Setting the Standard for Automation™

Risk Analysis for Industrial Control Systems

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Presenter

Dirk Sweigart, PMP

- Bachelor degrees in Mechanical Engineering and Computer Science, Master of Business Administration
- Chief of Information Security for DuPont ATS spinoff (INVISTA), 2001-2002
- CISSP, 2002-2005
- Joined Applied Control Engineering, Inc. (ACE) in 2015
- Based in ACE's Newark, DE headquarters working on information security and manufacturing execution systems

APPLIED CONTROL ENGINEERING

THE RIGHT SOLUTION. ON-TIME. ON-BUDGET.

Security Management

Primary Goals and Objectives - CIA

- Confidentiality – protection against unauthorized disclosure
- Integrity – internal and external consistency of data, objects, and resources
- Availability – timely and uninterrupted access to objects

Concepts in Risk Management

- Asset and asset valuation
- Threats and vulnerabilities
- Exposure
- Risk = threat x vulnerability
- Safeguards

Industrial control systems are set apart by the potential impact of a disruption of an ICS process

Quantitative Risk Analysis

- Assign an Asset Value (AV)
- Calculate Exposure Factor (EF)
- Calculate Single Loss Expectancy (SLE)
- Assess the Annualized Rate of Occurrence (ARO)
- Drive the Annualized Loss Expectancy (ALE)
- Perform cost/benefit of analysis of countermeasures

Asset Valuation (AV)

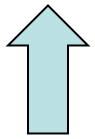
- Purchase cost/ development cost
- Value to owners, users, or competitors
- Operational cost of asset presence or loss
- Results in a dollar value ($)

Threats and Vulnerabilities

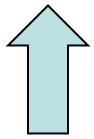
- Physical damage – purposeful, environmental, or accidental
- Electronic access – users or hackers
- This is likely a long list!
- For each asset, you need to calculate:
  - Exposure Factor (EF)
  - Single-Loss Expectancy (SLE)

Exposure factor (EF) and Single-Loss Expectancy (SLE)

Asset	Value	Threat	EF	SLE
Chiller PLC (cooling)	$50,000	physical damage	80.0%	$40,000
PID server	$2,000,000	unencrypted backup stolen	100.0%	$2,000,000
Engineer's laptop	$10,000	left at airport security	90.0%	$9,000
User workstation	$500	virus	90.0%	$450



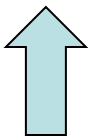
How much of the asset would be lost?



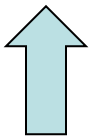
How much value could we lose?

Annualized Rate of Occurrence (ARO) and Annualized Loss Expectancy (ALE)

			Exposure Factor	Single-loss Expectancy	Annualized Rate of Occurrence	Annualized Loss Expectancy
Asset	Value	Threat	EF	SLE	ARO	ALE
Chiller PLC (cooling)	$50,000	physical damage	80.0%	$40,000	0.01	$400.00
PID drawing server	$2000,000	unencrypted backup stolen	100.0%	$2,000,000	0.001	$2,000.00
Engineer's laptop	$10,000	left at airport security	90.0%	$9,000	1.00	$9,000.00
User workstation	$500	virus	90.0%	$450	20.00	$9,000.00



How often could this occur in a year?



Possible yearly cost

Once the ALE is understood, economically appropriate mitigations can be determined

Risk Management

Developing appropriate safeguards to manage the risks

- What are potential safeguards? Calculate the costs of options
- Perform a cost/benefit analysis of the safeguard versus the threat to the asset using pre- and post-safeguard conditions

(pre-countermeasure ALE –
post-countermeasure ALE) -
annual cost of safeguard = value

For More Information

NIST - Guide for Conducting Risk Assessments
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

NIST - Guide to Industrial Control Systems (ICS) Security
http://dx.doi.org/10.6028/NIST.SP.800-82r2

ANSI/ISA-TR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems
https://www.isa.org/store/products/product-detail/?productId=116722

Setting the Standard for Automation™

Risk Analysis for Industrial Control Systems

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits