addressed throughout the execution of the project. To achieve this requirement, specific procedures shall be prepared by the Contractor and Vendor and included in the quality plan:

- Back-up management procedure during construction, testing and commissioning
- Management of modification or changes (evolution/error corrections, etc.)
- Management of physical access to construction/development platform
- Management of logical access to construction/development platform and related software (include password management and administrative rights)
- Antivirus shall be operational and updated during construction, test and commissioning
- Management of software's update (operating system and patches, specific Vendor software's, etc.)
- Operating system, network software, antivirus, etc. shall be updated during all life of the project (design/construction/FAT/commissioning, etc.) up to the end of warranty period. An additional one year upgrade support shall be given to allow for continuity with maintenance Contract.

During the design, construction and test phases of the SII functions, reviews by a Contractor assigned third party cyber security specialist shall be performed.

All passwords/pin numbers, etc., shall be initialized with new values before the handover of the systems.

All software licenses shall be transferred to Company at handover.

It shall be noted that cyber security rules shall be applied to all phases and parts of the project, including when a dedicated temporary or testing commissioning architecture is implemented.

16. Audits

Audits shall be initiated by Company to:

- Verify the documentation - Cyber Security Dossier
- Verify Operating System and network configurations
- Perform intrusion testing
- Evaluate system robustness to cyber attack
- Identify the vulnerabilities.
- Verify cybersecurity organization.

These audits shall be conducted during the Design Validation Test and the FAT, or at any other time defined by Company.

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: 20 of 24

17. Tests

Specific tests shall be performed to demonstrate the conformity to specification:

- Testing of SII to SIE communication with the configured Firewall
- Intrusion testing to verify Firewall configuration
- Testing of antivirus configuration to verify impact on control, detection capability and response
- Testing of antivirus update procedure
- Testing of operating system and network, access administration tools (password/key management, account organization, running system and network services, configuration of network equipments, file management system configuration, etc.)
- Testing of operating system and network configuration vulnerabilities (using specific tools)
- Testing of all back-up procedures (operating system and network configuration, historical data, specific and application software's)
- Testing of all restoration procedures (operating system and network configuration, historical data, specific and application software's)
- Test of remote connection and associated procedures when applicable
- Test of all maintenance tools.

Most of these tests shall be performed during the FAT (Factory acceptance tests).

Test program and results shall be validated by Company.

Operating and network related tests and audit shall be performed in two stages: a first test during the design validation tests and a second test during FAT to verify corrective actions.

18. Documentation - Cyber Security Dossier

A specific Cyber Security Dossier shall contain all related cyber security documents:

- Detailed SII Inventory list (hardware and software)
- Risk analysis and associated actions
- Risk Assessment Report
- Cyber Security Specification
- PDS/PI Study
- Cyber Security Communication Study
- SII, SIE and DMZ communication study which includes the detailed description of the PDS/PI and DMZ communication mechanisms (architecture drawing and list of source/destination/services & ports/function) and firewall configuration rules
- Operating system configuration detailed document (including list of services used, implemented restrictions)

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: 21 of 24

- File system permission description detailed document
- Network configuration detailed document (architecture drawing, list of services used, implemented restrictions)
- IP addressing plan
- Physical/logical protections implemented
- Logical access strategy implemented (ex: password strategy & configuration, etc.)
- Antivirus configuration detailed document
- Antivirus update and running procedures (system side)
- Remote Maintenance and Diagnostic Specific Study
- Back-up and restoration procedures for operating system, network configuration
- Back-up and restoration procedures for Archive and Historical Data
- Back-up and restoration procedures for specific and application software
- Specific Test reports.

These cyber security documents shall be classified as confidential and the distribution list shall be established with Company approval.

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: 22 of 24

Appendix 1

Appendix 1 SII Functions Sensitivity Example

Domain	Main Functions	Systems	Availability	Integrity	Confidentiality	Proof
SII INDUSTRIAL FACILITIES	SAFETY	Safety Instrumented Systems: PSS / ESD /FGS	4	4	1	3
	PROCESS CONTROL	PCS	4	4	1	3
		Human Machine Interface	3	3	1	2
	UNIT CONTROL & SAFETY (PACKAGE)	Machineries	3	3	1	2
		HVAC	4	4	1	2
		Electrical (PDCS)	3	3	1	2
		Custody metering	3	3	1	3
		Analyzer	3	3	1	2
	SUPERVISION & OPTIMISATION	Remote Supervision	1	3	1	3
		Full control of well (FCW)	2	3	2	2
	HISTORICAL DATA BASE	PDS/PI (database)	2	2	2	1
		Vibration analysis system	1	1	1	1
		Administration / Diagnostic	2	3	1	2
	ENGINEERING / MAINTENANCE	Configuration	1	4	1	4

Availability: Threat (Non-availability within the required time, for the execution of an operation)

Integrity: Threat (Incorrect or illicit Modifications)

Confidentiality: Threat (Disclosure or Loss)

Proof (Traceability): Threat (Impossibility to check or prove the quality of an information item or procession operation)

4 VITAL Unacceptable Risk - extremely serious damage which may lead the entity to stop business or operations

3 VERY SERIOUS Critical risk - very serious damage but business or operation can go on

2 SERIOUS High risk - serious damage impacting entity operations, competitiveness or image

1 NOT SIGNIFICANT Low risk - no significant damage on entity operations, competitiveness or image

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: 23 of 24

Appendix 2

Appendix 2 Third Party Remote Access

Domain	Main Systems	Sub Systems	Type 1 Third Party Remote Maintenance (Data Collection)	Type 2 Third Party Remote Diagnostic (Trouble shooting)
E&P Affiliate Industrial Facilities	Safety Systems	Safety Instrumented Systems PSS / ESD / F&G/HIPS	Not Allowed	Not Allowed
	Process Control Systems	PCS	Allowed	Allowed
	Packages P3	General Package P3 e.g. Machinery	Allowed	Allowed
		HVAC	Allowed	Not Allowed
		Electrical PDCS	Allowed	Not Allowed
		Analyzer	Allowed	Not Allowed
		Off Loading Systems	Allowed	Not Allowed
		Vibration Analysis System	Allowed	Allowed
		Custody metering	Allowed	Not Allowed
		Subsea Control System	Allowed	Not Allowed
	Package P4	Monitoring Systems (e.g. Erosion, Corrosion, Well)	Allowed	Allowed
	Optimization	FCW / OCWR	Allowed	Not Allowed
	Historical Data	Production data (PDS/PI)	Allowed	Allowed

Example - Remote Access - Architectural diagram (Type 1b, no PDS/PI)

