DREAM TEAM:
BUILDING THE PERFECT ICS TEAM

SANS Industrial Control Security

Conference Singapore

December 3, 2013

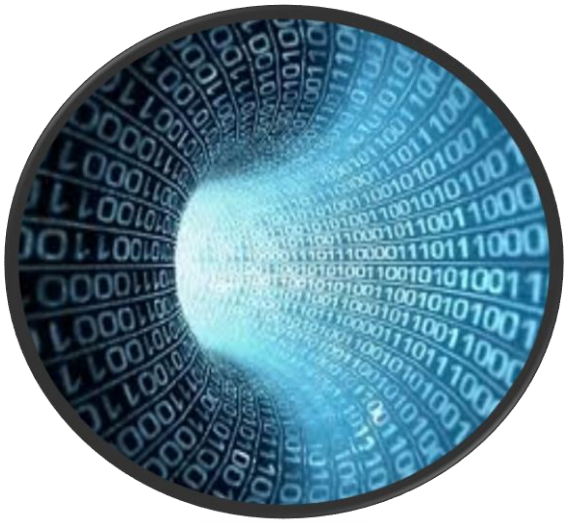
Tyler Williams & Paul Piotrowski, GICSP, CISSP, CRISC
ICS Solutions Manager & Senior PCD Security Engineer

INDUSTRIAL CYBER SECURITY – A HYBRID SKILL-SET REQUIREMENT

The Starting Point

To effectively design, develop, implement and maintain cyber security controls for industrial automation and control infrastructure, PCD IT Security practitioners require a unique set of skills, knowledge and abilities which span multiple domains such as Engineering, General IT and Cyber Security.

Industrial Automation & Control Systems



General Information Technology (IT)

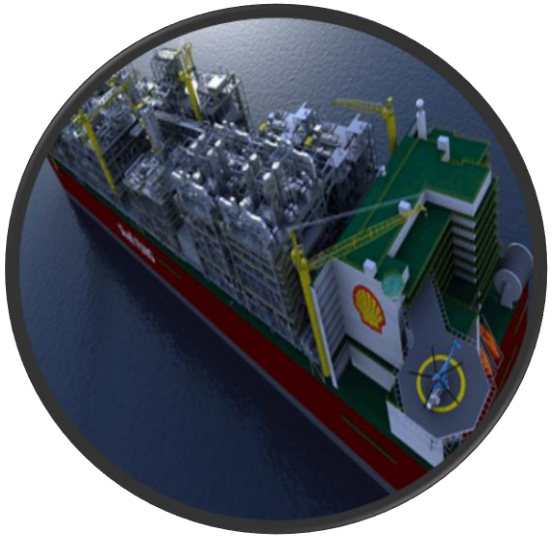
Cyber Security & Risk Management

INDUSTRIAL CYBER SECURITY – A MAJOR SKILLS GAP

The Lifecycle Dependency & Skill-shortage

Effective cyber risk management practices also require the application of security controls at many stages in the automation and control system life-cycle and involves many parties who also must have that same hybrid skill-set. A competency missing from the marketplace today.

Buy Secure
Robust Systems & Applications

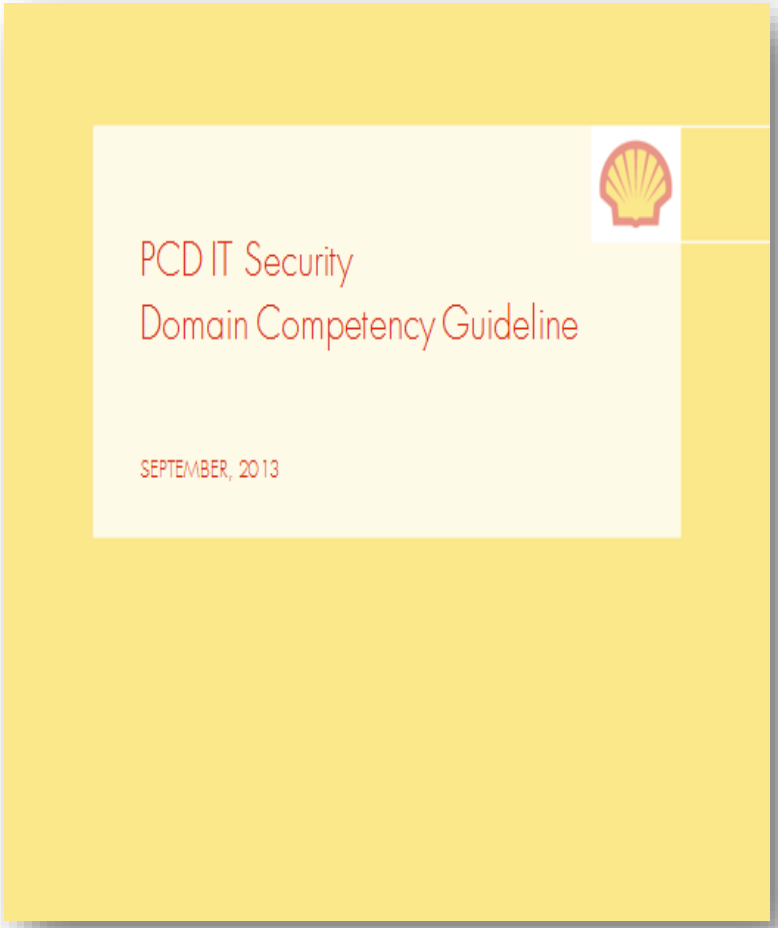


Deploy Secure
Secure Configurations

Run Secure
Compliance Monitoring

INDUSTRIAL CYBER SECURITY – AN INTERNAL COMPETENCY

Step 1: *Design A Hybrid Competency Framework For Internal Practitioners*



IT & IT Security Competencies

- Business Risk Management
- Incident, Threath and Vulnerability Mgt
- IT Audit & Compliance
- IT Architecture

Engineering Competencies

- Process Automation Systems Engineering
- SIS & Safeguarding
- PCD Integrity & Security

Job Competency Profile for PCD IT Security

Job Category	PCD IT Security JG 6	PCD IT Security JG 5	PCD IT Security JG 4	PCD IT Security JG 3	PCD IT Security JG 2
Job Title	PCD IT Security Practioners			Experts	Authorities
Business Risk Management	K	K	S	S	S
Incident, Threath and Vulnerability Mgt	K	K	K	S	S
IT Audit & Compliance	K	K	K	S	S
IT Architecture				K	K
Process Automation Systems Engineering	K	K	K	K	S
SIS & Safeguarding			K	K	K
PCD Integrity & Security	K	K	S	S	M

K = Knowledge
S = Skills
M = Mastery

INDUSTRIAL CYBER SECURITY – AN INTERNAL COMPETENCY

Step 1: *Design A Hybrid Competency Framework For Internal Practitioners*

Process Automation Systems Engineerig

Definition: Specify, implement, maintain, modify, troubleshoot and assess performance of process automation systems (network architecture and control system). The focus is on Distributed Control Systems (DCS) as it is the larger and more commonly used control system. However, other engineered process control systems also fall under this competency such as Programmable Logic Controllers (PLCs); Supervisory Control and Data Acquisition (SCADA) system; tank gauging systems; 3rd party systems,…

LEVEL	PROOF POINTS:
Knowledge	**Distributed Control Systems**
	▪ Explain the purpose of the major components of the DCS architecture
	▪ Maintain and modify existing DCS operation in accordance with Shell and Supplier standards
	▪ Troubleshoot (with assistance) DCS control and network loading
	▪ Maintain and modify (with assistance) existing Asset Management system operational in accordance with Shell and Supplier standards
	▪ Describe the main communication protocols
	▪ Troubleshoot (with assistance) communication systems
	▪ Explain and evaluate existing DCS selection and installation against engineering standards and practices
	▪ Explain how DCS work procedures and practices relate to technology practices and standards
	▪ Execute, apply and maintain DCS maintenance procedures
	▪ Participate in factory acceptance test (FAT) or site acceptance test (SAT) of a process automation system
	Control Systems Architecture
	▪ Maintain and modify (with assistance) standard (vs. complex) control systems architecture
	▪ Explain the major elements of the control system architecture
	▪ Describe the benefits and limitations of different control system architecture
	▪ Maintain relevant control systems architecture documentation as-built
	▪ Explain the benefits and limitations of different communication networks used to transfer data between domains
	Systems Engineering - Other
	▪ Maintain and modify (with assistance) existing (other types of) monitoring, control and safeguarding systems
	▪ Troubleshoot (with assistance) existing (other types of) monitoring, control and safeguarding systems

Incident, Threat and Vulnerability Management

Definition: Principles, methods, tools and techniques for reporting, identifying and handling (a) information risk incidents, retaining evidence, establishing root causes (b) information threats (c) information vulnerabilities, and implementing improvements to processes.

LEVEL	PROOF POINTS:
Knowledge	▪ Describes the Incident/Threat/Vulnerability (ITV) Management process in detail
	▪ Has completed (external/internal) training in identifying different types of incidents, threats or Vulnerabilities and know the reporting and handling procedures for each
	▪ Able, with appropriate guidance, to contribute to the analysis of the root cause of incidents and Vulnerabilities or the potential impact of Threats
	▪ Knows how to collect and retain evidence of incidents without losing forensic evidence (I)
	▪ Recognises when an incident or Vulnerability is subject to legal and regulatory requirements or when a Threat may impact such requirements
	▪ Knows when to involve experts and/or authorities when the Incidents, Threats or Vulnerabilities involve legal and regulatory issues and can escalate these issues
Skill	▪ Able to give a comprehensive description of the ITV process
	▪ Designs, develops and implements ITV Management procedures,
	▪ Specifies procedures for collecting and retaining (potential forensic) evidence of incidents and advise Incident Managers in this area (I)
	▪ Specifies procedures for identifying and classifying Threats and advise Threat analysts in this area (T)
	▪ Able to analyse Threat data and asses its impact on Shell's (critical) Information Assets (T)
	▪ Specifies procedures for performing penetration tests, code inspection and vulnerability assessments (V)
	▪ Manages the contribution of experts and/or authorities when the analysis involves legal and regulatory issues
	▪ Sets up and manages a process for identifying the root cause of incidents or Vulnerabilities and manages the contributions of others in this process (I, V)
	▪ Sets up and manages a process for identifying and classifying Threats and manages the contributions of others in this process (T)
	▪ Coaches and trains others in the principles, methods and techniques for managing ITV

INDUSTRIAL CYBER SECURITY – AN INTERNAL COMPETENCY

Example:

PCD IT Security Site Focal Point

Competences:

Competences	JG 6	JG 5	JG 4	JG 3	JG 2
Business Risk Management		K	S		
Incident, Threath and Vulnerability Mgt		K	K		
IT Audit & Compliance		K	K		
IT Architecture					
Process Automation Systems Engineering		K	K		
SIS & Safeguarding			K		
PCD Integrity & Security		K	S		

Recommended training:

Training	JG 6	JG 5	JG 4	JG 3	JG 2
Network (CCNA or equivalent)					
Operating Systems (Windows MCSA modules)					
Cyber Security: SSCP					
Cyber Security: CISSP					
Cyber Security: CISSP-ISSMP or CISM					
Process Automation Systems Engineering - Awareness					
SIP-0 Introduction M269					
General PCD Security Training for Staff					
Basic PCD Security Training					
Advanced PCD Security training					

PCD IT Support

Competences:

Competences	JG 6	JG 5	JG 4	JG 3	JG 2
Business Risk Management	K	K			
Incident, Threath and Vulnerability Mgt	K	K			
IT Audit & Compliance	K	K			
IT Architecture					
Process Automation Systems Engineering	K	K			
SIS & Safeguarding					
PCD Integrity & Security	K	K			

Recommended training:

Training	JG 6	JG 5	JG 4	JG 3	JG 2
Network (CCNA or equivalent)					
Operating Systems (Windows MCSA modules)					
Cyber Security: SSCP					
Cyber Security: CISSP					
Cyber Security: CISSP-ISSMP or CISM					
Process Automation Systems Engineering - Awareness					
SIP-0 Introduction					
General PCD Security Training for Staff					
Basic PCD Security Training					
Advanced PCD Security training					

INDUSTRIAL CYBER SECURITY – AN INTERNAL COMPETENCY

Example:

Example Name *Job Competency Profile*

Role

Competences:

Competences	JG 6	JG 5	JG 4	JG 3	JG 2
Business Risk Management	K	K			
Incident, Threath and Vulnerability Mgt	K	K			
IT Audit & Compliance	K	K			
IT Architecture					
Process Automation Systems Engineering	K	K			
SIS & Safeguarding					
PCD Integrity & Security	K	K			

Recommended training:

Training	JG 6	JG 5	JG 4	JG 3	JG 2
Network (CCNA or equivalent)					
Operating Systems (Windows MCSA modules)					
Cyber Security: SSCP					
Cyber Security: CISSP					
Cyber Security: CISSP-ISSMP or CISM					
Process Automation Systems Engineering - Awareness					
SIF-0 Introduction					
General PCD Security Training for Staff					
Basic PCD Security Training					
Advanced PCD Security training					

INDUSTRIAL CYBER SECURITY – AN EXTERNAL REQUIREMENT

Step 2: *Establish An External & Standardized Benchmark For Industry*

- End Users
- System Vendors
- Integrators
- Security Consultants
- Government Agencies

WHAT DOES THIS LOOK LIKE AT A FACILITY?

- SUPPORT MODEL: BUSINESS/IT/BOTH
- DEVELOP TOOLS FOR SUCCESS
- HYBRID "ALL THE WAY"
- DEVELOP RESOURCES & BE PATIENT