Connecting the Dots with ICS Cyber Incidents

Joe Weiss, PE, CISM
Applied Control Solutions, LLC
(408) 253-7934
joe.weiss@realtimeacs.com

ICSJWG 2010 Spring Conference

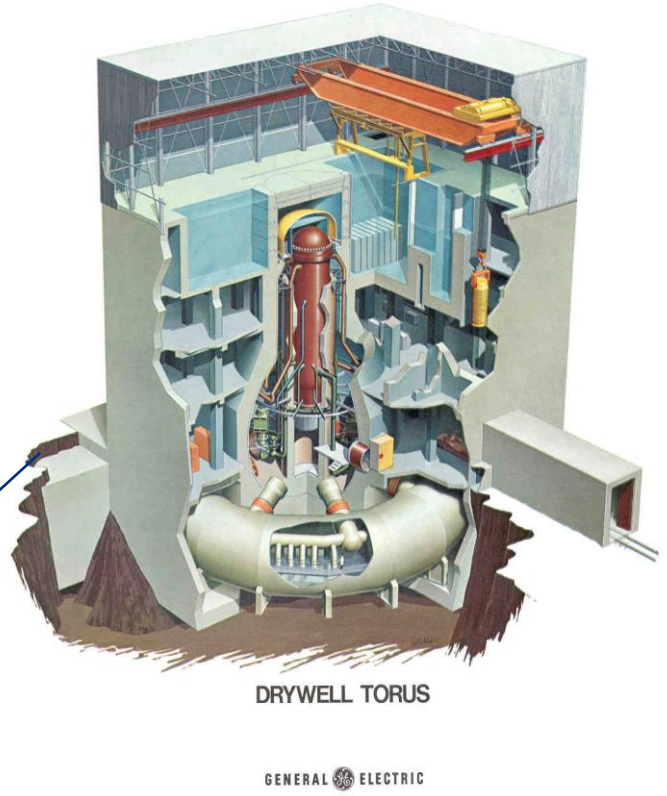
Targeted SCADA attack - US

- Insecure GIS mapping system integration led to targeted attack
- No SCADA servers or mapping system for two weeks
- 4 Man-months to recover
- Minimal forensics
- No information sharing with local law enforcement, FBI, or ES-ISAC

Plant typical of Browns Ferry and Hatch

Similar systems impacted
Inadequate policies
Inadequate design
Lack of forensics
Failsafes worked!

Same problems affected
many non-nuclear facilities



Reactor Coolant Pump

Pipeline rupture with fatalities

June 10, 1999 in Bellingham, WA
SCADA failure resulted in gasoline discharge into two creeks and ignited

Fireball killed three persons, injured eight; caused significant property damage; released ~230,000 gallons of gasoline causing substantial environmental damage

Previous SCADA problems
Minimal cyber forensics

DC Metro crash

June 22, 2009, two WMATA trains collide

- 9 fatalities; 52 injured

NTSB investigation determined the Automatic Train Protection (ATP) system failed to detect the presence of an idling train

ATP is a “vital system” provides protection agains collisions and over speed conditions

Sept 22 NTSB letters cite parasitic oscillations and unintended signal paths

Lack of alarms and adequate forensics

Unintended ICS impacts

A disturbance resulted in the loss of SCADA, AGC, Network Applications and ICCP. **The disturbance was caused by the implementation of a device locking security tool. The tool caused select hard drives to become unavailable**. The tool was being implemented in response to the Critical Infrastructure Protection (CIP) standards.

From January-June 2009 NERC Disturbance Reports