



Document No.	GP 30-60
Applicability	Group
Date	7 April 2009

GP 30-60

Automation Systems Digital Security and Integrity

Group Practice

**BP GROUP
ENGINEERING TECHNICAL PRACTICES**

Foreword

This issue of Engineering Technical Practice (ETP) GP 30-60 and has been renamed “Automation Systems Digital Security and Integrity” from “Process Control Networks”.

This issue includes the following significant changes:

1. Renaming of the ETP from ‘Process Control Networks’ to ‘Automation Systems Digital Security and Integrity’.
2. Complete restructuring, rewrite, and inclusion of extensive new content.
3. In conjunction with GP 59-05, replaces digital security requirement documents formerly found on the IT&S Cybersafe PCDS website.

Because this is a complete rewrite, revisions have not been indicated in the margin as is normal practice.

Copyright © 2009 BP International Ltd. All rights reserved.

This document and any data or information generated from its use are classified, as a minimum, BP Internal. Distribution is intended for BP authorized recipients only. The information contained in this document is subject to the terms and conditions of the agreement or contract under which this document was supplied to the recipient's organization. None of the information contained in this document shall be disclosed outside the recipient's own organization, unless the terms of such agreement or contract expressly allow, or unless disclosure is required by law.

In the event of a conflict between this document and a relevant law or regulation, the relevant law or regulation shall be followed. If the document creates a higher obligation, it shall be followed as long as this also achieves full compliance with the law or regulation.



Table of Contents

	Page
Foreword	2
1. Scope	5
2. Normative references.....	5
3. Terms and definitions.....	6
4. Symbols and abbreviations.....	8
5. Digital security: Hazard evaluation, risk assessment, and management	11
6. People	12
6.1. Training and competency assessment.....	12
6.2. Organisational capability and accountabilities	12
7. System design	13
7.1. General.....	13
7.2. Network tier definitions.....	13
7.3. Network segregation	16
7.4. Device redundancy	18
7.5. Physical and logical security	21
7.6. Remote access solutions	24
7.7. Wireless networks.....	25
8. Operational and maintenance requirements	29
8.1. Overarching DS philosophy and manual.....	29
8.2. Provision of ongoing digital security protection.....	29
8.3. Business continuity planning	31
8.4. Compliance health check.....	33
8.5. Management of change	34
8.6. Network management.....	34
8.7. Software backup	37
9. Project delivery requirements.....	38
9.1. General.....	38
9.2. Factory and site acceptance testing.....	39
9.3. Automation system component digital security qualification	39
10. Documentation.....	39
10.1. Project deliverables.....	39
10.2. Operations	40
Annex A (Informative) Interface protocol usage	41
Annex B (Informative) Example firewall rule base	43
Bibliography	44



List of Tables

Table 1 - Environment classes	23
Table 2 - Protection methods for environment classes	23
Table 3 - Usage classes for wireless instrumentation.....	26
Table 4 - Digital security compliance health check categories.....	33
Table 5 - Application business classifications.....	34

List of Figures

Figure 1 - Example of three tier automation system segregation.....	13
Figure 2 - System component location determination flowchart.....	20
Figure 3 - Remote user access to automation systems.....	25
Figure 4 - Wireless instrumentation: Serial connectivity to PCN/aPCN or PIN.....	28
Figure 5 - Wireless instrumentation: IP connectivity to PCN/aPCN or PIN	28
Figure 6 - PIN and PCN/aPCN antivirus updating methodology	30



1. Scope

- a. This GP provides overarching digital security and integrity requirements for design, testing, installation, commissioning, maintenance, and operation of network infrastructure supporting automation systems that are standalone or connected to external information technology (IT) systems.
- b. Specifically, this GP:
 1. Defines accountabilities and organisational capability requirements to properly specify, design, implement, and support automation system digital security and integrity expectations across BP group.
 2. Defines a set of minimum system design requirements for network segregation and redundancy.
 3. Details project delivery and operational maintenance requirements.
- c. This GP is applicable to wholly owned BP facilities and/or BP operated facilities and is highly recommended for joint venture (JV) facilities.
- d. This GP does not apply to IT infrastructure that supports “office systems” owned and managed by BP IT&S (e.g., internet gateways, passport servers, mega data centres, office wireless, MIS applications, and other business software systems).

2. Normative references

The following referenced documents may, to the extent specified in subsequent clauses and normative annexes, be required for full compliance with this GP:

- For dated references, only the edition cited applies.
- For undated references, the latest edition (including any amendments) applies.

BP

GDP 5.0-0001	Integrity Management.
GP 59-45	Field Wireless Network Design.
GP 59-64	Industrial Wireless Local Area Network and Wireless Voice Over IP Systems.
GRP STD 01	Integrity Management.
GRP STD 004	Digital Security.

Institute of Electrical and Electronics Engineers (IEEE)

IEEE 802.11	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
IEEE 802.15.4	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).
IEEE 802.16	Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems.



3. Terms and definitions

For the purposes of this GP, the following terms and definitions apply:

Advanced control

Multivariable control that provides closed loop optimisation against an objective function, usually sitting above the regulatory control layer.

Automation system

The collective term for system and legacy system types (integrated control and safety system [ICSS], supervisory control and data acquisition [SCADA], distributed control system [DCS], process automation system [PAS], process control system [PCS], process shutdown [PSD], emergency shutdown system [ESD], safety instrumented system [SIS], fire and gas [F&G], etc.) that perform safety, control, and/or monitoring functions on process facilities and may reside on or across process control networks (PCNs), process information networks (PINs), or similar systems below and segregated from business IT systems.

Bandwidth

Data/communications transmission capacity.

Common operating environment (COE)

BP standardised, common IT&S selection of hardware, application software, operating systems, and infrastructure referred to as the passport network.

Demilitarised zone (DMZ)

A demarcation zone or perimeter network that provides a physical or logical protection from critical systems to larger, untrusted networks, such as the internet. The intent of a DMZ is to prevent direct end to end connection between networks of differing security levels.

Encryption

Transformation of data, for the purpose of privacy, into a format that is unreadable until reformatted with a decryption key.

Entity or BP entity

An organisational unit within BP which may be a Performance Unit, Business Unit, Strategic Performance Unit, Segment or some logical subgroup of one of these, defined by the Segment, Function or Region.

Firewall

A functional unit that acts as an interface between a private, internal network (e.g., a BP facility network) and an external network (e.g., the internet). Firewalls filter (block and allow) traffic between networks to protect the private network from electronic intrusion and attack that originates from the external network.

Hypertext transfer protocol (HTTP)

Protocol used by web servers and client browsers to communicate and move documents on the internet.

Hypertext transfer protocol secure (HTTPS)

HTTP combined with a network security protocol.



Internet protocol (IP)

A standard protocol used with the internet that works with TCP protocol to allow communication between computers over networks. IP is the protocol responsible for moving packets of data between nodes and acts as an intermediary between the higher protocol layers and the physical network. Refer to TCP/IP.

Integrated control and safety system (ICSS)

An automaton system that provides a fully integrated (in terms of data transfer and connectivity though not necessarily in functionality or in geography) human machine interface (HMI), control, safety, historian, etc., functionality.

Local area network (LAN)

Data communications network within a defined geographical boundary, typically within a building or campus, to link computers and peripheral devices under some form of standard control.

Main automation contractor (MAC)

An organisation that provides automation equipment, management, and engineering services to a project and then subsequently ongoing engineering support and healthcare to the respective operating facility.

Object linking and embedding (OLE) for process control (OPC)

An open connectivity standard for interoperability in automation.

Packet

Unit (or set) of digital data organised in a specific way for electronic transmission.

Process control system (PCS)

Industrial control systems that reside on a PCN and usually consist of DCS, safety, or SCADA equipment.

Protocol

Specific set of rules for organising transmission of data in a network.

Router

A device that determines the next network point to which a data packet should be forwarded en-route toward its destination. A router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks to which it is connected. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.

Strong authentication (two factor authentication)

Method to fortify network access that requires two methods for authenticating users. For example, the use of two of the following: a physical token, a password, or a biometric. Typically, two factor authentication refers to the use of a token and a password.

Transmission control protocol/internet protocol (TCP/IP)

Standard set of protocols used on the internet for transferring information over networks between computers, handsets, and other devices. TCP is the protocol responsible for verifying delivery of packets moved through IP.

Wide area network (WAN)

Data communications network that connects geographically dispersed sites.



WiMax

A wireless digital communications system, also known as IEEE 802.16, which is intended for wireless “metropolitan area networks”.

4. Symbols and abbreviations

For the purpose of this GP, the following symbols and abbreviations apply:

aPCN	Auxiliary process control network.
ARP	Address resolution protocol.
ATM	Asynchronous transfer mode.
C&I	Control and instrumentation.
CCR	Central control room.
CCTV	Closed circuit television.
CMMS	Computerised maintenance management system.
COE	Common operating environment.
CPU	Central processing unit.
D2D	Data to desktop.
DCOM	Distributed component object model.
DCS	Distributed control system.
DHCP	Dynamic host configuration protocol.
DMZ	Demilitarised zone.
DNP3	Distributed network protocol 3.
DS	Digital security.
DSOP	Digital security operating practices.
DTS	Downhole temperature sensor.
E&P	Exploration and Production.
EA	Engineering authorities.
ESD	Emergency shutdown system.
F&G	Fire and gas.
FAT	Factory acceptance test.
FDS	Functional design specification.



FTE	Fault tolerant ethernet.
FTP	File transfer protocol.
HMI	Human machine interface.
HTTP	Hypertext transfer protocol.
HTTPS	Hypertext transfer protocol secure.
ICCP	Intercontrol centre communications protocol.
ICMP	Internet control message protocol.
ICSS	Integrated control and safety system.
iFAT	Integrated FAT.
IP	Internet protocol.
ISA	International Society of Automation.
ISIS	Integrated surveillance information system.
IT	Information technology.
IWLAN	Industrial wireless LAN.
JV	Joint venture.
LAN	Local area network.
LCN	Local control network.
LER	Local equipment room.
LLDP	Link layer discovery protocol.
MAC	Main automation contractor.
MBOS	Model based operational support.
MMS	Maintenance management system.
MOC	Management of change.
MPLS	Multiprotocol label switching.
MSSP	Managed security service provider.
NAT	Network address translation.
OEM	Original equipment manufacturer.
OLE	Object linking and embedding.
OPC	OLE for process control.



PAS	Process automation system.
PC	Personal computer.
PCS	Process control system.
PCDS	Process control digital security.
PCN	Process control network.
PIN	Process information network.
PLC	Programmable logic controller.
PSD	Process shutdown system.
R&M	Refining and marketing.
RF	Radio frequency
RPM	Remote performance management.
RTU	Remote terminal unit.
SAT	Site acceptance test.
SCADA	Supervisory control and data acquisition.
SETA	Segment engineering technical authority.
SIF	Safety instrumented function.
SIS	Safety instrumented system.
SNMP	Simple network management protocol.
SONET	Synchronous optical network
SPA	Single point of accountability.
SPU	Strategic performance unit.
TA	Technical authority.
TCP/IP	Transmission control protocol/internet protocol.
TDM	Time division multiplexing.
UDP	User datagram protocol.
USB	Universal serial bus.
uLAN	Utility LAN.
VLAN	Virtual LAN.
VOIP	Voice over IP.



VPN	Virtual private network.
WAN	Wide area network.
WEP	Wired equivalent privacy.
WLAN	Wireless local area network.

5. Digital security: Hazard evaluation, risk assessment, and management

- a. In support of this clause, reference should be made to the GRP STD 01 or GDP 5.0-0001, and GRP STD 004.
- b. Each BP entity shall perform a digital security risk assessment for local automation systems using the current BP process control digital security impact assessment tool, which is available from BP digital security.
- c. The assessment shall be performed prior to commissioning newly installed systems following any significant change or if the external risk environment changes with respect to the site automation systems.
- d. A BP entity should review and revalidate the risk assessment every 3 yr.
- e. The risk assessment and management process shall address all digital security risks and hazards associated with the associated automation technology.
- f. The assessment should be completed by site personnel that are able to decide upon:
 1. Level of business risk associated with a risk scenario.
 2. Consequences associated with a risk scenario.
 3. Remedial actions required to recover from a risk scenario.
- g. Risk assessment and mitigation shall be required throughout the lifecycle management of BP facilities and operations. Information generated from the hazard and risk management processes is used to generate risk registers and identify safety functions, safety critical equipment, and protective systems (e.g., GP 48-03).
- h. Automation systems shall be risk assessed and assigned a criticality according to overall business priorities using criteria that shall include:
 1. Whether the system supports processes that are critical to safety, environmental, and/or commercial aspects of any BP operations.
 2. Whether subsequent business impact of a digital security breach is at a local, regional, or group level, including impact on other digital assets or business processes.
- i. Each identified risk scenario shall have an associated management and recovery plan.
- j. If a digital security scenario is deemed to have a high criticality, according to the risk methodology, the system shall be reported to a digital security officer. With the support of digital security, security risks shall be assessed and appropriate additional security controls identified.
- k. Operations and project engineers that implement, develop, modify, or operate process control and safety systems shall:
 1. Ensure that systems, regardless of their assessed criticality, as a minimum, comply with the digital security requirements detailed in this GP.
 2. Apply additional security controls or requirements identified in accordance with the risk assessment.



Note that GRP STD 004 provides additional detail regarding accountabilities, risk identification process, and the application of digital security operating practices.

GRP STD 01 and segment guides provide additional details about hazard evaluation and risk management.

People

6.1. Training and competency assessment

- a. BP and non-BP staff associated with the design, implementation, commissioning, and maintenance of the automation system shall be trained on associated aspects of digital security and integrity.
- b. Staff shall receive appropriate training to cover digital security and integrity aspects of automation system design and maintenance relevant to the asset(s) they support.
- c. Training may be provided by the OEM, MAC, BP digital security, and/or approved third party specialising in digital security.
- d. Training requirements should be specified by asset digital security SPA in conjunction with the OEM, MAC, and/or approved third party specialising in digital security.
- e. SPAs and other key technical staff responsible for supporting automation systems should be formally competency assessed in automation system digital security and integrity. Results and training development plans should be recorded.
- f. Users of automation systems should be provided with basic system security awareness and training materials before access authorisation to the system is granted. For the PCN environment, this shall include control system specific information security awareness and training for specific PCN applications.
- g. Each BP entity should identify, document, and train personnel with significant automation roles and responsibilities in the design and maintenance of their networks.

6.2. Organisational capability and accountabilities

- a. Each major project and brownfield entity shall have an SPA for the digital security and integrity of the automation system.
- b. For E&P assets, the SPA shall be the asset C&I TA. For assets that do not have a designated C&I TA, the lead C&I engineer covering the asset shall act as SPA.
- c. For R&M sites, the SPA shall be a designated lead C&I engineer.
- d. Project C&I lead engineer shall have responsibility for the following until automation system handover to operations:
 1. System design, testing, and commissioning to meet minimum digital security and integrity requirements, as defined in this GP.
 2. System digital security and integrity 'as built' documentation for handover to operations.
 3. Associated digital security system management procedures.
 4. Training for designated operations staff in all 'as built' aspects of digital security relating to the automation system.
- e. The BP entity C&I lead engineer/TA shall have responsibility for system maintenance and development to maintain minimum digital security and integrity requirements as defined by this GP.
- f. The BP entity C&I lead engineer/TA may delegate the maintenance and/or development of the automation system network e.g., to IT&S or an approved third party support company, but shall retain overall responsibility for the system health and integrity.



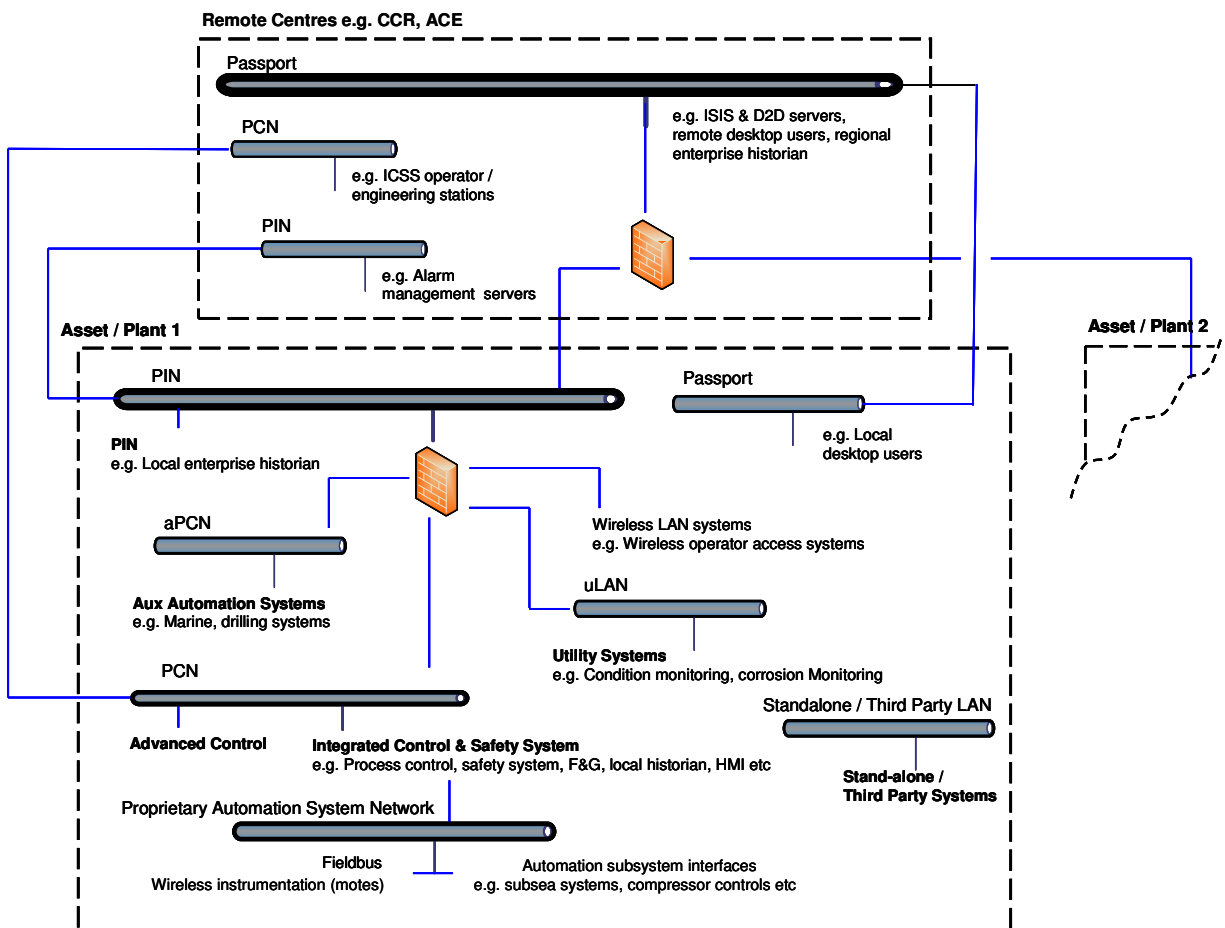
- g. The SPU C&I TA or SPU lead C&I engineer, or equivalent, shall have overall responsibility for automation system digital security and integrity across the entity.
- h. Any expansion (or reduction) of the automation system, including the addition or removal of connected devices, shall be subject to approval by the BP entity C&I lead engineer/TA.

7. System design

7.1. General

- a. System design aspects described in this clause are based on industry best practice, which attempts to minimise automation system security risks while meeting safety and control of the respective facility or plant.
- b. If connecting an automation system to external IT networks, a three tier architecture (e.g., PCN/aPCN <-> PIN/uLAN <-> Passport) shall be adopted. Figure 1 depicts an example of an automation network that complies with the three tier segregation model.

Figure 1 - Example of three tier automation system segregation



7.2. Network tier definitions

7.2.1. General

A BP entity may have one or more of the network tiers (7.2.2 through 7.2.10) in place, depending on automation function and complexity.

7.2.2. Proprietary automation system networks

Automation systems components sourced from the same vendor may be connected via a proprietary network.

7.2.3. PCN

- a. The PCN typically hosts the “mission critical” process control, safety, and data acquisition and visualisation systems.
- b. PCN devices and infrastructure are generally supported by either local process control/system engineers or automation vendor.
- c. Typical devices found on a PCN include:
 1. Process controllers.
 2. Safety logic solvers.
 3. PLCs.
 4. RTUs.
 5. Advanced control servers.
 6. Operator and engineer HMI workstations.
 7. Local historians.
 8. Alarm handling systems.
 9. Sequence of events recorders.
 10. Metering systems (if deemed “mission critical”).

7.2.4. aPCN

- a. An auxiliary process control network is a PCN dedicated to supporting “mission critical” process control and safety systems for a particular function or operation.
- b. aPCN devices and infrastructure are generally supported by either local process control/system engineers or automation vendor.
- c. Typical systems that could have a dedicated aPCN include:
 1. Drilling process control and safety systems.
 2. Subsea control and safety systems.
 3. Remote well pad control and safety systems.
 4. Marine control and safety systems.
 5. Guidance radar systems.

7.2.5. PIN

- a. A process information network is generally used to host systems that need to communicate to the PCN and/or aPCN and the passport network. Some other systems may be located in the PIN to enable tighter firewall rule bases to be defined. Examples include:
 1. Placing an antivirus repository on the production PIN.
 2. Locating an additional server that facilitates OPC communication.
- b. PIN devices and infrastructure are generally supported by local process control/system engineers, local IT&S personnel, or approved third parties.

