Safety Considerations for SCADA/DCS Cyber Security

Walter Sikora
Industrial Defender

ICSJWG 2010 Spring Conference

Introduction

- What's the difference between safety and security?
- Cyber Security culture
- Test your organization
- Examples of security incidents?
- Incident reporting
- Q&A

Massive gasoline pipeline explosion

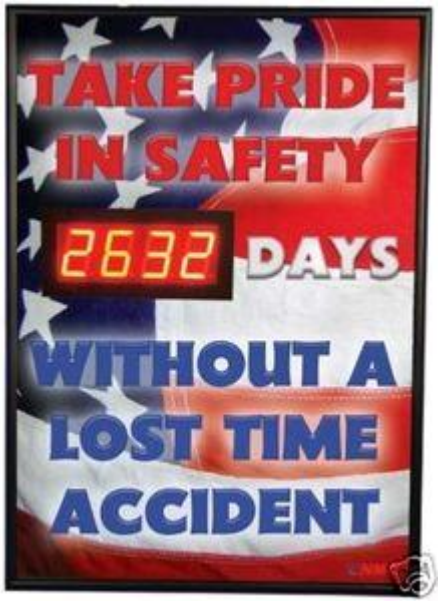
- Problem
  - On J… …nning
  - throu… …ses
  - inclu…
  - syste… …ors
  - coul… …ad
  - beer… …n first
  - teste…
- Consequ…
  - 3 de…
  - safe…
  - dest…
- Key Con…
  - Tech… …ring
  - Polic…

Factual Information 2 Pipeline Accident Report

Figure 1. Postaccident aerial view of portion of Whatcom Creek showing fire damage.

Source: Public Record http://www.ntsb.gov/publictn/2002/PAR0202.pdf

Safety First



Protect you Workplace

Justification to $pend…

- We cannot afford to protect everything, but we cannot simply stand by and protect nothing
- Companies have been trained by this economy to have no expenditures that do not produce profit within a few months
- Protective and preventative measures to defend against a terrorist act likely do not generate such a profit

Leverage ICS safety processes

- Appling every security control available to ensure the physical safety of plant is very well understood
- we need to educate folks to take the same approach now for cyber security.
- Use same or similar process like for example
- Getting Material Safety Data Sheet (MSDS) information out to work force to get the cyber security information out

Remote Control

- Threat of manipulating SCADA/DCS commands without the consent of the local plant ops, sys admins and plant engs
- Consider the safety implications of setpoints, open/close commands, and other SCADA/DCS functions being deployed at will from remote, what about unauthorized locations?
- The potential for safety hazards due to remote control of equipment is increased with the threat of a cyber attack on the SCADA/DCS system

Policy and Procedures

- Remote control safety threat has traditionally been mitigated by posting signs that read “This equipment is controlled by a remote computer system and may start at any time.”
- The company’s lock-out, tag-out policy also helps mitigate this risk, by locking out the electrical signals to the equipment it can then be worked on without remote start capabilities
- Security like safety has to be managed

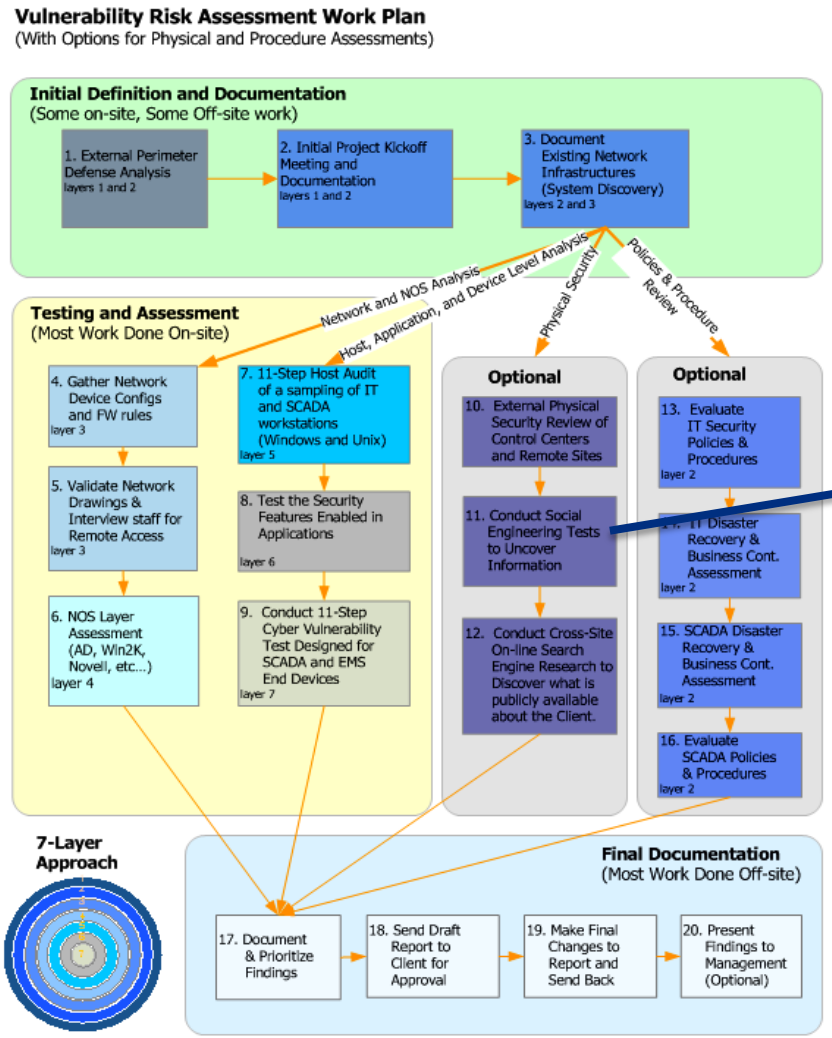
We all know it can be done…

- Unaware of the process, or what injected commands could do to the operations of the facility, a malicious hacker could send a command to set all outputs to an OFF state or to an ON state

- Security vulnerability and risks on control systems also create safety vulnerabilities and risks that must be evaluated and mitigated

- Administrators of SCADA/DCS systems must develop Contingency Plans that outline the actions and procedures to be taken if the facility were to ever experience a cyber attack

Social Engineering tests



Game playing crashes system

Problem

In 2005, a Scandinavian power generation company noticed their performance decreasing across all their Windows machines. After a long period of investigation it was discovered that there was an employee who installed a game from CD-ROM. The game contained a trojan which started propagating throughout the system.

Consequences

There was a system performance drop, investigation time used, and each system was shutdown to clean out the trojan. Although the control system wasn't taken down, the control system was spared infection because the control OS was HP-UX.

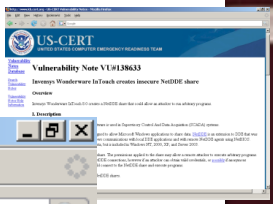
Key Control System Recommendations

Technology: Segmentation, NIDS, HIDS

Policy: Strict policy on computer system use

Source: Industrial Defender Contact

Wonderware InTouch NetDDE vulnerability



http://www.kb.cert.org - US-CERT Vulnerability Notes - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

View Notes By
Name
ID Number
CVE Name
Date Public
Date Published
Date Updated
Severity Metric

Vulnerability Note VU#138633

Invensys Wonderware InTouch creates insecure NetDDE share

Overview

Invensys Wonderware InTouch 8.0 creates a NetDDE share that could allow an attacker to run arbitrary programs.

I. Description

Invensys Wonderware InTouch HMI Software is used in Supervisory Control And Data Acquisition (SCADA) systems.

Dynamic Data Exchange (DDE) was designed to allow Microsoft Windows applications to share data. NetDDE is an extension to DDE that was developed by Wonderware. NetDDE allows communications with local DDE applications and with remote NetDDE agents using NetBIOS. NetDDE is not supported in Windows Vista, but is included in Windows NT, 2000, XP, and Server 2003.

InTouch 8.0 creates a universal NetDDE share. The permissions applied to the share may allow a remote attacker to execute arbitrary programs. Windows access permissions apply to NetDDE connections, however if an attacker can obtain valid credentials, or possibly if anonymous connections are enabled, the attacker could connect to the NetDDE share and execute programs.

Other vendors may also create insecure NetDDE shares.

II. Impact

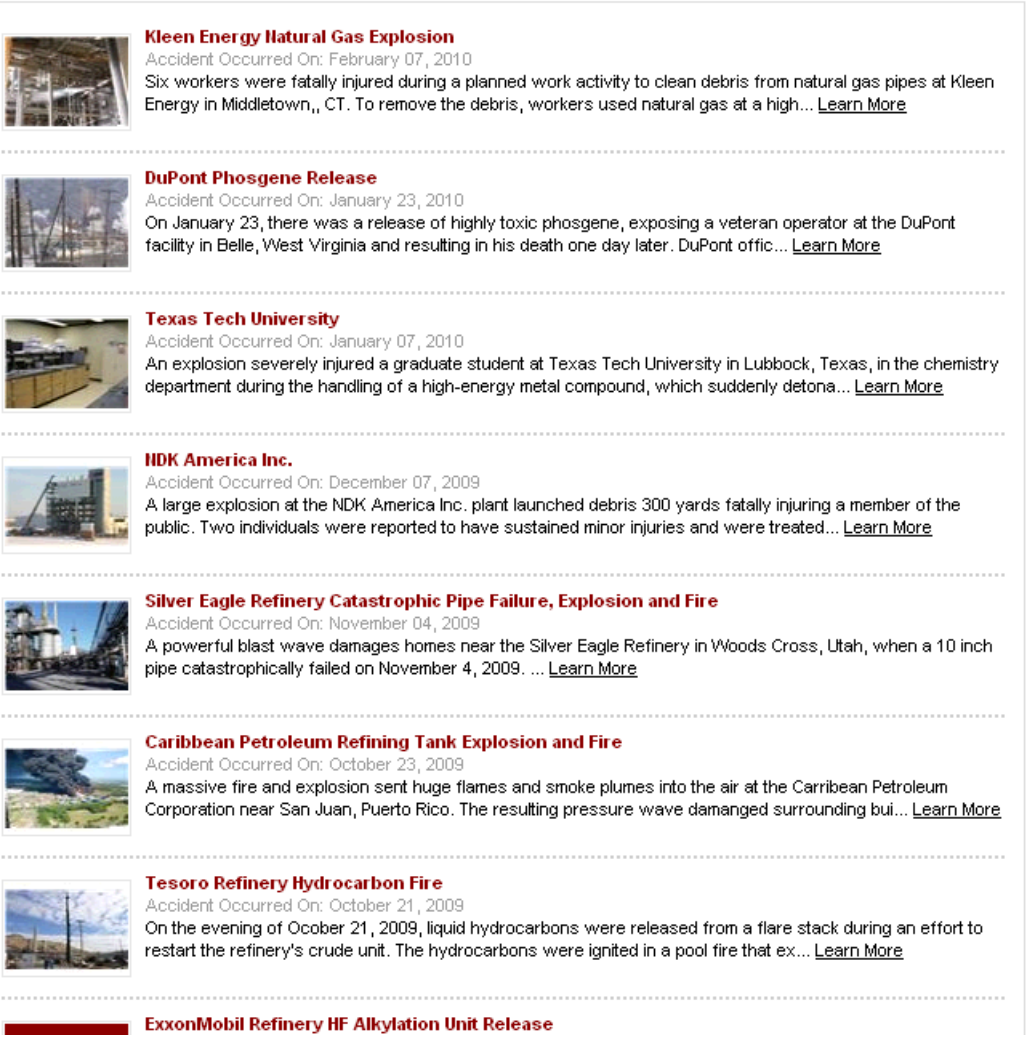
http://www.us-cert.gov/

NERC Advisory

2010 Advisories		
Date	**Description**	**Responsible Entities**
04.07.10	**CIP: SSH Brute-Force Scanning and Attacks**	Reliability Coordinator, Balancing Authority, Transmission Operator, Generation Operator, Generation Owner, Transmission Owner, Planning Authority (Coordinator), Load-Serving Entity, Distribution Provider, Purchasing-Selling Entity, Interchange Authority, Reserve Sharing Group, Transmission Planner, Transmission Service Provider, Resource Planner
02.25.10	**Reliability Risk – Interconnection Frequency Response - (Revision 1)** [Background]	Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Balancing Authorities, Reliability Coordinators, Load Serving Entities, and Distribution Providers
02.11.10	**Reliability Risk – Interconnection Frequency Response**	Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Balancing Authorities, Reliability Coordinators, Load Serving Entities, and Distribution Providers
02.03.10	**CIP: Rockwell Automation MicroLogix Controllers Password Security and Client Software Authentication Vulnerabilities**	Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Balancing Authorities, Reliability Coordinators, Load Serving Entities, and Distribution Providers
01.25.10	**CIP: ABB SPIDER/Network Manager Buffer Overflow**	Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Balancing Authorities, Reliability Coordinators, Load Serving Entities, and Distribution Providers
01.07.10	**Theft Concerns of Dielectric Used in Electrical Components**	Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Load Serving Entities, Distribution Providers

www.nerc.com

CSB investigations



Kleen Energy Natural Gas Explosion
Accident Occurred On: February 07, 2010
Six workers were fatally injured during a planned work activity to clean debris from natural gas pipes at Kleen Energy in Middletown,, CT. To remove the debris, workers used natural gas at a high... Learn More

DuPont Phosgene Release
Accident Occurred On: January 23, 2010
On January 23, there was a release of highly toxic phosgene, exposing a veteran operator at the DuPont facility in Belle, West Virginia and resulting in his death one day later. DuPont offic... Learn More

Texas Tech University
Accident Occurred On: January 07, 2010
An explosion severely injured a graduate student at Texas Tech University in Lubbock, Texas, in the chemistry department during the handling of a high-energy metal compound, which suddenly detona... Learn More

NDK America Inc.
Accident Occurred On: December 07, 2009
A large explosion at the NDK America Inc. plant launched debris 300 yards fatally injuring a member of the public. Two individuals were reported to have sustained minor injuries and were treated... Learn More

Silver Eagle Refinery Catastrophic Pipe Failure, Explosion and Fire
Accident Occurred On: November 04, 2009
A powerful blast wave damages homes near the Silver Eagle Refinery in Woods Cross, Utah, when a 10 inch pipe catastrophically failed on November 4, 2009. ... Learn More

Caribbean Petroleum Refining Tank Explosion and Fire
Accident Occurred On: October 23, 2009
A massive fire and explosion sent huge flames and smoke plumes into the air at the Carribean Petroleum Corporation near San Juan, Puerto Rico. The resulting pressure wave damanged surrounding bui... Learn More

Tesoro Refinery Hydrocarbon Fire
Accident Occurred On: October 21, 2009
On the evening of Ocober 21, 2009, liquid hydrocarbons were released from a flare stack during an effort to restart the refinery's crude unit. The hydrocarbons were ignited in a pool fire that ex... Learn More

ExxonMobil Refinery HF Alkylation Unit Release

www.csb.gov

OSSHA?

Occupational Safety and Security Protection For Employees of the *(Insert Your Agency Here)*

The Occupational Safety and Security Act of 2012, Executive Order 007 and 29 CFR 2012 require the heads of Federal agencies to furnish to employees places and conditions of employment that are free from job safety, security and health hazards.

Responsibilities of Your agency

1. General Requirements
The *head of your agency* will furnish *Your agency* employees places and conditions of employment that are free from on-the-job safety, health and Security hazards.

2. OSSHA Regulations
Your agency will comply with applicable regulations of the Occupational Safety and Health Administration.

3. Reporting Hazards
Your agency will respond to employee reports of hazards in the workplace.

8. Reporting Security Incidents, Accidents, Injuries and Occupational Illnesses
Supervisors must submit a supervisor's report of accidental injury/illness for all work-related accidents, injuries or occupational illnesses experienced by employees under their supervision.

9. Security, Safety and Health Committees
Your agency will support any safety and health committees that are formed from management and employee representatives.

Employee Responsibilities

1. Compliance with Standards

3. Reporting Hazards
Employees and their representatives shall have the right to report un secure, unsafe or unhealthful working conditions to appropriate officials and to request an inspection of the workplace. The name of the employee making the report will be kept confidential if requested.

4. Freedom from Fear of Reprisal
Employees and their representatives are protected from restraint, interference, coercion, discrimination, or reprisal for exercising any of their Safety and Health Program rights under the *Your agency*

Responsible Officials

The Designated Agency Safety and

Need a "Open" Security Incident Database

http://www.osha.gov/pls/odi/establi

nt Specific Injury and Ill...

DEPARTMENT OF L

Occupational Safety & Healt

OSHA Home

Each year the Occupational Safety and Health
within specific industry and employment size s
provided is used by OSHA to calculate establis
name, address, industry, and associated Total
Away From Work (DAFWII) case rate for the e
(collection of CY 2007 data). This database do
unreliable data. The 2007 data is available in a

Access information is provided below for each
DAFWII, TCR and DART. See Explanatory Note

Search by:

Establishment:

City:

State: All States

Zip:

Year range: 1996 200

SIC:

NAICS:

TCR:

DART:

DAFWII[1]:

Submit

UNITED STATES
DEPARTMENT OF LABOR
Occupational Safety & Health Administration

A to Z Index | En Español | Conta

OSHA Home

RSS Feeds | Print This Page

Search Items	Date Range	State
	2006 to 2007	DE

Sort By: | TCR | DART | DAFWII | Return to Search

Result Page: 1 2 3 4 5 6 7 8 9 10 ...

Results 1 - 20 of 354
By State, Name, Street, City, Year

Establishment Name	Street	City	State	Zip	Year	SIC	NAICS	TCR	DART	DAFWII
A H Angerstein Inc	315 New Road	Wilmington	DE	19805	2007	5211	423310	14.12	11.3	11.3
A H Angerstein Inc	315 New Road	Wilmington	DE	19805	2006	5211	423310	6.97	4.65	2.32
Aearo Corporation	650 Dawson Dr	Newark	DE	19713	2007	3081	326113	0	0	0
Allied Waste Services	1420 New York Ave	Wilmington	DE	19801	2007	4953	562219	7.71	6.61	6.61
Allied Waste Services	1420 New York Ave	Wilmington	DE	19801	2006	4953	562219	2.14	1.07	1.07
Allied Waste Services Llc	907 Willow Grove Rd	Felton	DE	19943	2007	4212	562219	12.72	11.56	6.94
Allied Waste Services Llc	907 Willow Grove Rd	Felton	DE	19943	2006	4212	562219	9.81	8.72	8.72
Acme Markets Inc	1901 Concord Pike	Wilmington	DE	19803	2007	5411	445110	11.28	4.83	1.61
Agilent Technologies Inc	2850 Centerville Rd	Wilmington	DE	19808	2007	3826	334516	1.11	.32	.16
All-Span, Inc.	9347 Allspan Dr	Bridgeville	DE	19933	2006	3448	332311	15.95	4.56	2.28
Allen Family Foods Inc	Rr 5	Harbeson	DE	19951	2007	2015	311615	2.51	2.51	.61
Allen Family Foods Inc	Rr 5	Harbeson	DE	19951	2006	2015	311615	3.73	3.38	.8
Allens Hatchery Inc	126 N Shipley St	Seaford	DE	19973	2007	0254	112340	4.73	0	0
Allens Hatchery Inc	126 N Shipley St	Seaford	DE	19973	2006	0254	112340	10.55	4.87	4.87
Allens Hatchery Inc	Rr Box 13a	Delmar	DE	19940	2006	2048	311119	7.61	5.07	2.54
Alternate Care Inc	715 E King St	Seaford	DE	19973	2006	8051	623110	5.76	1.28	1.28
American Cedar & Millwork Inc	17993 American Way	Lewes	DE	19958	2007	5031	423310	27.85	23.21	23.21

Safety & Security convergence

- Company culture around security must start from the top
- Employees need to understand cyber security risks and how it could affect safety
- Need to educate employees on “what is safe computing”
- Like safety – security compromise – should have zero tolerance
- Consider publishing internal security metrics for all to see
- Security Management Metrics
- OSHA for security?

Resources

- *Repository of Industrial Security Incidents (www.securityincidents.org). RISI is a non-profit organization that maintains a database of cyber security incidents compiled over more than 20+ years. It focuses on incidents in process control systems, industrial automation environments, and SCADA systems in an objective, factual way.*

- *U.S. Department of Homeland Security (www.us-cert.gov/control_systems). The U.S. government offers abundant free resources and safety and security information from training to standards to technical information. Its Control System Security Program specifically addresses efforts to reduce industrial control system risks.*

http://kenexis.com/Default.aspx

Kenexis is a global consulting and engineering firm. Our experts assist process industry facilities to improve safety and efficiency. We do this by helping to ensure that engineered safeguards are applied in an optimal fashion, resulting in best in class safety at costs that are in line with industrial peers.

Questions and Answers

Walter Sikora
wsikora@industrialdefender.com
508-718-6706
Twitter @nerccip