The Industrial Control System
Cybersecurity Lifecycle

exida

	INPUT	PROCESS	OUTPUT	exida services
ASSESS PHASE	Corporate /site policies and procedures Project Specific Requirements Architecture Drawing(s) Regulations (e.g. NERC CIP, CFATS, etc.) Standards (e.g. ISA/IEC 62443.3.3)	**Scope Definition and Project Setup** (ISA/IEC 62443.3.2)	Project Management Plan	• Analyze and create existing architecture drawing(s) • Policy development and/or review • Cybersecurity Awareness Training
		Cybersecurity Vulnerability Assessment	Cybersecurity Vulnerability Assessment Report	• Perform Cybersecurity Vulnerability Assessment • Update Architecture Drawing(s) • Evaluation of existing countermeasures • Windows Security Vulnerability Assessment (WSVA)
	HAZOP & SIL Selection Cybersecurity Risk Assessment Procedure Knowledge of process and business impact	**Cybersecurity Risk Assessment** (ISA/IEC 62443.3.2)	Cybersecurity Risk Assessment Report	• Development of a cybersecurity risk assessment • Train staff on risk assessment procedure • Facilitate and Document Risk Assessment • Threat Modeling
	Tolerable Risk Guidelines	**Cybersecurity Target Selection** (ISA/IEC 62443.3.2)		• Facilitate Cybersecurity Target Selection
	Standards e.g. ISA/IEC 62443.3.2) Reference Architectures & Best Practices	**Zone and Conduit Model** (ISA/IEC 62443.3.2)	Zone and Conduit Drawing(s)	• Zoning and Conduit Modeling - Development of corporate reference models - High-level diagrams - Detailed design - Design reviews
		Document Requirements (ISA/IEC 62443.3.2)	Cybersecurity Requirements Specification (CRS)	• Cybersecurity Requirements Specification (CRS) Template • CRS Development • CRS Review
IMPLEMENT PHASE	Cybersecurity Requirements Specification (CRS)	**Conceptual Design** (ISA/IEC 62443.3.2)	Cybersecurity Design Spec (CDS)	• Cybersecurity Design Specification (CDS) Consultation • CDS Review • Technology Investigation
		Design Validation (ISA/IEC 62443.3.2)	Validation Report	• Defense-in-Depth Analysis (analysis of effectiveness of defense layers) • Detection-in-Depth Analysis (analysis of effectiveness of monitoring layers)
		Adequate Design? NO		
	Cybersecurity Design Spec (CDS)	**Detailed Design**	Design Package (Drawings, Configurations, Procedures)	• Development of Procedures • ACL Development/Review • Design Reviews
	Cybersecurity Requirements Specification (CRS) Security Manuals of ICS Products	**Develop Test Plans** (ISA/IEC 62443.3.2)	Cybersecurity Factory Acceptance Test (CFAT) Plan Cybersecurity Site Acceptance Test (CSAT) Plan	• Cybersecurity Factory Acceptance Test (CFAT) Plan Development • Cybersecurity Site Acceptance Test (CSAT) Plan Development • Test plan review
	Design Package (Drawings, Configurations, Procedures)	**Implement Design**		
	Cybersecurity Factory Acceptance Test (CFAT) Plan	**Cybersecurity Factory Acceptance Test (CFAT)** (ISA/IEC 62443.2.4)	Cybersecurity Factory Acceptance Test (CFAT) Report	• Cybersecurity Factory Acceptance Testing (CFAT) • Windows Security Vulnerability Assessment (WSVA)
		Installation / Commissioning (ISA/IEC 62443.2.4)		
	Cybersecurity Site Acceptance Test (CSAT) Plan	**Cybersecurity Site Acceptance Test (CSAT)** (ISA/IEC 62443.2.4)	CSAT Test Report	• Cybersecurity Site Acceptance Testing (CSAT) • Windows Security Vulnerability Assessment (WSVA)
MAINTAIN PHASE	Patch Management Procedure Antivirus Management Procedure	**Countermeasure Maintenance**	Maintenance Records	• Vulnerability Management Service
	Security Monitoring Procedure	**Security Monitoring**	System Logs (IDS / SIEM)	• Develop logging requirements • Design monitoring methods • Review
	Change Management Procedure	**Modifications or Decommision**	Impact Analysis Change Request	• Impact Analysis Review
		YES Modifications? (To appropriate lifecycle phase)		
	ICS Cybersecurity Assessment Procedure	**Periodic Assessment**	ICS Cybersecurity Assessment Report	• Perform ICS Cybersecurity Assessment • Windows Security Vulnerability Assessment (WSVA) • Cybersecurity Scorecard

Control System Security Management Program: Policy, Standards, Procedures, Training, Awareness
(ISA/IEC62443.2.1 formerly ISA99.02.01)

©Copyright 2012-2013 exida Consulting LLC

Version 1.19 January 2013

www.exida.com/Security
Security@exida.com