Supply Chain Issues with Energy Sector ICS Software

Laura S. Tinnel

Sr. Computer Scientist, laura.tinnel@sri.com

October 2021

SRI International®

Some of the work by SRI International was funded by the U.S. DHS S&T Directorate under Contract No. HSHQDC-16-C-00034. The opinions, findings, conclusions, and recommendations expressed in this material are those of the authors, do not necessarily reflect the views of DHS or its partners and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DHS or the U.S. government.

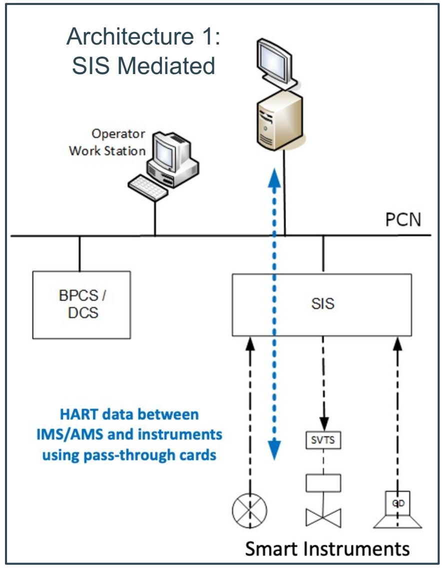
LOGIIC Project: Safety System Instruments

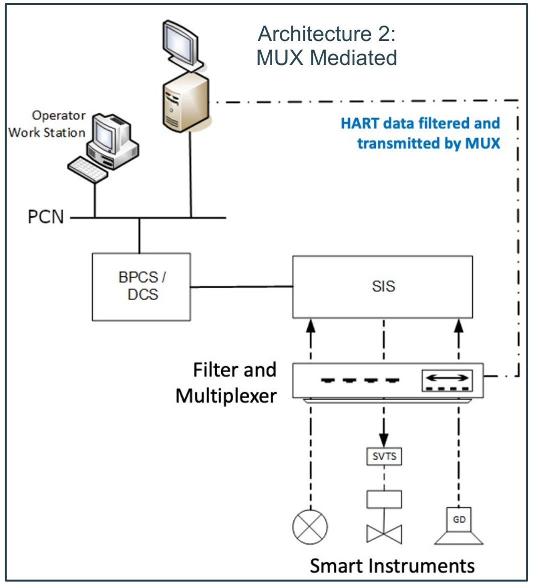
Cybersecurity Challenges in the ICS

- Business networks + operational networks
- Operational Technology (OT) devices
  - Hardware + Firmware + Software + Configuration Files
  - Often “deploy and forget” – may be in the field for over 30 years
  - OT device management
    - Management software runs on commodity IT computers and operating systems (OT/IT combined)
    - Often runs on old, unsupported operating systems (have seen Windows XP still in use)
- Often connected to business IT networks and/or remote access for ease of management
- Typically, do not follow IT security best practices
  - Insecure by design networks and systems
  - Supply chain vulnerable to simple attacks (low hanging fruit)
  - Due to
    - Belief that applying best practices will harm operations
    - Operators think systems are isolated and unreachable
    - General lack of awareness of what can happen and recommended practices

What is a Safety Instrumented System?

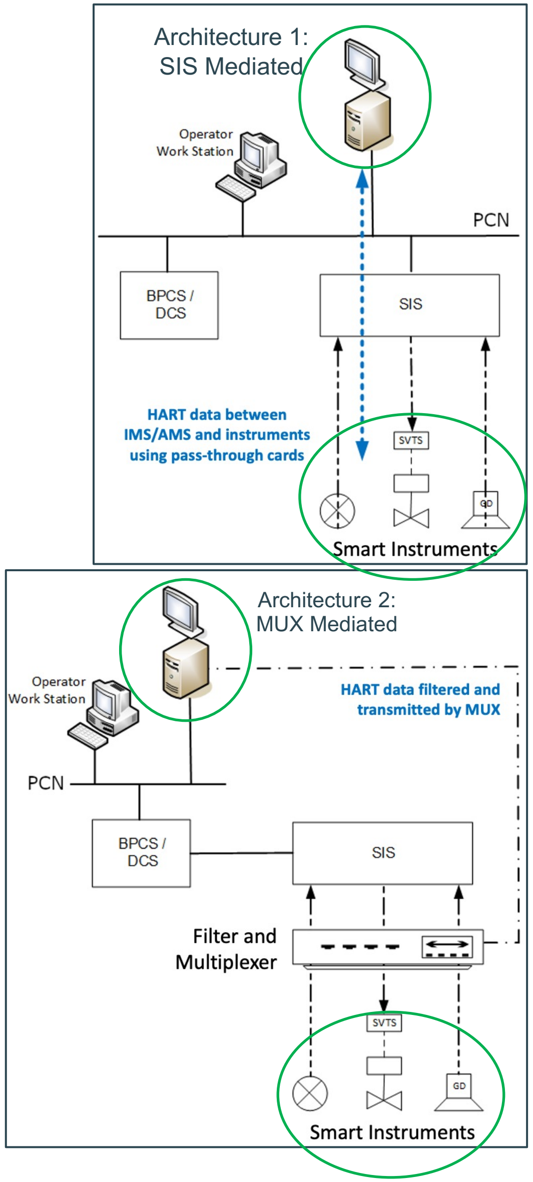
- Industrial Control Systems (ICS) control high-risk physical processes in manufacturing and industrial facilities
- Safety instrumented systems (SIS) are logic controllers with dedicated sensors that independently monitor ICS operations for unsafe conditions and take automated corrective actions to maintain safe state (“fail safe”)
- Used broadly across the globe in many contexts
- Main components frequently arranged into two common architectures
  - Safety Instrumented System or SIS (logic controller or brain)
  - Instruments (sensors, actuators)
  - Instrument or asset management console (IMS or AMS)
- Communicate using HART protocol via serial or via an IP wrapper (e.g., HART-IP) for IP network communications (depends on the system architecture)

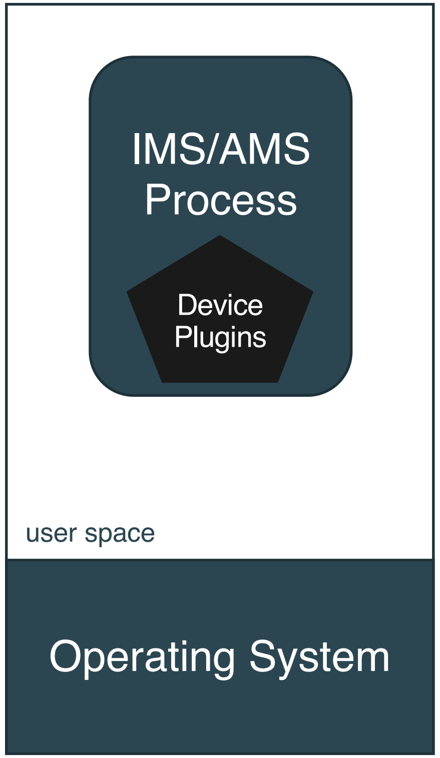

Architecture 1:
SIS Mediated
Operator
Work Station
PCN
BPCS / DCS
SIS
HART data between IMS/AMS and instruments using pass-through cards
SVTS
GD
Smart Instruments


Architecture 2:
MUX Mediated

What is a Safety Instrumented System?

- Industrial Control Systems (ICS) control high-risk physical processes in manufacturing and industrial facilities
- Safety instrumented systems (SIS) are logic controllers with dedicated sensors that independently monitor ICS operations for unsafe conditions and take automated corrective actions to maintain safe state (“fail safe”)
- Used broadly across the globe in many contexts
- Main components frequently arranged into two common architectures
  - Safety Instrumented System or SIS (logic controller or brain)
  - Instruments (sensors, actuators)
  - Instrument or asset management console (IMS or AMS)
- Communicate using HART protocol via serial or via an IP wrapper (e.g., HART-IP) for IP network communications (depends on the system architecture)

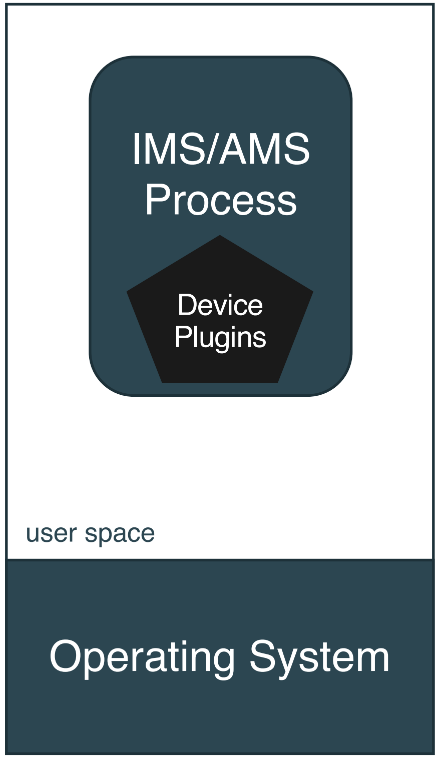




Safety System Trusted Platform

What software is used on management consoles?

- Base operating system
- Vendor device management product
- Device plugins that enable the vendor software to control unique features in 3rd party devices
  - Device Description (DD) files OR
  - Device Type Manager (DTM) packages



Safety System Trusted Platform

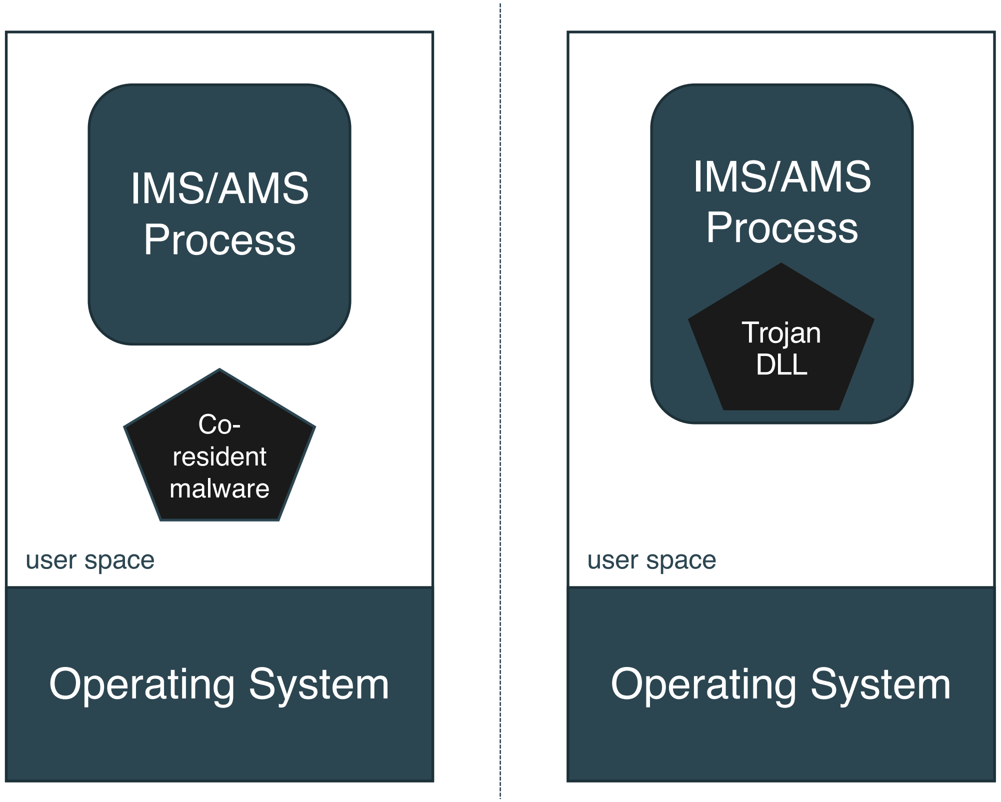
What supply chain attack opportunities exist?

- Base operating system (Windows)
  - Vendor certifies MS updates OR
  - Updates provided directly from vendor
- Vendor IMS/AMS product
  - Updates provided directly from vendor
  - Integrity protections unknown
- DDs and DTMs (of those tested)
  - Packages typically provided on device vendor web sites
  - Packages have few or no integrity protections
  - Operator downloads, puts on thumb drive (assuming console doesn’t have Internet access), installs using Administrator account

Operators implicitly trust vendors

Why are DDs and DTMs attractive to attackers?

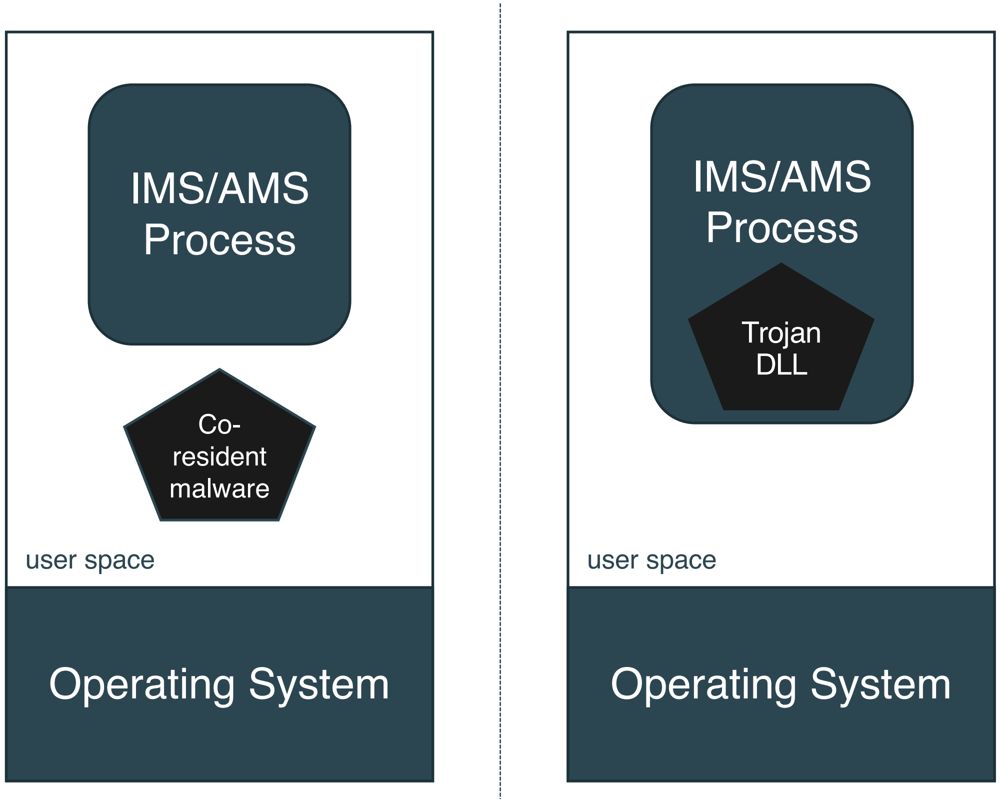
- Relatively easy to compromise
- Administrative privilege required to install DDs and DTMs
- Malicious software can be easily installed along with legitimate software
  - Malware executables along side legitimate software files
  - Trojan configuration files
  - Malware that runs directly in the process space of the trusted device manager



Safety System Trusted Platform

Why are DDs and DTMs attractive to attackers?

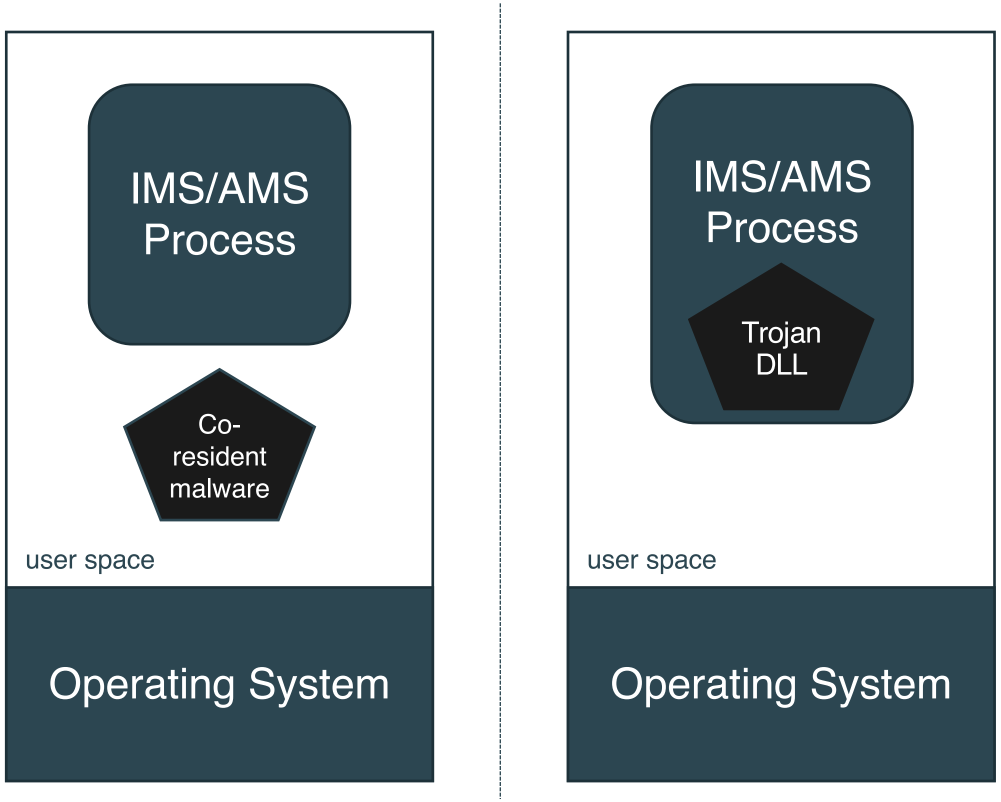
- All tested IMS/AMS solutions loaded DTMs and DDs without first checking their integrity
- Allows attacker to gain a foothold on a trusted platform and bypass most existing security controls



Safety System Trusted Platform

Why are DDs and DTMs attractive to attackers?

- All tested IMS/AMS solutions loaded DTMs and DDs without first checking their integrity
- Allows attacker to gain a foothold on a trusted platform and bypass most existing security controls; can be used
- We created and inserted trojan DDs and DTMs that successfully altered device configurations for 78% of tested devices



Safety System Trusted Platform

CRITICAL FINDING

“The practiced method of distributing and installing device type manager (DTM) software opens the door to supply chain attacks and thus [when combined with other findings] *poses significant risk to IMS/AMS platforms. These platforms are trusted and can be used as a launch point for device attacks.”*

What can be done by using malware on the IMS platform and exploiting the trust relationship?

- In the absence of device hardware write protection or other non-bypassable protective measures, attackers can execute any device-supported HART command at will from the IMS/AMS host platform

Configurations	States	Reset/Evasion
Password and pin code values	Disable write protect	Wipe device alert logs
Alarm settings	Enable write protect	Wipe device history
Valid range limits	Force offline	Reset device change bit
Scaling factors	Put in firmware upgrade mode	
Valve high-low cut off values	Conduct partial stroke test	
Valve positioner feedback values	Put in fixed current mode	
Relay latching behavior	Put in loop current mode	
Partial stroke values	Reset device repetitively	
Positioner calibration	Value position (override)	
Polling address		

- What can be done depends on the commands implemented by each device
- Multiple commands can be combined to create a greater effect

Additional Information

LOGIIC Safety Instrumentation and Management Technical Report

Available at https://LOGIIC.org

“When Safety Instrument Control Goes Rogue”

Presented at ICS Joint Working Group (ICSJWG) Spring 2021

(Presentation currently unavailable)

LOGIIC Project 12: Safety Instrumentation Discussion

Published by S4 Events at https://www.youtube.com/watch?v=eZo6fAMSLzg

Getting to the HART of the Matter:

An Evaluation of Real-World Safety System OT/IT Interfaces, Attacks, and Countermeasures

Published at the 14th Cyber Security Evaluation and Test (CSET) workshop

https://cset21.isi.edu/papers/cset21-8.pdf

Safety Systems Already Under Attack

- Triton/Trisis – first spotted in **2017**, but believe attack was active in **2014**; used again in **2019**
- High profile, drawing attention to these systems
- Schneider Electric Triconex Safety System was target
  - Attacker goal: cause process shutdowns, tamper with safety systems
  - Method: breach business net, pivot to OT engineering workstation
  - Code can disable safety systems designed to prevent catastrophic industrial accidents
- FireEye linked Triton to Russia's Central Scientific Research Institute of Chemistry and Mechanics research lab, based in Moscow, with "high confidence."
- Sources
  - https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/
  - https://www.zdnet.com/article/us-treasury-sanctions-russian-research-institute-behind-triton-malware/
  - https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/
  - https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/
  - https://www.scmagazine.com/home/security-news/malware/second-triton-trisis-critical-infrastructure-attack-spotted/

TECHNOLOGY

Trisis has the security world spooked, stumped and searching for answers

(CyberScoop/Jolie Gender)

Written by Chris Bing

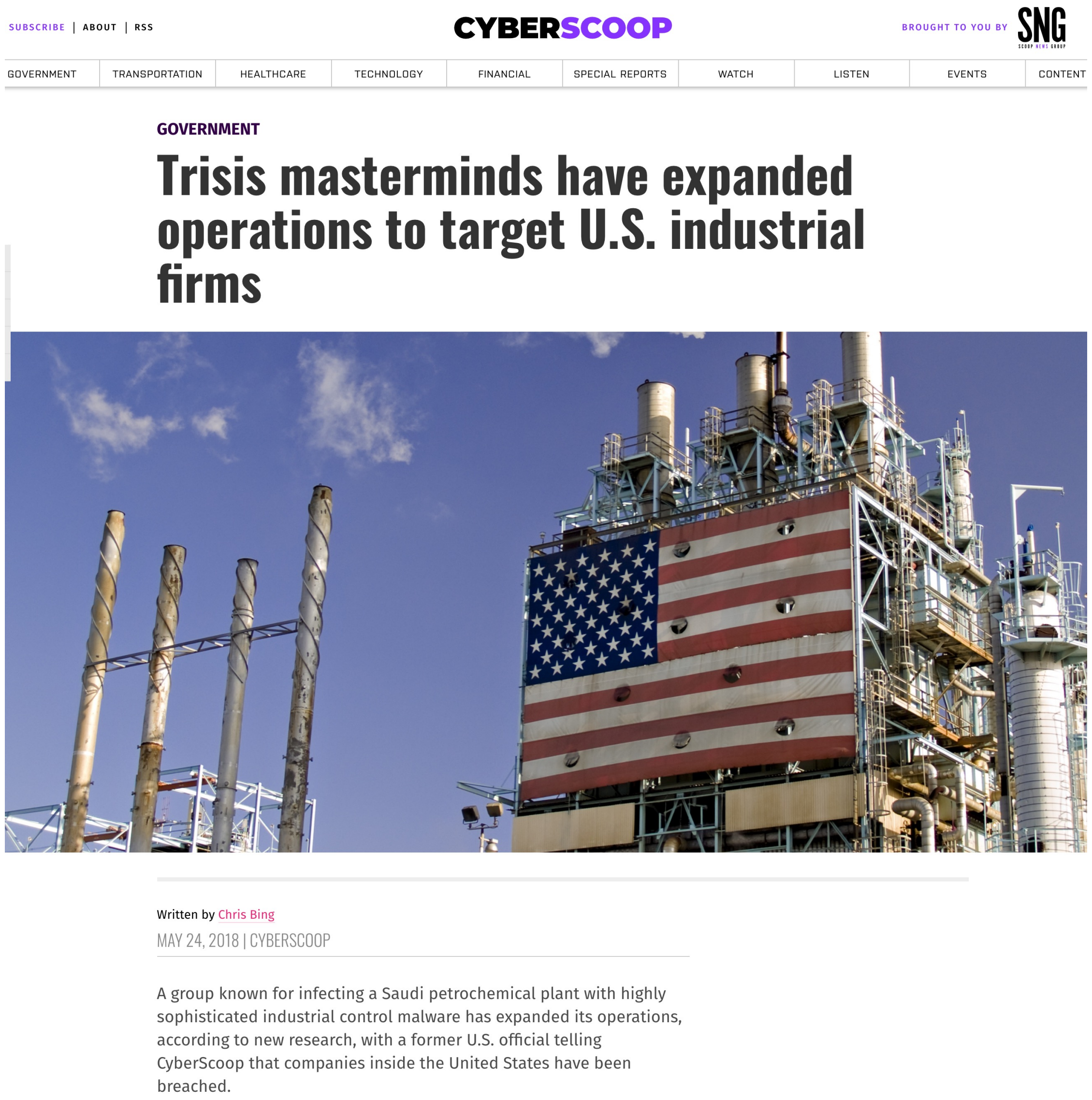
JAN 16, 2018 | CYBERSCOOP

At first, technicians at multinational energy giant Schneider Electric thought they were looking at the everyday software used to manage equipment inside nuclear and petroleum plants around the world. They had no idea that the code carried the most dangerous industrial malware on the planet.

Continued Attacks on SIS

2018

- “Group known for infecting a Saudi petrochemical plant with highly sophisticated industrial control malware has expanded its operations […] companies inside the United States have been breached
- While Trisis exploited one particular industrial control system, researchers say a new variant impacts a variety of safety instrumented systems
- “What is apparent, however, is that a dangerous and imminent threat looms over critical infrastructure providers inside the US”, Sergio Caltagirone, Dragos’s director of threat intelligence and analytics
- **Uses social engineering to breach admin accounts, traverses network looking for bridges to OT network**
- Sources
  - https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/



GOVERNMENT

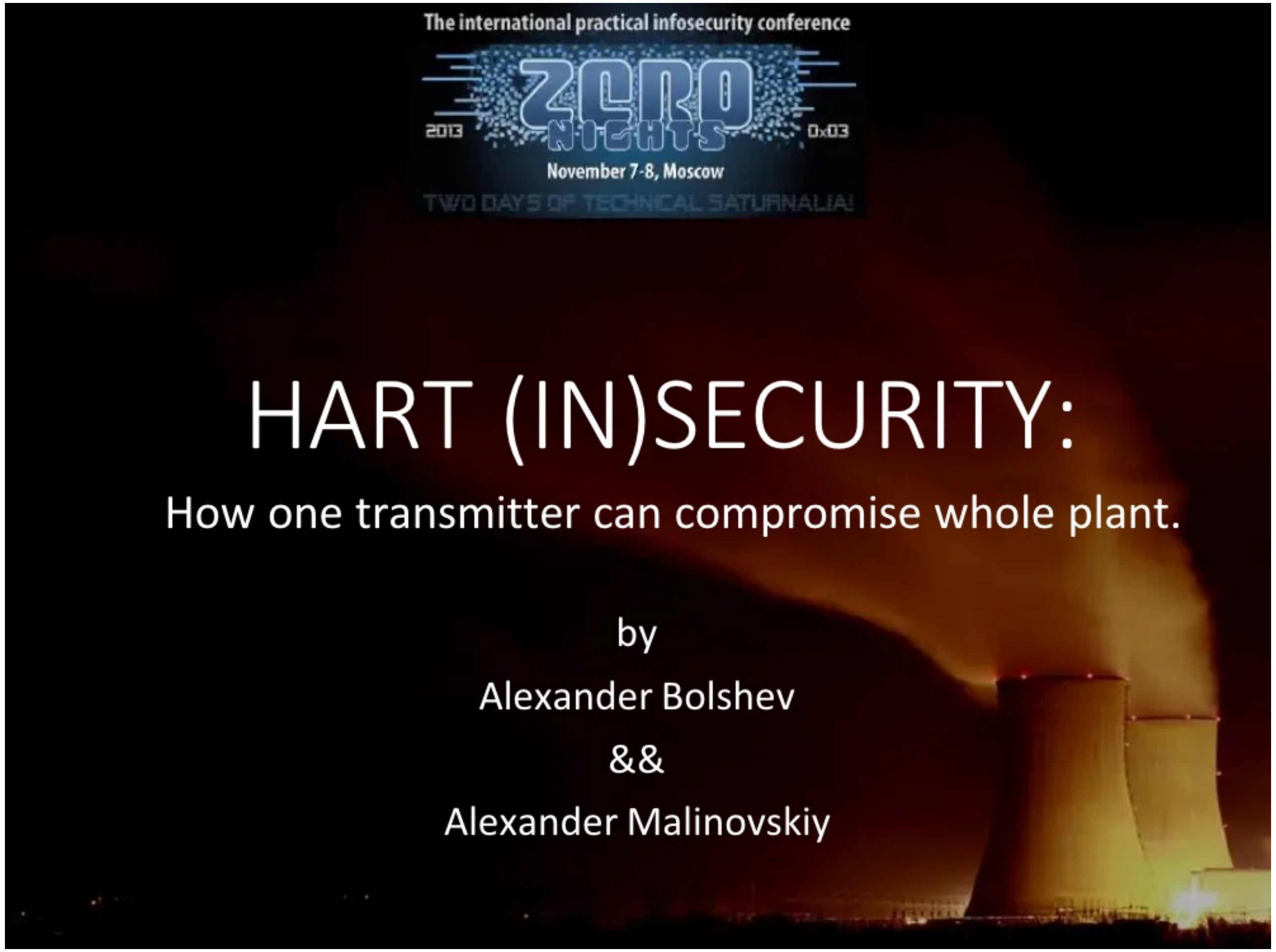
Trisis masterminds have expanded operations to target U.S. industrial firms

Written by Chris Bing

MAY 24, 2018 | CYBERSCOOP

A group known for infecting a Saudi petrochemical plant with highly sophisticated industrial control malware has expanded its operations, according to new research, with a former U.S. official telling CyberScoop that companies inside the United States have been breached.

Related Work by Russian Vulnerability Researcher (circa **2013**)



The international practical infosecurity conference

ZERO NIGHTS

2013 0x03

November 7-8, Moscow

TWO DAYS OF TECHNICAL SATURNALIA!

HART (IN)SECURITY:

How one transmitter can compromise whole plant.

by

Alexander Bolshev

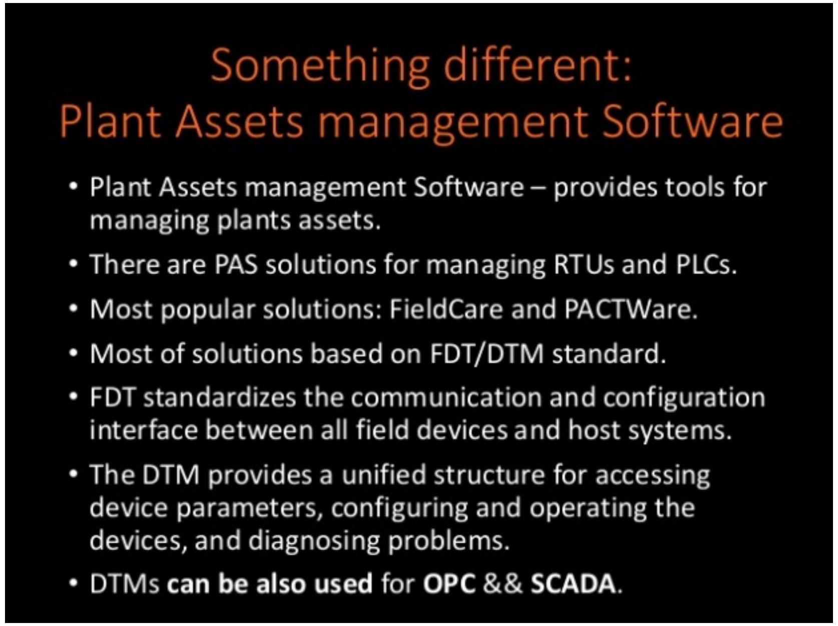
&&

Alexander Malinovskiy

- HART & HART-IP protocol analysis
- Fuzzing device inputs
- Using DTMs to target device management console input parser errors

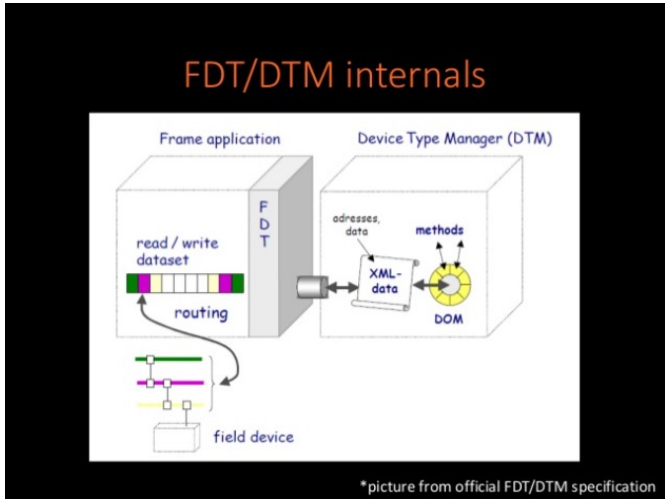
- @dark_k3y, DEFCON Moscow
- https://www.scribd.com/document/274365753/HART-in-Security
- https://www.slideshare.net/DefconRussia/alexander-bolshev-alexander-malinovsky-hart-insecurity

Related Work by Russian Vulnerability Researcher (circa **2013**)



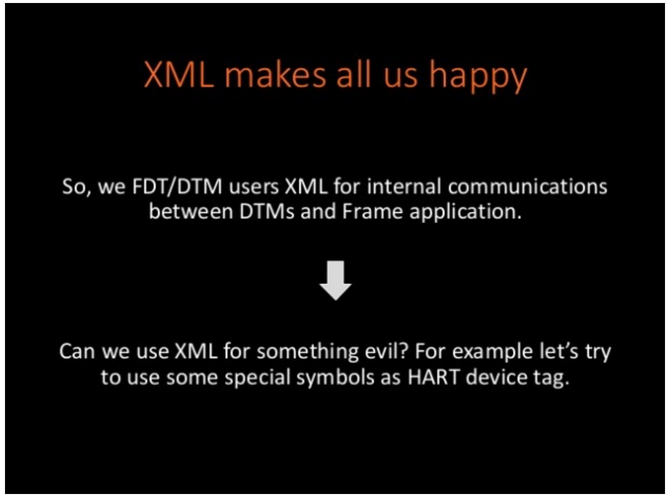
Something different: Plant Assets management Software

- Plant Assets management Software – provides tools for managing plants assets.
- There are PAS solutions for managing RTUs and PLCs.
- Most popular solutions: FieldCare and PACTWare.
- Most of solutions based on FDT/DTM standard.
- FDT standardizes the communication and configuration interface between all field devices and host systems.
- The DTM provides a unified structure for accessing device parameters, configuring and operating the devices, and diagnosing problems.
- DTMs **can be also used** for **OPC && SCADA**.



FDT/DTM internals

*picture from official FDT/DTM specification

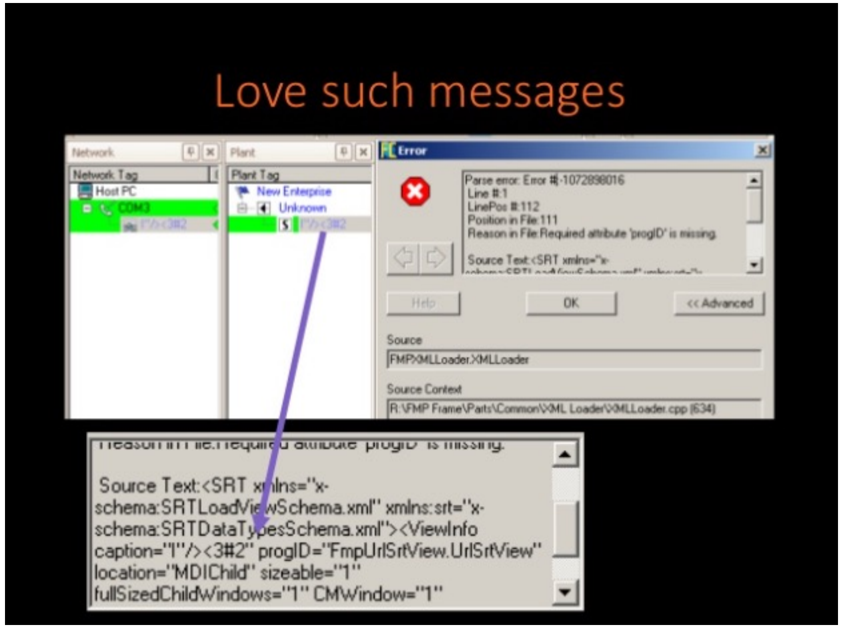


XML makes all us happy

So, we FDT/DTM users XML for internal communications between DTMs and Frame application.

⬇

Can we use XML for something evil? For example let's try to use some special symbols as HART device tag.



Love such messages

```
Parse error: Error #-1072898016
 Line #:1
 LinePos #:112
 Position in File:111
 Reason in File:Required attribute 'progID' is missing.

 Source Text:<SRT xmlns="x-
```

Source
FMPXMLLoader.XMLLoader

Source Context
R:\FMP Frame\Parts\Common\XML Loader\XMLLoader.cpp (634)

```
Reason in File:Required attribute 'progID' is missing.

 Source Text:<SRT xmlns="x-
schema:SRTLoadViewSchema.xml" xmlns:srt="x-
schema:SRTDataTypesSchema.xml"><ViewInfo
caption="I"/><3#2" progID="FmpUrlSrtView.UrlSrtView"
location="MDIChild" sizeable="1"
fullSizedChildWindows="1" CMWindow="1"
```

- @dark_k3y, DEFCON Moscow
- https://www.scribd.com/document/274365753/HART-in-Security
- https://www.slideshare.net/DefconRussia/alexander-bolshev-alexander-malinovsky-hart-insecurity

Urgent Need: secure the safety system software supply chain to prevent potentially catastrophic industrial events

SRI International®

Laura S. Tinnel
laura.tinnel@sri.com