Report: M 2784 - X-10

Published by WIB, Second issue, October-2010

Index Classification 50.1- version: 2.0

PROCESS CONTROL DOMAIN-
SECURITY REQUIREMENTS FOR VENDORS

WIB working group: Plant security

INTERNATIONAL INSTRUMENT USERS' ASSOCIATIONS - EWE
EVALUATION INTERNATIONAL (EI) / WIB / EXERA

EVALUATION INTERNATIONAL (EI) / WIB / EXERA

CIRCULATION

This report has been produced for the in-house use of EI, WIB and EXERA (EWE) members. The contents ofthe report must not be divulged by them to persons not employed by EWE member companies without theexpress consent of the issuing organisation.

This report must not be used for commerical or promotional purposes.

ABOUT EWE (EI, WIB and EXERA)

EI, -WIB and EXERA are international instrument users' associations who collaborate in the sponsoring,planning and organisation of instrument evaluation programs. They have the long term objective ofencouraging improvements in the design, construction, performance and reliability of instrumentation andrelated equipment.

The evaluation of the selected instruments is undertaken by approved. independent and impartial laboratorieswith respect to the manufacturers' performance specifications and to relevant International and Nationalstandards.

Each evaluation report describes the assessment of the instrument concerned and the results of the testing. Noapproval or certification is intended or given. It is left to the reader to determine whether the instrument issuitable for its intended application- Reports are circulated throughout the entire membership of the EWEAssociations.

EI-Evaluation International, The International Instrument Users' Association
East Malling Enterprise Centre
New Road, East Malling , Kent
United Kingdom ME19 6BJ

International Instrument Users' Association -WIB
Prinsessegracht 26
2514 AP, The Hague.
The Netherlands

EXERA Association des Exploitants d'Equipements de Mesure, de Regulation et d'Automatisme.
4 Cité d'Hauteville,
75010 Paris
France

Disclaimer:
Every effort is made to provide accurate information in this document. However WIB, nor any of its members, makes any warranty of any kind about the quality or correctness of the information included in this document. WIB will not be liable for any damages of any kind arising from the use of this document.

Comments sent by E-mail:
You are invited to provide us with your personal comments or questions in an E-mail, directed to manager@wib.nl. We will use this information to improve the content of this document.

International Instrument Users' Associations

EWE Membership List

March 2010

Acetex Chimie
Adisseo
Aeroport de Paris
Agence de L'Eau Artois Picardie
Air Liquide
AkzoNobel T&E
Aramco Overseas Company BV
AREVA
Arkema
AWE
Axens
BAE Systems
BP PLC
BP Refinery Rotterdam BV
British Energy plc
CETIAT
Chiyoda Corporation
C&Tsi
DCNS
DGA
DOW Benelux
DSM BV
Du Pont de Nemours BV
EADS/AIRBUS
EDF
ENEL Generazione
EniACQUA CAMPANIA
ExxonMobil USA
GDF
Health & Safety Executive
Heineken SCS
IGR
INEOS
INERIS
INRS
Intertek Polychemlab
IRA
KEMA Nederland BV
Kuwait Petroleum Europoort BV
Laborelec
Lanxess
LNE
Lubrizol France
Lyondell Basell
Magnox Electric Ltd
M+W Process Automation
Nantes Metropole – Direction de l'Eau
Nederlands Meetinstituut-NMi
NPL Management Ltd
Petro SA
Polimeri Europa
RATP
Renault SA
RHODIA
Rolls-Royce Submarines
SABIC
SANOFI PASTEUR
Schering-Plough Corp.
Sellafield Ltd
Shell Global Solutions International BV
ShinEtsu-PVC BV
Sicilaque
SIP Standardiserad Instrumentprovning
Solvay SA
Suez Environnement
Total
Università di Genova
Università di Pisa
Urenco ChemPlants-Ltd
Véolia eau
Waternet
Wintershall Noordzee BV

TABLE OF CONTENTS

APPENDICES

1. INTRODUCTION

1.1 SCOPE

This document specifies requirements and gives recommendations for IT security to be fulfilled by vendors of process control & automation systems to be used in Process Control Domains (PCDs).

This covers both policy; addressing the Vendor's organization, IT security processes, technological solutions and governance of IT security. When a Vendor's solution complies with this set of requirements, the solution is considered by the WIB to be PCD Security Compatible.

An 'End User' or 'the Principal' shall comply with its own security policies, standards and specifications for the PCD and this can vary for each Principal. This requirements documentis a subset of aPrincipal's security policies, standards and specifications for the PCD, containing the common requirements of all Principals into one set of minimum requirements for Vendors to comply with.

PCD Security Compatible solutions contribute in attaining this compliancy, but must be supplemented with additional security controls; e.g. adequate work procedures, skills & competencies of staff, remote access via a Process Control Access Domain (PCAD), governance and management of the PCAD and PCD. An asset is considered to be PCD Security Compliant when it fulfills all of these requirements, or has documented variances to these requirements approved by the Principal's management.

Prior to procurement, the Principal shall ensure that control & automation solutions tendered to Principal are fully PCD Security Compatible. Vendors are required to document and inform the Principal of any deviation their solutions may have from the requirements in this document. The Principal may require demonstration of the solution at the Vendor's premises or in a WIB approved laboratory as part of the process of verifying that a solution is PCD Security Compatible.

Supplementing to this document, a suite of 'End-user' specific Design and Engineering Specifications and/or Guidelines could provide more guidance on how to produce a PCD Security Compatible solution.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by WIB, the distribution of this requirements document is confined to WIB Members and their Contractors and Manufacturers/Suppliers (existing or potential).

This requirements document is intended for use in, but not limited to, oil refineries, chemical plants, gas plants, exploration and production facilities, pharmaceutical facilities, water industry, and energy and supply/distribution installations including smart grid.

When this document is applied, a Management of Change (MOC) process should be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this requirements document, the Vendor shall determine by careful scrutiny, which of the requirements are the more stringent and which combination of requirements will be acceptable with regard to the safety, environmental, economic and legal aspects. In all cases the Vendor shall inform the Principal of any deviation from the requirements of this requirements document, which is considered to be necessary in order to comply with national and/or local laws and/or regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this requirements document as closely as possible.

1.3 DEFINITIONS*AND* ABBREVIATIONS

GENERAL DEFINITIONS

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

A **Vendor** is a company that supplies or intends to supply the Principal with equipment, or commissioning/maintenance services associated with equipment, located on PCD network levels L3, L2 or L1 and having TCP/IP networking protocols enabled.

The **Principal** is the party that initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

When '**its systems'** is used in this document, this refers to all systems supplied and supported by Vendor over the systems lifecycle.

A **system** is a combination of hardware and software components, which together provides a function or service.

A Vendor is **compatible** to Principal's security policy and standards, when Vendor is **compliant** to this industry standard. The Vendor cannot be compliant to Principal's policy and security standards, because part of this should be realised by the Principal.

A **network device** is equipment that connects or manages network traffic; e.g. switches, routers and firewalls.

A **Delegated Technical Authority** is a person who has received delegated authority from the Principal to approve Derogations from the Process Safety requirements.

A **Derogation** is an authorised variance or exemption from a Process Safety requirement, with specified conditions.

Process Safety is the management ofhazards that can give rise to major accidents involving, personnel safety, the release of potentially dangerous materials, and release of energy (such as fire or explosion) or both. The word **SHALL [PS]** indicates a Process Safety requirement.

In this document, **IT security** is equivalent to Process Control System Cyber Security, and Process Control System Cyber Security Controls.

Note: Derogations from these requirements SHALL [PS] be approved by WIB

The word **shall** indicate a 'must comply requirement'.

The word **should** indicate a 'strong recommendation'.

ABBREVIATIONS

ACL	Access Control List
AES	Advanced Encryption System
API	American Petroleum Institute
ASD	Automation System Domain
AV	Aniti-Virus
BP	Base Practice
BR	Base Requirement
CIP	Critical Infrastructure Program
CSAD	Control System Access Domain
CSN	Control System Network
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DoS	Denial of Service
FAT	Factory Acceptance Testing
FIPS	Federal Information Processing Standard
HIDS	Host-based Intrusion Detection System
HMI	Human to Machine Interface
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electric and Electronic Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
ISA	International Society for Automation
ISO	International Standards Organization
L1	Network Level 1 - Basic Control System
L2	Network Level 2 - Area Supervisory Control
L3	Network Level 3 – Site Manufacturing Operations Layer Note: Equivalent to the Control System Network (CSN)
L4	Network Level 4 – Site Business Planning Note: Equivalent to the Office Domain (OD)
L5	Network Level 5 - Enterprise

M	Mandatory
MIB	Management Information Base
MoC	Management of Change
MRE	Minimum Required Evidence
NIST	National Institute Of Science and Technology
NTFS	New Technology File System
NTP	Network Time Protocol
O	Optional
OAGi	Open Applications Group industry
OD	Office Domain
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PA	Process Area
PAS	Process Automation System (ICS, DCS, PLC, etc.)
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCN	Process Control Network
PCS	Process Control System
PLC	Programmable Logic Controller
PtW	Permit to Work
Q&A	Question and Answer
RDP	Remote Desktop Protocol Note: Used by Microsoft Terminal Services
RE	Requirement Enhancement
RF	Radio Frequency
SAT	System Acceptance Testing
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SNMP	Simple Network Management Protocol
SLA	Service Level Attainment
SP	Special Publication
SSID	Service Set Identifier
T&C	Terms and Conditions
TCP	Transport Control Protocol
TPA	Third Party Access

USB	Universal Serial Bus
VPN	Virtual Private Network
WMI	Windows Management Instrumentation
WPA	Wireless Protected Access (Note: WPA2 has replaced WPA)

1.4 CROSS-REFERENCES

Where cross-references to other parts of this requirements document are made, the referenced section number is shown in brackets. Other documents referenced are listed in *References*.

1.5 PROCESS SAFETY REQUIREMENTS

Below is a summary of the Process Safety requirements in this requirements document, together with the lifecycle phase in which they occur. Derogations from these requirements SHALL [PS] be approved by the Delegated Technical Authority.

Design	**Operation**	**Process Safety risk mitigation**
X		To reduce the risk of unauthorized or inadvertent changes to the SIS configuration
X		To avoid loss of SIS integrity due to the controller stalling as a result of denial of service in communications

2 RECOMMENDATIONS TO THE READER

2.1 WIB REQUIREMENTS

This document specifies requirements and gives recommendations for IT security to be fulfilled by Vendors of control systems and automation systems to be used in Automation System Domains (ASDs). From a Vendor point-of-view, it is important to understand the underlying assumption and context factored into the WIB requirements.

a) Principals will comply with their own security policies, standards and specification for the ASD and this can vary with each Principal. For this reason, the WIB requirements are a unified subset of the Principal's security policies, standards and specification for the ASD. It is this subset of minimum requirements that Vendors must comply with.
b) Vendors are required to document and inform the Principal of any deviation their solutions may have from the WIB requirements. When deviations occur the Principal may require demonstration of the solution at the Vendor's premises or in a WIB approved laboratory as part of the process of verifying that a solution is ASD Security Compatible.
c) Principals are encouraged to supplement the WIB requirements with a suite of 'End-user' specific Design and Engineering Practices, specifications and/or guidelines that could provide more guidance on how to produce a ASD Security Compatible solution.
d) If national or local regulations exist in which some of the requirements may be more stringent than the WIB requirements, the Vendor will determine by careful scrutiny, which of the requirements are the more stringent and which combination of requirements will be acceptable with regard to the safety, environmental, economic and legal aspects. In all cases, the Vendor must inform the Principal of any deviation from the WIB requirements, which is considered necessary in order to comply with national or local laws and//or regulations. The Principal may then negotiate with the national or local authorities concerned to obtain an agreement to follow the WIB requirements as closely as possible.

2.2 PROCUREMENT LANGUAGE

WIBprovides the following sample procument language that Principals may include in their Vendor procurement documents.

> ***[Supplier/Seller/Contractor]*** *shall ensure that effective <Month day, year>all equipment, systems and services delivered having TCP/IP networking protocols enabledwith the purpose or intent to connect to* ***[Purchaser Group/Buyer Group/Company Group]*** *process control domain systems, levels L3, L2, or L1, shall be compliant with all requirements and specifications of the latest revision of TheInternational Instrument Users' Association (WIB) report:*
>
> *WIB Report M 2784 X10, Process Control Domain – Security Requirements for Vendors, 2nd Issue: October 2010, Index Classification 50.1 – v: 2.0 .*
>
> *To demonstrate compliance of the equipment, systems and services,* ***[Supplier/Seller/Contractor]****shall provide to* ***[Purchaser/Buyer/Company],*** *on acceptance of orderat no cost to* ***[Purchaser/Buyer/Company]****, a Wurldtech Achilles Practices Certificate (APC), level <Bronze> is required , <Silver> is prefered.*

3 INTRODUCTION TO BASE PRACTICES

3.1 GENERAL APPROACH TO BASE PRACTICES

Four Process Areas(PA's) domains are used to separate the basic characteristics of the security engineering process from the management and institutionalization characteristics.

PAs consist of all practices that define security engineering. These practices are called Base Practices (BPs) and are designated Bronze, Silver or Gold to indicate the level of security maturity defined by achieving the Base Practice and appointed Requirement Enhancements.

3.2 PROCESS AREAS

There are 35 defined PAs thatare organized into four logical categories:

- **Organizational PAs** include BP requirements and Requirement Enhancements for policies and procedures.

- **System Capability PAs** include BP requirements and Requirement Enhancements for security functions to be designed into the Vendor's system, and compensating security functions used to protect Vendor system components and subsystems which do not have built-in security capabilities.

- **System Acceptance Testing and Commissioning PAs** include BP requirements and Requirement Enhancements for demonstrating correct implementation of security functions built into the Vendor's system, and readiness of system turnover for operation by the Principal or selected Operator.

- **Maintenance and Support PAs** include BP requirements and Requirement Enhancements for demonstrating correct maintenance of security functions built into the Vendor's system, and timely support in response to security related events.

Table 1 shows the industry agreement that describes the PAs in each category.

Table 1 Logical Categories of PAs

	Process Area Categories	Process Area ID	Process Area Subject
	Organizational Process Areas	PA01	Prepare & Inform Personnel
		PA02	Designate a Security Contact
		PA03	Specify Base Practices
	System Capability Process Areas	PA04	Harden the System
		PA05	Protect from Malicious Code
		PA06	Implement Patch Management
		PA07	Secure Account Management
		PA08	Support Backup/Restore
		PA09	Increase Network Visibility
		PA10	Standardize Historian Interfaces
		PA11	Verify Operations
		PA12	Connect Wirelessly
		PA13	Fortify Safety Instrumented System (SIS) Connectivity
		PA14	Provide Remote Access
		PA15	Protect Data
	System Acceptance Testing & Commissioning Process Areas	PA16	Manage the Deployment
		PA17	Harden the System
		PA18	Protect from Malicious Code
		PA19	Implement Patch Management
		PA20	Secure Account Management
		PA21	Support Backup/Restore
		PA22	Implement the Architecture
		PA23	Connect Wirelessly
		PA24	Provide Remote Access
		PA25	Protect Data
	Maintenance & Support Process Areas	PA26	Manage the Deployment
		PA27	Harden the System
		PA28	Protect from Malicious Code
		PA29	Implement Patch Management
		PA30	Secure Account Management
		PA31	Support Backup/Restore
		PA32	Implement the Architecture
		PA33	Connect Wirelessly
		PA34	Provide Remote Access
		PA35	Protect Data

3.3 BASE PRACTICES

Table 2shows the extended industry agreement that describes the BPs and specific BP objectives associated with each PA.

Table 2 BP Objectives

	Process Area Categories	PA	BP ID	Base Practice Objective
	Organizational Process Areas	PA01: Prepare and Inform Personnel	BP.01.01	Requirement recognition and enforcement
			BP.01.02	Ensure alignment
			BP.01.03	Protect sensitive documentation
			BP.01.04	Background checks
			BP.01.05	Competent personnel
			BP.01.06	Confidentiality and user agreements
		PA02: Designate a Security Contact	BP.02.01	Nominate the role
		PA03: Specify Base Practices	BP.03.01	Standards employed
			BP.03.02	Security certificates
	System Capability Process Areas	PA04: Harden the System	BP.04.01	Document requirements
			BP.04.02	Manage 3rd party software
			BP.04.03	Conduct 3rd party security architecture reviews
			BP.04.04	Declaration of trusted interfaces
			BP.04.05	Strengthen Protocol
		PA05: Protect from Malicious Code	BP.05.01	Support anti-virus software
			BP.05.02	Proper installation instructions
			BP.05.03	Virus-free equipment
		PA06: Implement Patch Management	BP.06.01	Policy documentation
			BP.06.02	Patch qualification
			BP.06.03	Provide patch list
			BP.06.04	Prompt patch notification
			BP.06.05	Audit tools
			BP.06.06	Patching documentation
		PA07: Secure Account Management	BP.07.01	Multiple default passwords
			BP.07.02	Removable default accounts
			BP.07.03	Minimum password strength
			BP.07.04	Password lifetimes and reuse restrictions
			BP.07.05	Persistence of special accounts
			BP.07.06	Role-based access for network devices
			BP.07.07	Unified account management
			BP.07.08	Maintain account logs

	Process Area Categories	PA	BP ID	Base Practice Objective
		PA08: Support Backup/Restore	BP.08.01	Backup documentation
			BP.08.02	Backup process
		PA09: Increase Network Visibility	BP.09.01	Security monitoring protocols
			BP.09.02	Management Information Base
		PA10: Standardize Historian Interfaces	BP.10.01	Historian data collection
			BP.10.02	Data warehouses
			BP.10.03	Log and event management
		PA11: Verify Operations	BP.11.01	Operator acknowledgement
			BP.11.02	Automated Operations
		PA12: Connect Wirelessly	BP.12.01	Approved standards
			BP.12.02	Configuration methods
		PA13: Fortify SIS Connectivity	BP.13.01	Configuration key switch
			BP.13.02	Third-party assessment
			BP.13.03	Communications integrity
			BP.13.04	Layer 3 connections
			BP.13.05	DCS communications
			BP.13.06	SIS EWS
		PA14: Provide Remote Access	BP.14.01	Remote access applications
			BP.14.02	Remote update applications
		PA15: Protect Data	BP.15.01	Protect data at rest
			BP.15.02	Protect data in transit
			BP.15.03	Encryption
	System Acceptance Testing & Commissioning Process Areas	PA16: Manage the Deployment	BP.16.01	Risk assessment
			BP.16.02	Inventory register
			BP.16.03	Temporary account removal
			BP.16.04	Network scan
			BP.16.05	Relevant processes
			BP.16.06	Timely notification
		PA17: Harden the System	BP.17.01	Hardened system demonstration
			BP.17.02	Firewall use
		PA18: Protect from Malicious Code	BP.18.01	Quality definition files
			BP.18.02	General anti-virus policy
			BP.18.03	Portable media procedure
			BP.18.04	Anti-virus management
			BP.18.05	Anti-virus demonstration
		PA19: Implement Patch Management	BP.19.01	Up-to-date systems
		PA20: Secure Account Management	BP.20.01	Individual accounts
			BP.20.02	Default passwords
			BP.20.03	Minimum password strength
			BP.20.04	Password lifetimes and

	Process Area Categories	PA	BP ID	Base Practice Objective
				reuse restrictions
			BP.20.05	Persistence of special accounts
			BP.20.06	Role-based access for network devices
			BP.20.07	Workstation session lock
		PA21: Support Backup/Restore	BP.21.01	Regular backups
			BP.21.02	Backup demonstration
		PA22: Implement the Architecture	BP.22.01	Architecture drawings
			BP.22.02	Network layer separation
			BP.22.03	Time synchronization
		PA23: Connect Wirelessly	BP.23.01	Service Set Identifier (SSID)
			BP.23.02	Wireless device maintenance
			BP.23.03	Safeguarding functions
			BP.23.04	Secure accounts
			BP.23.05	Wireless workers and CSAD
			BP.23.06	Architecture documentation
		PA24: Provide Remote Access	BP.24.01	Remote access documentation
			BP.24.02	Connection approval and review
		PA25: Protect Data	BP.25.01	Protect data at rest
			BP.25.02	Protect data in transit
			BP.25.03	Encryption
			BP.25.04	Encryption key management
			BP.25.05	Digital certificate management
	Maintenance & Support Process Areas	PA26: Manage the Deployment	BP.26.01	Risk assessment
			BP.26.02	Inventory register
			BP.26.03	Temporary account removal
			BP.26.04	Network scan
			BP.26.05	Relevant processes
			BP.26.06	Timely notification
		PA27: Harden the Systems	BP.27.01	Harden system demonstration
			BP.27.02	Firewall use
		PA28: Protect from Malicious Code	BP.28.01	General anti-virus policy
			BP.28.02	Portable media procedure
			BP.28.03	Anti-virus management
		PA29: Implement Patch Management	BP.29.01	Up-to-date systems
		PA30: Secure Account Management	BP.30.01	Individual accounts
			BP.30.02	Minimum password strength
			BP.30.03	Password lifetimes and reuse restrictions

	Process Area Categories	PA	BP ID	Base Practice Objective
			BP.30.04	Persistence of special accounts
			BP.30.05	Role-based access for network devices
			BP.30.06	Workstation session lock
		PA31: Support Backup/Restore	BP.31.01	Regular backups
			BP.31.02	Backup prior to change event
			BP.31.03	Backup demonstration
		PA32: Implement the Architecture	BP.32.01	Architecture drawings
			BP.32.02	Network layer separation
		PA33: Connect Wirelessly	BP.33.01	Service set identifier (SSID)
			BP.33.02	Wireless device maintenance
			BP.33.03	Safeguarding functions
			BP.33.04	Secure accounts
			BP.33.05	Wireless workers and CSAD
			BP.33.06	Architecture documentation
		PA34: Provide Remote Access	BP.34.01	Remote access documentation
			BP.34.02	Connection approval and review
		PA35: Protect Data	BP.35.01	Protect data at rest
			BP.35.02	Protect data in transit
			BP.35.03	Encryption
			BP.35.04	Encryption key management
			BP.35.05	Digital certificate management

3.3.1 BP REQUIREMENTS: ORGANIZATIONAL PAs

There areBase Requirements (BRs) and Requirement Enhancements (REs) for each BP that isassociated with an organizational PA. A BR and RE can be mandatory or strongly recommended. Table 3lists the requirements.

Table 3 BP Requirements: Organizational PAs

	Process Area	Base Practice Objective	Requirements	Level
	PA01: Prepare and Inform Personnel	BP.01.01: Requirement recognition and enforcement	BR: The Vendor shall ensure that personnel within its organization, subcontractors, and consultants who are assigned to activities of the Principal have been informed that the Vendor Base Practices (this document) contains mandatory requirements for all services or deliverables to the Principal. Note: Terms and Conditions (T&C) for subcontractor and consultant contracts and purchase orders should include a requirement to adhere to the WIB standards and practices.	Bronze
			RE(1): Vendor representatives shall enforce the control system security procedures specified in this document and the Vendor's applicable security policies during engagement in activities on the Principal's site.	Silver
			RE(2): The Vendor shall have policies and procedures to support an incident response team led by the Principal.	Silver
			RE(3): The Vendor shall ensure that personnel within its organization, subcontractors, and consultants acknowledge and comply with security policies enforced by the Principal.	Gold
		BP.01.02: Ensure alignment	BR: The Vendor shall, within its organization, practice and maintain policies, standards and procedures which are compliant with the requirements specified in this document. Note: Alignment is only required for Vendor organizational components which are directly involved in the processes/practices that pertain to the product/services subject to this document.	Bronze
			RE(1): The Vendor shall enforce with its subcontractors and consultants policies, standards and procedures which are compliant with the requirements specified in this document.	Gold
		BP.01.03: Protect sensitive documentation	BR: The Vendor shall not publish descriptions of the Principal's Control System Domain (CSD) systems or architecture as publicly available sources of information without prior risk assessment and approval by the Principal.	Bronze
			RE(1): The Vendor shall enforce with its subcontractors and consultants adherence to all policies and procedures required to protect sensitive documentation.	Gold
		BP.01.04: Background checks	BR: The Vendor should conduct security-related background checks on personnel before they are assigned to projects for the Principal; e.g., identity verification and criminal record check.	Silver
			RE(1): The Vendor shall enforce with its subcontractors and consultants adherence to all policies and procedures required to performing	Gold

	Process Area	Base Practice Objective	Requirements	Level
			security-related background checks.	
		BP.01.05: Competent personnel	BR: The Vendor shall ensure that competent security leads are assigned to the Principal's projects.	Bronze
			RE(1): The Vendor shall enforce with its subcontractors and consultants adherence to all security policies and procedures.	Gold
		BP.01.06: Confidentiality and user agreements	BR: Confidentiality and user agreements (following applicable standards and procedures) shall be signed by all persons having access to the Principal's ASD.	Bronze
	PA02: Designate a Security Contact	BP.02.01: Nominate the role	BR: The Vendor shall nominate a Control System Security Focal Point in its organization who is responsible and accountable for the following activities. a. Acting as liaison with the Principal, as appropriate, about compliance of the Vendor's system with this document. b. Communicating the Vendor's point-of-view on control system security to the Principal's staff. c. Ensuring that tenders to the Principal are aligned and in compliance with both this document and the Vendor's internal requirements for control system security. d. Communicating deviations from, or other issues not conforming with, the this document to the Principal's organization requesting the tender. Note: The evidence requirement in the Vendor Submittal only requires that a control system security focal point be designated.	Bronze
			RE(1): Providing the Principal with timely information about cyber security vulnerabilities in the Vendor's supplied systems and services.	Bronze
			RE(2): Providing timely support and advice to the Principal in the event of cyber security incidents involving the Vendor's systems or services.	Silver
	PA03: Specify Base Practices	BP.03.01: Standards employed	BR: The Vendor shall provide a list of membership and level of membership participation in recognized security standards development working groups or other process control security initiatives. Note: ICSJWG is an example of a PCS security initiative.	Bronze
			RE(1): The Vendor shall participate in at least one standard workgroup activity. Note: Participation may be enabled as a corresponding member, but the participation should be active, not passive.	Silver
		BP.03.02: Security certificates	BR: The Vendor should obtain control security certificates (e.g., Wurldtech Security Technologies' Achilles Communications Certification) and shall inform the Principal of any such certificates. Note: Communications certification by a reputable company is only one example.	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			RE(1): The Vendor should obtain from its subcontractors and consultants control security certificates and shall inform the Principal of any such certificates.	Gold

3.3.2 BP REQUIREMENTS: SYSTEM CAPABILITY PAs

System capability PAs include process requirements and functional requirements. Process requirements ensure that real evidence, in document form, is used to verify compliance with the requirement. Functional requirements ensure that real evidence, in the form of measurements or quantitative analysis based on unit testing and Factory Acceptance Testing, is used to verify compliance with the requirement.

There are BRs and REs for each BP that is associated with a system capability PA. A BR and RE can be mandatory or strongly recommended. Table 4 lists the requirements.

Note: Unit testing and Factory Acceptance Testing (FAT) are performed by the Vendor at the Vendor's site. Unit tests are usually performed in accordance with an Engineering test script and the results are documented in an Engineering report. Successful completion of unit tests is the basis for engineering to declare the Vendor's system ready for formal FAT. It is assumed that FAT is performed in accordance with predefined/approved procedures and acceptance criteria. Furthermore, FAT tests are witnessed by Quality Assurance representatives from the Vendor and Principal who sign-off and certify that the test is completed satisfactorily. Satisfactory completion of all FAT tests results in the readiness to ship the Vendor's system to the Principal for System Acceptance Testing and Commissioning. Readiness to ship is the milestone which completes FAT defines the "as-built" Vendor system.

Table 4 BP Requirements: System Capability PAs

	Process Area	Base Practice Objective	Requirements	Level
■	PA04: Harden the System	BP.04.01: Document requirements	BR: The Vendor shall document the hardening requirements for its system in a distributable hardening guide, which includes at least the following: a. Removal or non-installation of software and functionality that is not required by the Principal, nor for the intended functional purpose of the system; email, office applications, games, USB ports, Bluetooth and Wi-Fi communications, etc. b. Protection of physical and logical access to diagnostic and configuration ports. c. Disabling all unused ports on switches and routers to assist in preventing unauthorized access to the ASD network infrastructure. d. Proper maintenance processes to maintain the system-hardened state during the system lifetime.	Bronze
■			RE(1): The Vendor shall document data flows and storage points with identification of sensitive information. Note: Requirements for sensitive information should be approved by the Principal.	Silver
■			RE(2): The Vendor shall document the segmentation architecture between the control system domain and other domains; e.g., separation between the development domain and the control system domain. Note: Separation between domains will be vetted by 3rd party security architecture reviews required by BP.04.03 supported by BP.22.01.	Silver

	Process Area	Base Practice Objective	Requirements	Level
■			RE(3): The Vendor shall document the data retention capability provided by the Vendor's system including data pruning functions, retention timeouts, data purging, etc.	Silver
■			RE(4): The Vendor shall document the formatting of security extensions provided for servers used in the Vendor's system. Note: Formatting security extensions as strong as New Technology File System (NTFS) are desired; e.g., access control lists and files system journaling.	Silver
■		BP.04.02: Manage 3rd party software	BR: The Vendor shall have policies and procedures for security testing and approval and maintenance policies and procedures for 3rd party software integrated in the Vendor's system. Note: The evidence requirement is to have policies and procedures in place. Bronze level requirements do not address the effectiveness of the implementation of those policies and procedures.	Bronze
■		BP.04.03: Conduct 3rd party security architecture reviews	BR: The Vendor shall have policies and procedures for 3rd party security architecture reviews including security risk assessments.	Bronze
■			RE(1):The Vendor shall have policies and procedures to ensure that only those ports and services required for normal and emergency operations are enabled. Note: Listing the enabled status of ports and services required for normal and emergency operations is needed for effective firewalling.	Silver
■		BP.04.04: Declaration of trusted interfaces	BR: The Principal shall have policies and procedures for declaring external interfaces to the Vendor's system as trusted or untrusted. Note: The declaration of trust is needed to establish the requirements for compensating security mechanisms – see BP.04.04RE(1).	Bronze
■			RE(1): For interfaces declared to be untrusted, the Vendor's system shall incorporate compensating security mechanisms to protect the control system.	Bronze
■		BP.04.05: Strengthen protocol	BR: The Vendor shall document special mechanisms and procedures needed to minimize recognized security weaknesses inherent in communication protocols. Note: Function codes used to execute programs or state changes should be given special attention.	Bronze
■	BronPA05: Protect from Malicious Code	BP.05.01: Support anti-virus software	BR: The Vendor's system shall support use of anti-virus software. Note 1: Symantec or McAfee anti-virus solutions are preferred. Note 2: If not applicable, the Vendor should state the reason it is not applicable and address the requirement stated in BP.05.01 RE(1).	Bronze

	Process Area	Base Practice Objective	Requirements	Level
■			RE(1): Components for which the installation of anti-virus software is not technically possible shall be listed and other mitigating controls shall be documented and implemented to reduce the risk of infection.	Bronze
■		BP.05.02: Proper installation instructions	BR: The Vendor shall provide the Principal with documented instructions for the proper installation, configuration and update of anti-virus software.	Bronze
■		BP.05.03: Virus-free equipment	BR: The Vendor shall provide evidence that all equipment has been checked to be free of malicious code prior to shipment to the Principal.	Silver
■	PA06: Implement Patch Management	BP.06.01: Policy documentation	BR: The Vendor shall provide documentation describing the software patching policy for its system.	Bronze
■			RE(1): The Vendor shall review its patching policy at least annually to address new threats and vulnerabilities.	Bronze
■			RE(2): The Vendor shall include in their patching policy controls to ensure that patching does not reinstall software that has been removed for hardening purposes, or change system configuration settings. Note: Vendor needs to describe the process/tools used to verify that patching does not reinstall software that has been removed, or that system configuration settings have not been changed.	Silver
■		BP.06.02: Patch qualification	BR: The Vendor shall qualify all relevant software patches and service packs for use on its system during its supported lifetime including security patches that are released by the manufacturer of the operating system and third party software used on their system. Note: Patch testing and qualification, and more importantly deploying necessary patches should follow the guidelines offered in ISA-99.02.03.	Bronze
■			RE(1): If a security patch is considered not relevant by the Vendor for use on its system, the reason shall be provided to the Principal.	Bronze
■			RE(2): If a security patch is not approved by the Vendor for use on its system, then the reason and remediation plan shall be provided to the Principal. The remediation plan shall describe how a solution will be provided within 12 months.	Bronze
■		BP.06.03: Provide patch list	BR: The Vendor shall maintain and provide secure access to a list of software patches and service packs relevant to its system including the approval status of each; i.e., approved, not approved, in test.	Bronze
■			RE(1): For Microsoft software, the Vendor's on-line patch list shall be in a standardized downloadable format, preferably compatible with Microsoft Windows Update Services (WSUS) or	Silver

	Process Area	Base Practice Objective	Requirements	Level
			equivalent. Note: WSUS is not a requirement per se, it is the preferred approach. The Vendor may use an equivalent standardized downloadable format.	
■		BP.06.04: Prompt patch notification	BR: The Vendor shall inform the Principal about approved, not approved and not relevant software patches within 30 days after release by the manufacturer of the software.	Bronze
■			RE(1): Software patch status notification shall also include a warning if the application of a patch requires or causes a re-start of the system.	Silver
■			RE(2): Patches and service packs approved by the Vendor shall not be re-distributed by the Vendor, but shall be made available to the Principal directly from the manufacturer of the software unless otherwise approved by the Principal..	Silver
■		BP.06.05: Audit tools	BR: The Vendor should provide tools to audit the current security patch status of the Vendor's system and provide a list of missing security patches. Note: Tools may include any means (manual or automated) to audit the current security patch status.	Bronze
■		BP.06.06: Patching documentation	BR: The Vendor shall describe the approved patching procedure and configuration instructions for its system, describing how to perform patching both manually and via a patch management server. a. When using a patch management server, documentation shall be provided to show how to configure the Vendor's system to receive updates. b. For manual patching using portable media, detailed instructions shall be supplied on how to install patches and how patching status reports shall be provided.	Bronze
■			RE(1): The Vendor shall describe a recommended roll-out procedure for software patching and upgrading all parts of its system.	Bronze
■	PA07: Secure Account Management	BP.07.01: Multiple default passwords	BR: The Vendor's system shall provide the capability to support default passwords used for system accounts (such as an administrators account) which can be changed by the Principal.	Bronze
■		BP.07.02: Removable default accounts	BR: The Vendor's system shall provide the capability to remove or disable unused default system accounts; e.g., Vendor "back-door", "super-user" and "guest" accounts.	Silver
■		BP.07.03: Minimum password strength	BR: The Vendor's system shall provide the capability to use passwords comprised of at least eight characters in length and consisting of a combination of at least three of the following four	Silver

	Process Area	Base Practice Objective	Requirements	Level
			character sets: lowercase, uppercase, numeric digit, and special character (%, #, etc.).	
■		BP.07.04: Password lifetimes and reuse restrictions	BR: The Vendor's system shall provide the capability to set local and domain user account passwords on their host-based devices to automatically expire every [user defined] days with a default of180,, and prevent reuse of the three previously used passwords.	Silver
■			RE(1): The Vendor's system shall provide the capability for users to be prompted to change their passwords [user defined] days prior to expiration with a default of 30 days.	Bronze
■			RE(2): The Vendor's system shall log and report unsuccessful login attempts in a timely manner to an interface specified by the Principal.	Bronze
■			RE(3): The Vendor's system shall restrict the use of shared passwords except for shared passwords approved by the Principal. Note: Requirements stated in RE(3) only apply to system generated passwords.	Silver
■		BP.07.05: Persistence of special accounts	BR: The Vendor's system shall provide the capability to set service, auto-login, and operator accounts so they never expire nor be disabled automatically.	Bronze
■		BP.07.06: Role-based access for network devices	BR: The Vendor's network devices shall provide the capability to enable role-based access features (e.g., separate passwords for administrators and operators). Note: Normally network devices are only accessed by administrators so only one role needs to be defined. However, if the Principal's operating procedures allow access to the network devices by administrators and others, then multiple roles need to be defined.	Bronze
■			RE(1): The Vendor's network devices shall provide the capability to encrypt passwords within the network device.	Silver
■			RE(2): The Vendor's system shall provide the capability to enable the use of encryption for administration of network devices within the control system over Ethernet.	Silver
■			RE(3): Where applicable, the Vendor's system shall provide the capability to enforce multi-factor access control. Note: Multi-factor access control requirements are a local matter defined by the Principal.	Gold
■			RE(4): Where required, the Vendor's system shall provide the capability to enforce two-way authentication of all network traffic. Note: Two-way authentication requirements are a local matter defined by the Principal.	Gold

	Process Area	Base Practice Objective	Requirements	Level
■		BP.07.07: Unified account management	BR: The Vendor's system shall provide the capability to support unified account management to centralize security policies and to decentralize execution of the security policies.	Bronze
■			RE(1): The Vendor's system shall provide the capability to restrict creation or modification of an account to an authorized user.	Bronze
■			RE(2): The Vendor's system shall provide the capability to locally manage security accounts in accordance with a centralized security policy.	Silver
■		BP.07.08: Maintain account logs	BR: The Vendor shall establish methods, processes and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.	Bronze
■	PA08: Support Backup/Restore	BP.08.01: Backup documentation	BR: The Vendor shall describe the recommended backup strategy and architecture for its system, including but not limited to the following: 01 Provisions for regular back-ups at intervals which fulfil the data restore and disaster recover objectives for the system. 02 Provisions to back-up the following types of data: Operation system files, Applications [including middleware, such as an OPC tunneller), Configuration data, Database files, Log files, Electronic log book, Unconventional file types (e.g., network equipment settings, Control System controller settings (tuning parameters, set points, alarm levels, etc.), field instrumentation parameters and Microsoft Active Directory]. 03 Provisions to back-up other files identified by the Vendor which are required to create a complete backup of the system. 04 Instructions on how to make a full backup of its system using at least one of the following methods: Proprietary backup architecture on removable media, Single system backup architecture on removable media, Distributed back-up architecture (using a backup system per group of ASD Systems, located close to these systems in the ASD), and Centralized back-up architecture (using one backup system for the whole ASD at a convenient location in the ASD). Note: Centralized backup architecture is preferred.	Bronze
■			RE(1): The Vendor shall recommend a procedure for verification of successful system back-up.	Bronze
■			RE(2): The Vendor's system shall provide the capability to generate and maintain an	Silver

	Process Area	Base Practice Objective	Requirements	Level
			audit log of all backup and restore activities.	
■		BP.08.02: Backup process	BR: The Vendor's system should provide the capability for the Principal's control and automation technicians to restore the system.	Bronze
■			RE(1):Commensurate with the Principal's process and procedures, the Vendor shall describe procedures for control and management of removable backup media. Note: Special attention should be given to Vendor procedures which are extensions of the Principal's procedures for control and management of removable backup media.	Bronze
■			RE(2): The Vendor's system shall provide the capability to restore the system back to a fully functioning system or to a simulation system from any point in the backup process.	Silver
■			RE(3): The Vendor's system shall function normally whilst a backup is in progress.	Silver
■	PA09: Increase Network Visibility	BP.09.01: Security monitoring protocols	BR: The Vendor's system shall provide the capability to monitor system security using at least one of the following methods: HIDS, Syslog, WMI or SNMP traps.	Bronze
■		BP.09.02: Management Information Base	BR: Where applicable for open systems supporting a Management Information Base (MIB), the Vendor shall install and test a MIB for sharing system configuration information and for monitoring system security performance. Note: Unit testing and Factory Acceptance Test are sufficient.	Silver
■			RE(1): The Vendor's system shall demonstrate a robust capability to protect against system scans during normal operation. Note: Achilles Communication Certification is an acceptable form of demonstration.	Silver
■	PA10: Standardize Historian Interfaces	BP.10.01: Historian data collection	BR: The Vendor's system shall provide the capability to collect historian data using an open standard communication protocol.	Bronze
■			RE(1): the Vendor shall provide a method for collecting historian data in a secure fashion. Note: Examples include but are not limited to OPC UA, OPCXI, SSL MatrikonOPC Tunneller.	Silver
■		BP.10.02: Data warehouses	BR: the Vendor's system shall provide the capability to securely interface to applicable data warehouses which are part of the Vendor's system or those provided by the Principal.	Silver
■		BP.10.03 Log and event management	BR: The Vendor's system shall provide the capability to log all state changes.	Bronze
■			RE(1): The Vendor's system shall securely report events to an interface	Silver

	Process Area	Base Practice Objective	Requirements	Level
			defined by the Principal. Note: For external interfaces to the Vendor's system, the communication protocol and semantics of the data reported will be defined by the Principal to support correlation of data.	
■			RE(2): The Vendor shall notify the Principal in a timely manner of a significant change in Vendor, Subcontractor or Consultant personnel who have digital access to the control system. Note: Access Control Lists (ACLs) containing personnel access and use privileges should be updated to reflect personnel changes.	Silver
■			RE(3): The Vendor's system shall log and report in a timely manner a security compromise detected in its system to an interface specified by the Principal.	Gold
■			RE(4): The Vendor's system shall securely respond to events in such a manner as to minimize the impact on normal or emergency operations. Note: Denial of Service (DoS) due to multiple alarm broadcasts should be the Vendor's primary concern.	Gold
■	PA11: Verify Operations	BP.11.01: Operator acknowledgement	BR: When changes to operating conditions come from remote or advisory set points, the Vendor's system shall provide the capability to acknowledge Operator action to verify a new set point or modification of an existing set point. If not acknowledged, the last approved set point shall be used.	Bronze
■			RE(1): When the new set point is outside the user-selected range, the Vendor's system shall provide the capability to generate an alarm, and the new set point shall not be used unless specifically approved by the Operator.	Silver
■		BP.11.02: Automated operations	BR: When operating conditions change due to automated operation (those without human intervention), the Vendor's system shall provide the capability to log the event and notify the operator in a timely manner. Note: Timely manner is a local matter which should be defined by the Principal.	Bronze
■	PA12: Connect Wirelessly	BP.12.01: Approved standards	BR: Where wireless devices are appropriate, the Vendor's system shall provide the capability to use wireless devices that comply with approved international wireless standards (e.g., IEEE, ISA, IEC).	Bronze
■			RE(1): The use of proprietary and non-standard protocols shall not be used unless approved by the Principal.	Bronze
■			RE(2): Industrial wireless field devices should be based on ISA 100 or WirelessHART. The use of other techniques shall not be used unless	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			approved by the Principal.	
■			RE(3): Wireless devices and systems (including infrared and non-RF) shall comply with approved international standards (e.g., NIST, ANSI, IEEE, IEC, ISO) or with regulatory requirements governing licensing of frequency bands.	Bronze
■		BP.12.02: Configuration methods	BR: The Vendor's system should provide the capability for the control system to configure wireless field instruments in a similar manner used to configure to wired field instruments.	Bronze
■			RE(1): The Vendor's system should provide the capability to view the latest configuration of a wireless field device used for monitoring and control from the control system.	Bronze
■	PA13: Fortify SIS Connectivity	BP.13.01: Configuration key switch	BR: The Vendor's system shall provide the capability to equip each SIS with a key switch to disable the SIS configuration mode.	Silver
■			RE(1): The Vendor's system shall implement a hardware (not software) key switch with the provision to remove the key from the switch when in the disable mode.	Silver
■			RE(2): An independent third party (e.g., TÜV, Oreda or Wurldtech) shall certify that it is not possible to change the configuration of the SIS when this key switch is in the disable mode.	Gold
■		BP.13.02: Third-party assessment	BR: The Vendor shall have periodic security risk assessments performed by a reputable third party (e.g., Exida, SAIC or Wurldtech) on SIS communications between, both internal and external to the safety network.	Gold
■		BP.13.03: Communications integrity	BR: The Vendor's system shall hard-wire, or logically separate connections between the SIS and safety-related communications (for SIL 1 and above) from other control system networks.	Bronze
■		BP.13.04: Layer 3 connections	BR: The Vendor's SIS shall not have a direct Ethernet connection to Layer 3.	Bronze
■			RE(1): The Vendor's SIS Engineering Work Station (EWS) shall only be connected to Layer 3 with a firewall or router that includes an Access Control List (ACL).	Silver
■		BP.13.05: DCS communications	BR: The Vendor's system shall not provide data connection between the DCS and SIS for safety-critical communications.	Bronze
■		BP.13.06: SIS EWS	BR: The Vendor's SIS EWS shall only be connected to the SIS directly (one-to-one connection) or via Layer 2 using a dedicated gateway.	Bronze
■			RE(1): The Vendor's SIS EWS shall be restricted to performing SIS functions.	Silver
■			RE(2): The Vendor's system shall not allow remote access to the SIS EWS.	Silver

	Process Area	Base Practice Objective	Requirements	Level
■	PA14: Provide Remote Access	BP.14.01: Remote access applications	BR: If remote access is required, the Vendor's system shall provide the capability for remote access using at least one of the following connectivity options (specified or later versions): a. Microsoft Terminal Services v5.2 (RDP), b. Symantec pcAnywhere V10.51, c. RealVNC v4.0, d. TeamSoftware Solutions Public Web Browser v2.09, e. Citrix ICA v9.151, f. Sun Microsystems Tarantella, g. NetSupport Manager v10	Bronze
■			RE(1): The Vendor shall provide detailed instructions for how to install, configure and operate the selected remote access software on the Vendor's system.	Bronze
■			RE(2): The Vendor shall provide adequate information about proposed methods of data transfer between its system and other systems and networks to allow the Principal to assess the risk and approve the method of data transfer before it is implemented.	Bronze
■		BP.14.02: Remote update applications	BR: The Vendor's system shall provide the capability to update firmware in remote devices in a secure manner with the provision to restrict read/write privileges. Note: Restricting read/write privileges is required to manage access to remote device data such as meter readings, but allow "write" to initiate a control action; e.g., disconnect the meter.	Gold
■	PA15: Protect Data	BP.15.01: Protect data at rest	BR: The Vendor's system shall provide the capability to protect selected data residing in any control system repository from unauthorized access or use.	Gold
■		BP.15.02: Protect data in transit	BR: The Vendor's system shall provide the capability to protect selected data in transit over any control system network or interface from unauthorized access or use, and protect the integrity of the data.	Gold
■		BP.15.03: Encryption	BR: The Vendor's system shall provide the capability to use encryption keys that provide at least 128 bit encryption.	Silver
■			RE(1): The Vendor's system shall provide the capability to use strong encryption (WPA2 or AES-256) or use VPN tunnels secured with IPSec or SSL for wireless bridges used for point-to-point backbone connectivity.	Gold
■			RE(2): The Vendor's system shall comply with FIPS 140-2 cryptographic module requirements.	Gold
■			RE(3): When applicable, the Vendor's system shall support use of ANSI X.509 digital certificates administered by the Principal.	Gold

	Process Area	Base Practice Objective	Requirements	Level
■			RE(4): The Vendor's system shall protect encryption keys and credential secrets such as passwords at all times, whether at rest or in transit.	Gold
■			RE(5): The Vendor's system shall provide the capability to manage keying material from a central console. Note: Keying material includes hardware devices (secure USB memory sticks, smart cards, etc.) and cryptographic keys for access and use control authentication.	Gold
■			RE(6): The Vendor's system shall provide the capability to automate all aspects of key exchange process in a reliable and fault tolerant manner.	Gold
■			RE(7): The Vendor's system shall provide the capability to manage at least six active encryption keys.	Gold
■			RE(8) The Vendor's system shall provide the capability to continue normal data processing during a period when a new definable key is being deployed.	Gold
■			RE(9): The Vendor's system shall provide the capability to manage keying material for legacy devices in a reliable and fault tolerant manner.	Gold

3.3.3 BP REQUIREMENTS: SYSTEM ACCEPTANCE TESTING & COMMISSION PAs

System Acceptance Testing and Commissioning PAs include process requirements and functional requirements. There are BRs and REs for each BP that is associated with a System Acceptance Testing and Commissioning PA. A BR and RE can be mandatory or strongly recommended. Table 5 lists the requirements.

Note: System Acceptance Testing (SAT) is performed by the Vendor at the Principal's site. It is assumed that SAT is performed in accordance with predefined/approved procedures and acceptance criteria. Furthermore, SAT tests are witnessed by Quality Assurance representatives from the Vendor and Principal who sign-off and certify that the test is completed satisfactorily. Satisfactory completion of all SAT tests results in commissioning the Vendor's system for operation and turn-over to the Principal for operations. Turn-over is the milestone which completes SAT and Commissioning and begins the Maintenance and Support phase of the Vendor's system life cycle.

Table 5 BP requirements: System Acceptance Testing & Commissioning PAs

	Process Area	Base Practice Objective	Requirements	Level
■	PA16: Manage the Deployment	BP.16.01 Risk assessment:	BR: The Vendor shall conduct a control system security risk assessment at the beginning of the commissioning phase.	Bronze
■			RE(1): The Vendor shall describe potential security risks and recommended mitigation procedures to the commissioning team during security awareness training. Note 1: Risk assessment at the time of commissioning is required because the Principal now has a benchmark based on the achieved or as-built security system. Note 2: Risk assessment is needed on a continuing basis to assess the achieved or current system security assurance level given the emerging threats and degradation in security capability of the installed system. Such an assessment should be used to continually revisit the pre-planned product improvements for the security system.	Silver
■		BP.16.02: Inventory register	BR: The Vendor shall document and maintain an inventory register of all components supplied by the Vendor.	Bronze
■			RE(1): The Vendor shall provide the Principal with documentation describing the as-built and installed equipment connections and configurations; e.g., manufacturing data files, keying management data, Principal's test files.	Bronze
■		BP.16.03: Temporary account removal	BR: After the completion of commissioning, the Vendor's system shall remove all temporary user accounts used during system testing and commissioning.	Bronze
■			RE(1): After system testing and commissioning have been completed, the Vendor's system shall generate an audit log showing all temporary accounts have been removed. Note: If not automated so the log is produced by the Vendor's system, then a	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			manual system is used to produce the log which significantly increases the cost to produce the log and to process the log.	
■		BP.16.04: Network scan	BR: During system testing and commissioning and upon request by the Principal the Vendor's system shall perform a network scanto discover hidden systems or vulnerabilities. Note 1: Where applicable, the network scan should include all devices with wired and wireless communication interfaces to the control system. Note 2: Network scans should be scheduled in accordance with the Principal's standard operating procedures.	Bronze
■			RE(1): During testing and commissioning the Vendor shall obtain approval from thePrincipal for the use of troubleshooting tools prior to being used on the ASD infrastructure.	Bronze
■			RE(2): During testing and commissioning the Vendor shall inform the Principal of any adverse effects that hardware or software troubleshooting tools may have on ASD network performance.	Bronze
■			RE(3): During testing and commissioning the Vendor shall perform an analysis of the network scan results to confirm that the configurations of communications ports are in compliance with the specifications.	Silver
■		BP.16.05: Relevant processes	BR: Prior to system testing and commissioning the Vendor's system shall verify that the Principal's Management of Change (MoC) and Permit To Work (PtW) processes has been followed for changes involving devices or connections between devices in the ASD.	Bronze
■			RE(1): During system testing and commissioning the Vendor shall certify that its sanitization process has removed all sensitive information from any part that will be replaced or that the part and the sensitive information have been destroyed.	Silver
■		BP.16.06: Timely notification	BR: During system testing and commissioning the Vendor's system shall demonstrate timely generation, logging and reporting of a simulated security compromise approved by the Principal.	Silver
■	PA17: Harden the Systems	BP.17.01: Harden system demonstration	BR: During system testing and commissioning, the Vendor's system shall demonstrate security mechanisms have been installed in accordance with approved procedures. Note: "approved procedures" should be compliant with the Vendor's hardening guide in BP.04.01BR.	Bronze
■			RE(1): During system testing and commissioning the Vendor's system shall verify the following conditions have been	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			successfully completed. a. Software and functionality that is not required for the intended functional purpose of the system; email, office applications, games, USB ports, Bluetooth and Wi-Fi communication, etc have been removed or not installed unless approved by the Prinicpal. b. Physical and logical access to diagnostic and configuration ports is protected. c. Unused ports on switches and routers that have been disabled so as to prevent unauthorized access to the ASD network infrastructure. d. If requested by the Principal, demonstrate maintenance processes that maintain the system-hardened state during the system lifetime.	
■		BP.17.02: Firewall use	BR: During system testing and commissioning the Vendor's system shall verify thatthe point of connection to a control system network includes a stateful firewall with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal prior to system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(1): During system testing and commissioning the Vendor's system should verify that the point of connection within the control system network between wired and wireless networks is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal prior to system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(2): During system testing and commissioning the Vendor's system should verify that the point of connection within the control system network to the SIS is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal prior to system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(3): During system testing and commissioning the Vendor's system should verify that the point of connection within the control system network to a data warehouse is firewalled with	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal prior to system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	
■	PA18: Protect from Malicious Code	BP.18.01: Quality definition files	BR: The Vendor shall have a process in place for qualifying virus definition files and provide documentation describing how approval of virus definition files shall be communicated to the Principal.	Bronze
■			RE(1): Virus definition files shall be 'released-for-installation' by the Vendor as soon as possible, with a maximum of 30 days after initial release. Note: RE(1) does not require installation within 30 days, only that the files be released for installation within 30 days.	Silver
■		BP.18.02: General anti-virus policy	BR: Prior to system testing and commissioning the Vendor shall update the document describing the configuration of the virus detection software installed on each ASD component.	Bronze
■			RE(1): Where the installation of anti-virus software is not technically possible, Prior to testing and commissioningthe Vendor shall update the document describing all computers where anti-virus software cannot be installed.	Bronze
■			RE(2): Prior to testing and commissioning the vendor shall update the document describing all the use of all mitigating features and functions used to reduce the risk of infection.	Bronze
■		BP.18.03: Portable media procedure	BR: The Vendor shall document a procedure for its staff stating that portable media (e.g. laptops and USB storage) used by the Vendor for system testing and commissioning of equipment or devices in the ASD are used for this purpose only.	Bronze
■			RE(1): The Vendor's portable media procedure shall include instructions for ensuring that the portable media is free of malicious code.	Silver
■		BP.18.04: Anti-virus management	BR: Prior to system testing and commissioning, the Vendor shall provide documentation to ensure thatthe use of correctly installed, configured and up-to-date anti-virus software has been verified.	Bronze
■			RE(1): Prior system testing and commissioning the Vendor shall document that the installation of qualified virus definition files have beenconducted and the files are current to within 30 days..	Bronze
■		BP.18.05: Anti-virus demonstration	BR: The Vendor's system shall demonstrate during system acceptance testing that malicious code can be detected and correctly handled by the anti-virus software. Note:A commonly accepted practice is to use the EICAR test file to document	Silver

	Process Area	Base Practice Objective	Requirements	Level
			detection and isolation of malicious code.	
■	PA19: Implement Patch Management	BP.19.01: Up-to-date systems	BR: For systems maintained by the Vendor, the Vendor shall keep the security patch levels of all ASD systems current to within 3 months of the security patch being available and qualified by the respective system Vendor.	Bronze
■			RE(1): If the installation of patches requires an outage that can impact operations or impacts performance, the Vendor shall develop and document a mitigation plan subject to approval by the Principal.	Bronze
■			RE(2): Vendor approved patches shall be approved by the Principal before they are installed on the Vendor's system.	Bronze
■	PA20: Secure Account Management	BP.20.01: Individual accounts	BR: During system testing and commissioning the Vendor's system shall demonstrate that invalid login attempts are logged and reported in a timely manner to an interface specified by the Principal.	Bronze
■			RE(1): During system testing and commissioning the Vendor's system shall demonstrate the capability to create unique user names and passwords.	Bronze
■			RE(2): Prior to system testing and commissioning the Principal shall verify that individual passwords have not been divulged to other persons and if so, have been changed.	Bronze
■			RE(3): Prior to system testing and commissioning the Vendor will verify that user names and passwordsapproved by the Principal to be shared by a Vendor's service group are correctly logged and maintained. Note: Principal approved names and passwords to be shared are owned by a named representative of the Vendor, who is also accountable and responsible for maintaining a log of each individual's usage of that account.	Bronze
■			RE(4): During system testing and commissioning the Principal shall verify that all users other than operators and service groups have unique individual user names and passwords in those cases where such are generated by the system.	Silver
■		BP.20.02: Default passwords	BR: During system testing and commissioning, the Vendor's system shall demonstrate the capability to create and maintain system accounts (such as an administrator account).	Bronze
■			RE(1): During system testing and commissioning the Vendor's system shall demonstrate the capability to restrict the use of default passwords.	Silver
■			RE(2): During testing and commissioning the Vendor's system shall demonstrate the capability to change default	Silver

	Process Area	Base Practice Objective	Requirements	Level
			passwords in accordance predefined timeout requirements	
■			RE(3): During system testing and commissioning the Vendor's system shall demonstrate the capability to remove or disable unused system default accounts; e.g., Vendor "back-door", "super-user" and "guest" accounts..	Silver
■		BP.20.03: Minimum password strength	BR: During testing and commissioning, the Vendor's system shall demonstrate and verify that all passwords are comprised of at least eight characters in length and consist of a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special character (%, #, etc.).	Silver
■		BP.20.04: Password lifetimes and reuse restrictions	BR: During system testing and commissioning the Vendor's system shall demonstrate that users are prompted to change their passwords [user defined] days prior to expiration with a default of 30 days.	Bronze
■		BP.20.05: Persistence of special accounts	BR: During system testing and commissioning the Vendor's system shall demonstrate that service, auto-login and operator accounts are configured so that they never expire nor become disabled automatically.	Silver
■		BP.20.06: Role-based access for network devices	BR: During system testing and commissioning, the Vendor's system shall demonstrate that encryption is used during administration of network devices within the ASD over Ethernet.	Silver
■			RE(1): During system testing and commissioning the Vendor's system shall demonstrate that network devices have passwords encrypted within the device	Silver
■			RE(2): During system testing and commissioning the Vendor's system shall demonstrate that network devices are implemented with role-based access (e.g. separate passwords for administrators and operators)..	Gold
■		BP.20.07: Workstation session lock	BR: During system testing and commissioning the Vendor's system shall demonstrate and verify that work stations located in areas that are normally unattended have the required authentication and have an active automatic locking or disconnection mechanism.	Bronze
■	PA21: Support Backup/Restore	BP.21.01: Regular backups	BR: During system testing and commissioning the Vendor's system shall perform a back-up and verify thatthe Vendor's system has regularly backed-up at scheduled intervals which fulfil the data restore and disaster recovery objectives for the system.	Bronze
■		BP.21.02: Backup demonstration	BR: During system testing and commissioning the Vendor's system shall demonstrate that it is possible to create a complete back-up of their system, and that it is possible to perform disaster recovery by restoring a fully functioning	Silver

	Process Area	Base Practice Objective	Requirements	Level
			system from this back-up.	
■	PA22: Implement the Architecture	BP.22.01: Architecture drawings	BR: Prior to system testing and commissioning the system design Vendor (or Contractor) shall provide the Principal with logical and physical infrastructure architecture drawings in AutoCAD or Microsoft Visio drawing formats, which verify that the Vendor's systems and components are compliant with the infrastructure architectural requirements described in this document.	Bronze
■		BP.22.02: Network layer separation	BR: During system testing and commissioning, the Vendor's system will verify that the Control System Network (CSN or Layer 3) and Distributed Control System (DCS) internal bus (Layer 2) are physically separated in a secure fashion. Note: A dedicated firewall (preferred), or dedicated router with an Access Control List (ACL) or by dual-homing connections without routing between these connections (lest preferred) are accepted.	Bronze
■		BP.22.03: Time synchronization	BR: During system testing and commissioning the Vendor's system shall perform and verify all time-synchronization of ASD equipment from a secure and accurate source; e.g. via a Network Time Protocol (NTP) server connected to Layer 3.	Silver
■	PA23: Connect Wirelessly	BP.23.01: Service set identifier (SSID)	BR: During system testing and commissioning the Vendor's system shall demonstrate that unique, location-specific SSIDsare used and verify that all SSIDs are descriptive acronyms which are not obviously associated with a Principal's location by the general public. Note: For example, PRINCIPAL_PLANT is not allowed.	Gold
■			RE(1): During system testing and commissioning the Vendor's system shall verify that the SSID is only sent using a broadcast or multicast message if services require its visibility.	Silver
■			RE(2): During system testing and commissioning the Vendor's system shall verify that wireless devices connected to a TCP/IP port use static IP addresses and Dynamic Host Configuration Protocol (DHCP) are disabled.	Silver
■		BP.23.02: Wireless device maintenance	BR: During system testing and commissioning the Vendor's system shall, where applicable, verify thatmaintenance and engineering of wireless devices connected to Layer 1 or Layer 2 are routed through the control system management workstation. Note: Direct access to these devices using wireless connections which bypass the DCS is not allowed.	Bronze
■			RE(1): During system testing and commissioning the Vendor's system shall verify thatremote maintenance and remote engineering of wireless devices connected to Layer 3 is only possible via	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			wired connections through the ASD firewall. Note: Direct access to these devices using wireless connections is not allowed.	
■		BP.23.03: Safeguarding functions	BR: During system testing and commissioning and if applicable the Vendor's system shall verify thatwireless devices are not allowed as an integral part of safeguarding functions (i.e. SIF, IPF, SIL 1 or higher) and that all sensors and final elements are directly wired to the SIS. Note: This requirement is to ensure the enforcement the Principal's policy that wireless is not allowed to be used as a communication bus within SIL related processes.	Bronze
■			RE(1): During system testing and commissioning the Vendor shall verify thatdue to the response time of wireless devices, their use as part of a control loop is approved by the Principal.	Bronze
■		BP.23.04: Secure accounts	BR: During system testing and commissioning the Vendor's system shall verify thatsecure usernames and passwords are used on all wireless devices, and thatmanufacturers' default user names and passwords are changed to locally specified ones when technically feasible.	Gold
■			RE(1): During system testing and commissioning, the Vendor's system shall verify that unused ports provided on wireless devices, such as a RS232 interface for configuration, should be made physically secure or disabled where possible.	Silver
■		BP.23.05: Wireless workers and CSAD	BR: During system testing and commissioning the Vendor's system shall verify thatif a worker uses a wireless handheld device as a DCS HMI in the field, then all wireless handheld device connectivity to the office domain shall be routed through the CSAD.	Gold
■		BP.23.06: Architecture documentation	BR: Prior to system testing and commissioning the system Vendor shall verify that its system architecture documentation describing wireless systems is up-to-date in its description of the following. a. Data exchange between Layer 1 and wireless instrumentation. b. Data exchange between Layer 2 and Layer 3 through a secure wireless link c. Bridge connecting the Layer 3 network using a secure wireless link d. Security mechanisms that prevents an intruder from gaining access to the ASD systems using the wireless system. e. Security mechanisms that restrict access within the ASD by workers	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			with handheld wireless devices f. Where required, security mechanisms that provides remote management of wireless systems.	
■			RE(1): During system testing and commissioning the system Vendor shall verify thatits system plan for the use of frequencies in wireless infrastructures, addressing non-interference and co-existence is up-to-date and approved by the Principal.	Bronze
■	PA24: Provide Remote Access	BP.24.01: Remote access documentation	BR: During system testing and commissioning the Vendor's system shall demonstrate during acceptance testing thatif remote access is required it is possible to remotely access its system using one of the allowed connectivity applications which comply with BP.14.01 requirements.	Bronze
■			RE(1): During system testing and commissioning the Vendor's system shall verify that if remote Vendor support is to be provided via Internet, then the Principal's Third Party Access (TPA) connection using encrypted transmissionis used to connect to the Principal's Global Infrastructure network from the Internet.	Silver
■			RE(2): During system testing and commissioning the Vendor's system shall verify that modem access to systems in the ASD is used subject to the following conditions. • A TCP/IP network connection is not feasible. • The modem used is approved by the Principal • The modem used is physically disconnected when not in use Note 1: If the Vendor is performing or supporting system testing and commissioning the Vendor should be able to ensure that the modem is physically disconnected when not in use. Note 2: If the Vendor is not performing or supporting system testing and commissioning the responsibility for RE(2) is not applicable to the Vendor.	Silver
■		BP.24.02: Connection approval and review	BR: Prior to system testing and commissioning the Vendor shall verify that all system-to-system connections and user-to-system connections are approved by the Principal in accordance with the requiredreview time.	Bronze
■	PA25: Protect Data	BP.25.01: Protect data at rest	BR: During system testing and commissioning the Vendor's system shall verify that access to and use of selected data in control system repositories is adequately protected. Note 1: "Adequately protected" is a local matter because it depends on specific sensitivity of the data to be protected. But, the protection requirements should be defined by a cyber-expert familiar with	Gold

	Process Area	Base Practice Objective	Requirements	Level
			accepted industry best practices. Note 2: See PA15 requirements to provide the capability to protect data. Note 3: See PA10 requirements to interface to standard historians and data warehouses.	
■		BP.25.02: Protect data in transit	BR: During system testing and commissioning the Vendor's system shall verify that access to and the integrity of selected data in transit within the control system network is adequately protected.	Gold
■			RE(1): During system testing and commissioning the Vendor's system shall verify that access to and the integrity of selected data in transit between the control system network and external interfaces to the control system is adequately protected. Note: BP.25.01 notes apply to BP.25.02.	Gold
■		BP.25.03: Encryption	BR: During system testing and commissioning the Vendor's system shall verify that ACLs and authentication methods are implemented to secure the wireless network	Silver
■			RE(1): During system testing and commissioning the Vendor's system shall verify that for wireless connections, the highest feasible level of WPA, WPA2 or AES security and encryption is used.	Gold
■			RE(2): During system testing and commissioning the Vendor's system shall verify that encryption or a secure tunnel between wireless devices are used where possible..	Gold
■		BP.25.04: Encryption key management	BR: During system testing and commissioning, and when encryption is required, the Vendor's system shall demonstrate that encryption keys and pre-shared keys input to devices are managed to ensure they are protected and accessible with the appropriate permissions.	Gold
■			RE(1): During testing and commissioning, the Vendor's system shall demonstrate automated fault tolerant key material management from a central console.	Gold
■		BP.25.05: Digital certificate management	BR: During testing and commissioning the Vendor's system shall, when applicable, verify that ANSI X.509 digital certificates administered by the Principal are securely protected.	Gold

3.3.4 BP REQUIREMENTS: MAINTENANCE & SUPPORT PAs

Maintenance and SupportPAs include process requirements and functional requirements. There are BRs and REs for each BP that is associated with a Maintenance and SupportPA. A BR and RE can be mandatory or strongly recommended. Table 6lists the requirements.

Note: In the context of the BP's related to Maintenance & Support, requirements apply to Maintenance or Support Events that could potentially effect the system's security posture, such as but not limited to, changes in software, firmware, system configurations, or components connected to the network.

Table 6 BP Requirements: Maintenance & Support PAs

	Process Area	Base Practice Objective	Requirements	Level
■	PA26: Manage the Deployment	BP.26.01 Risk assessment:	BR: Prior to scheduled maintenance testing, the Vendor shall conduct a control system security risk assessment of all Vendor system changes that will be verified in the next maintenance cycle. Note: Risk assessment is needed on a continuing basis to assess the achieved or current system security assurance level given the emerging threats and degradation in security capability of the installed system. Such an assessment should be used to continually revisit the pre-planned product improvements for the security system.	Bronze
■		BP.26.02: Inventory register	BR: Prior to scheduled maintenance testing, the Vendor shall update the inventory register of all components supplied by the Vendor.	Bronze
■		BP.26.03: Network scan	BR: During scheduled maintenance the Vendor's system shall perform a network scan at to discover hidden systems or vulnerabilities which may have been introduced since the last scan cycle. Note 1: Where applicable, the network scan should include all devices with wired and wireless communication interfaces to the control system. Note 2: Network scans should be scheduled in accordance with the Principal's standard operating procedures.	Bronze
■			RE(1): After scheduled maintenance testing the Vendor shall perform an analysis of the latest scan results to confirm that the configurations of communications ports are in compliance with the specifications.	Bronze
■			RE(2): Prior to scheduled maintenance, the Vendor shall inform the Principal of any adverse effects that existing or new hardware or software troubleshooting tools may have on ASD network performance.	Bronze
■			RE(3): Prior to scheduled maintenance testing the Principal shall approve the use of troubleshooting tools prior to being used on the ASD infrastructure.	Bronze
■		BP.26.04: Relevant processes	BR: Prior to scheduled maintenance testing the Vendor shall verify that the Principal's Management of Change (MoC) and Permit To Work (PtW) processes has been followed for changes involving devices or connections between devices in the ASD.	Bronze
■		BP.26.05: Timely notification	BR: Prior to scheduled maintenance testing, the Vendor's system shall	Silver

	Process Area	Base Practice Objective	Requirements	Level
			demonstrate timely generation, logging and reporting of a simulated security compromise approved by the Principal.	
■	PA27: Harden the Systems	BP.27.01: Harden system demonstration	BR: Prior to scheduled maintenance testing the Vendor shall verify that changes to or new security mechanisms have been installed in accordance with approved procedures. Note: “approved procedures” should be compliant with the Vendor’s hardening guide in BP.04.01BR.	Bronze
■		BP.27.02: Firewall use	BR: During scheduled maintenance testing the Vendor’s system shall verify thatthe point of connection to a control system network includes a stateful firewall with up-to-date documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal at system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(1): During scheduled maintenance testing the Vendor’s system should verify that the point of connection within the control system network between wired and wireless networks is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal at system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(2): During scheduled maintenance testing the Vendor’s system should verify that the point of connection within the control system network to the SIS is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal at system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze
■			RE(3): During scheduled maintenance testing the Vendor’s system should verify that the point of connection within the control system network to a data warehouse is firewalled with documented and maintained firewall rules. Note: Responsibility for maintaining up-to-date firewall rules and documentation may have been transferred to the Principal at system turnover. If this is the case, the Vendor role is, if required, to support verification that the firewall rules are up-to-date.	Bronze

	Process Area	Base Practice Objective	Requirements	Level
■	PA28: Protect from Malicious Code	BP.28.01: General anti-virus policy	BR: Prior to scheduled maintenance, the Vendor shall update the document describing the configuration of the virus detection software installed on each ASD component.	Bronze
■		BP.28.02: Portable media procedure	BR: Prior to schedule maintenance the Vendor shall update documents describing changes to a procedure for its staff stating that portable media (e.g. laptops and USB storage) used by the Vendor for commissioning and maintenance of equipment or devices in the ASD are used for this purpose only.	Bronze
■		BP.28.03: Anti-virus management	BR: Prior to scheduled maintenance, the Principal shall document changes to the installation of virus definition files have been installed and verified within 30 days after being qualified by the system Vendor.	Bronze
■	PA29: Implement Patch Management	BP.29.01: Up-to-date systems	BR: Prior to scheduled maintenance, for systems maintained by the Vendor, the Vendor shall update the security patch levels of all ASD systems current to within 3 months of the security patch being available and qualified by the respective system Vendor.	Bronze
■	PA30: Secure Account Management	BP.30.01: Individual accounts	BR: Prior to scheduled maintenance, the Principal shall reconfirm that all users other than operators and service groups shall have unique individual user names and passwordsin cases where such are generated by the system.	Bronze
■			RE(1): During scheduled maintenance testing the Vendor's system shall demonstrate that invalid login attempts are logged and reported in a timely manner to an interface specified by the Principal.	Bronze
■		BP.30.02: Minimum password strength	BR: During scheduled maintenance testing, the Vendorshall re-verify that controls are in place to ensuresystem passwords are comprised of at least eight characters in length and consist of a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special character (%, #, etc.).	Bronze
■		BP.30.03: Password lifetimes and reuse restrictions	BR: During scheduled maintenance testing the Vendor's system shall re-verify that local and domain user account passwords have been configured to automatically expire every 180 days or otherwise as request by the Pricipal.	Bronze
■			RE(1): Prior to scheduled maintenance, the Vendorshall re-verify that users are prompted to change their passwords [user defined] days prior to expiration with a default of 30 days.	Bronze
■			RE(2): During scheduled maintenance, the Vendor shall re-verify that controls are in place to prevent systemusers from reuse of ther last three passwords.	Silver

	Process Area	Base Practice Objective	Requirements	Level
		BP.30.04: Persistence of special accounts	BR: Prior to scheduled maintenance the Vendor's system shall re-verify that service, auto-login and operator accounts are configured so that they never expire nor become disabled automatically.	Bronze
		BP.30.05: Role-based access for network devices	BR: During scheduled maintenance the Vendor's system shall re-verify that network devices retain approved role-based access configurations including encrypted passwords within the device.	Silver
		BP.30.06: Workstation session lock	BR: During scheduled maintenance testing the Vendor's system shall demonstrate and re-verify that workstations located in areas that are normally unattended have the required authentication and have an active automatic locking or disconnection mechanism.	Silver
	PA31: Support Backup/Restore	BP.31.01: Regular backups	BR: During scheduled maintenance testing the Vendor's system shall perform a back-up and verify thatthe Vendor's system has regularly backed-up at scheduled intervals which fulfil the data restore and disaster recovery objectives for the system.	Gold
		BP.31.02: Backup prior to change event	BR: During scheduled maintenance testing the Vendor's system shall perform a back-up and verify that a back-up has been completed prior to an engineering change being made to the hardware or software or installing an operating system patch or upgrade.	Gold
			RE(1): During scheduled maintenance testing the Vendor's system shall perform a back-up and verify thatbefore back-up occurred before a change is made for which automatic roll-back is impossible, orafter modifications to the system resulting from scheduling changes, or authorization and authentication changes, or after process trip or alarm level changes or application changes.	Gold
		BP.31.03: Backup demonstration	BR: During scheduled maintenance testing the Vendor's system shall verify that a complete back-up the system and restoration is functioning properly from this back-up..	Gold
	PA32: Implement the Architecture	BP.32.01: Architecture drawings	BR: Prior to scheduled maintenance testing the Vendor shall re-verify that logical and physical infrastructure documents have been updated to include any changes and are compliant with the infrastructure architectural requirements described in this document.	Bronze
		BP.32.02: Network layer separation	BR: During scheduled maintenance testing the Vendor's system shall verify that the physical network separation requirement remains properly implemented.	Bronze
	PA33: Connect Wirelessly	BP.33.01: Service set identifier (SSID)	BR: During scheduled maintenance testing the Vendor's system shall re-verify that unique, location-specific	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			SSIDs are used.	
■		BP.33.02: Wireless device maintenance	BR: scheduled maintenance testing the Vendor's system shall re-verify, where applicable, thatmaintenance and engineering of wireless devices connected to Layer 1 or Layer 2 are routed through the control system management workstation. Note: Direct access to these devices using wireless connections which bypass the DCS is not allowed.	Bronze
■			RE(1): During scheduled maintenance testing the Vendor's system shall verify thatremote maintenance and remote engineering of wireless devices connected to Layer 3 is only be possible via wired connections through the ASD firewall. Note: Direct access to these devices using wireless connections is not allowed.	Bronze
■		BP.33.03: Safeguarding functions	BR: During scheduled maintenance testing the Vendor's system shall re-verify thatwireless devices are not allowed as an integral part of safeguarding functions (i.e. SIF, IPF, SIL 1 or higher) and that all sensors and final elements are directly wired to the SIS. Note: This requirement is to ensure the enforcement the Principal's policy that wireless is not allowed to be used as a communication bus within SIL related processes.	Silver
■			RE(1): During scheduled maintenance testing the Vendor's system shall re-verify thatdue to the response time of wireless devices, their use as part of a control loop is approved by the Principal.	Bronze
■		BP.33.04: Secure accounts	BR: During scheduled maintenance testing the Vendor's system shall re-verify thatsecure usernames and passwords are used on all wireless devices, and thatmanufacturers' default user names and passwords are changed to locally specified ones when technically feasible.	Silver
■		BP.33.05: Wireless workers and CSAD	BR: During scheduled maintenance testing the Vendor's system shall re-verify thatif a worker uses a wireless handheld device as a DCS HMI in the field, then all wireless handheld device connectivity to the office domain shall be routed through the CSAD.	Gold
■		BP.33.06: Architecture documentation	BR: Prior to scheduled maintenance the system Vendor shall re-verify that its system architecture documentation describing wireless systems is up-to-date.	Bronze
■			RE(1): Prior to scheduled maintenance, the system Vendor shall re-verify thatits system plan for the use of frequencies in wireless infrastructures, addressing non-interference and co-existence is up-to-	Bronze

	Process Area	Base Practice Objective	Requirements	Level
			date and approved by the Principal.	
■	PA34: Provide Remote Access	BP.34.01: Remote access documentation	BR: During scheduled maintenance testing the Vendor's system shall re-verify that if remote Vendor support is to be provided via Internet, then the Principal's Third Party Access (TPA) connection using encrypted transmissionis used to connect to the Principal's Global Infrastructure network from the Internet.	Gold
■		BP.34.02: Connection approval and review	BR: Prior to scheduled maintenance the Vendor shall re-verify that all system-to-system connections and user-to-system connections are approved by the Principal in accordance with the requiredreview time.	Bronze
■	PA35: Protect Data	BP.35.01: Protect data at rest	BR: During scheduled maintenance testing the Vendor's system shall re-verify that access to and use of selected data in control system repositories is adequately protected.	Gold
■		BP.35.02: Protect data in transit	BR: During scheduled maintenance testing the Vendor's system shall re-verify that access to and the integrity of selected data in transit within the control system network is adequately protected.	Gold
■			RE(1): During scheduled maintenance testing the Vendor's system shall verify that access to and the integrity of selected data in transit between the control system network and external interfaces to the control system is adequately protected.	Gold
■		BP.35.03: Encryption	BR: During scheduled maintenance testing the Vendor's system shall re-verify that encryption or a secure tunnel between wireless devices are used where possible.	Gold
■			RE(1): During scheduled maintenance testing the Vendor's system shall re-verify that for wireless connections, the highest feasible level of WPA, WPA2 or AES security and encryption is used.	Gold
■			RE(2): During scheduled maintenance, the Vendor's system shall re-verify that ACLs and authentication methods are implemented to secure the wireless network.	Gold
■		BP.35.04: Encryption key management	BR: During scheduled maintenance testing the Vendor's system shall re-verify that encryption keys and pre-shared keys input to devices are managed to ensure they are protected and accessible with the appropriate permissions.	Gold
■			RE(1): During scheduled maintenance testing the Vendor's system shall re-verify automated fault tolerant key material management process from a central console is performed in accordance with the Principal's security operating policies and practices.	Gold

	Process Area	Base Practice Objective	Requirements	Level
■		BP.35.05: Digital certificate management	BR: During scheduled maintenance testing the Vendor's system shall, when applicable, re-verify that ANSI X.509 digital certificates administered by the Principal are securely protected.	Gold

APPENDIX 1 REFERENCES

In this REQUIREMENTS DOCUMENT, reference is made to the following publications:

NOTES: The latest edition of each publication shall be used, together with any amendments, supplements or revisions thereto.

STANDARDS

Manufacturing and Control Systems Security Part 1: Concepts, Models and Terminology	ISA-99.01.01
Manufacturing and Control Systems Security Part 2: Establishing an IACS Security Program	ISA-99.02.01
Cyber Security - Systems Security Management	NERC CIP-007-1
Recommended Security Controls for Federal Information Systems	NIST 800-53 Revision 2
Security for industrial-process measurement and control - Network and systems security	IEC 62443-3
Guide to ICS Security	NIST 800-82
Guidelines for Smart Grid Cyber Security	NISTIR 7628 Vol 1,2,3
Department of Homeland Security: Cyber Security Procurement Language for Control Systems	August 2008
Code of Practice for Informarion Security Management	ISO 27002
IT Network Security - Securing Remote Access	ISO 18028-4
American Chemistry Council's Chemical Information Technology Center: Roadmap to Secure Control Systems in the Chemical Sector	ChemITC
Open Application Group, Inc.	OAGi

APPENDIX 2 ARCHITECTURE LEVELS IN ISA-99.00.01, PART 1

Ref.: ISA-99.00.01-2005, Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models, Figure 5 – DCS Example using the General Reference Model.

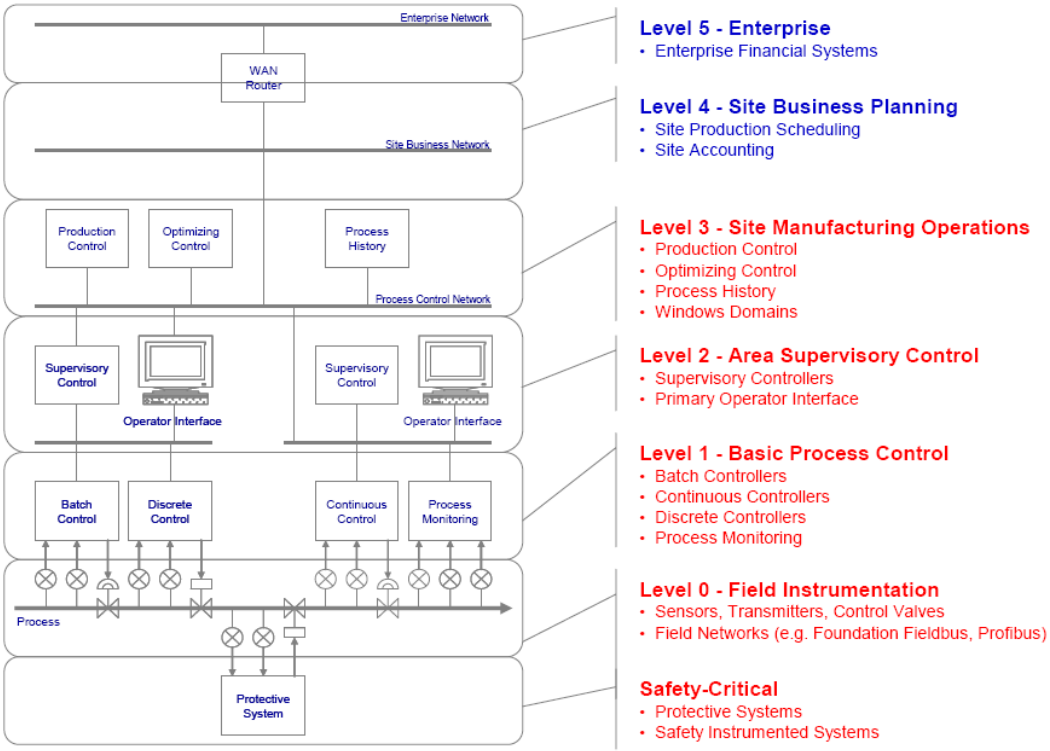
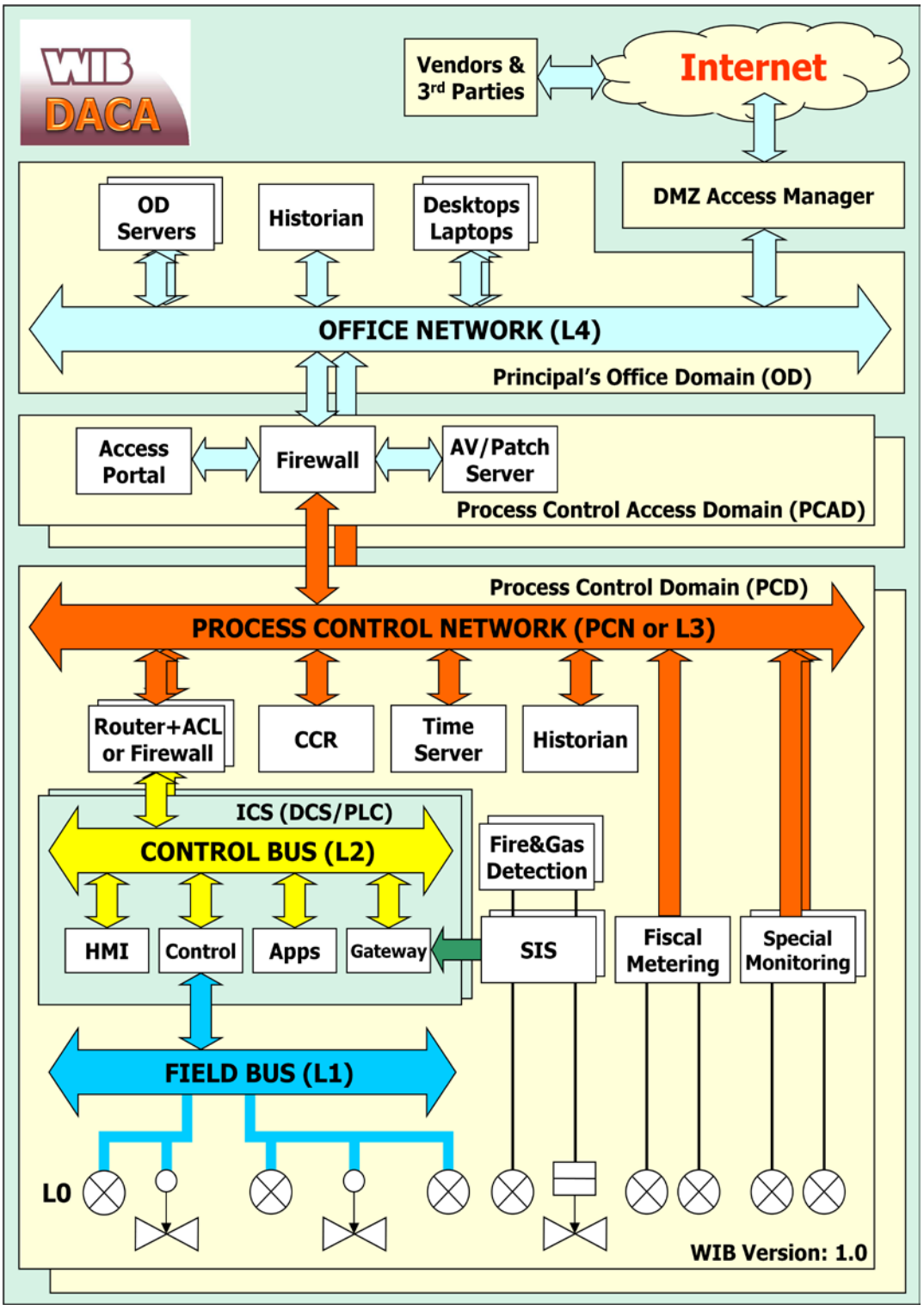


Figure 5 – DCS Example using the General Reference Model

APPENDIX 3 WIB's DACA (DATA ACQUISITION AND CONTROL ARCHITECTURE)



The above is WIB's Reference Architecture and an example. Other system architectures are possible and allowed.

APPENDIX 4 WIB'S APPROVED 'CONNECTIVITY APPLICATIONS'

If required, the Vendor shall provide remote access using at least the connectivity applications specified (or later versions) as listed below in this Appendix.

- Microsoft Terminal Services v5.2 (RDP)
- Symantec pcAnywhere v10.51
- RealVNC v4.0
- TeamSoftware Solutions Public Web Browser v2.09
- Citrix ICA v9.151
- Sun Microsystems Tarantella
- NetSupport Manager v10

End of document – last page