



CREDC

CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

Seminar Series

Industrial Cyber Threats and Future Planning



Robert M. Lee

Twitter: [@RobertMLee](#)

Email: rlee@dragos.com

Web: www.dragos.com



Agenda

- Where We Are
 - Selected Case Studies in Cyber Attacks
- Where We're Heading
- Recommendations

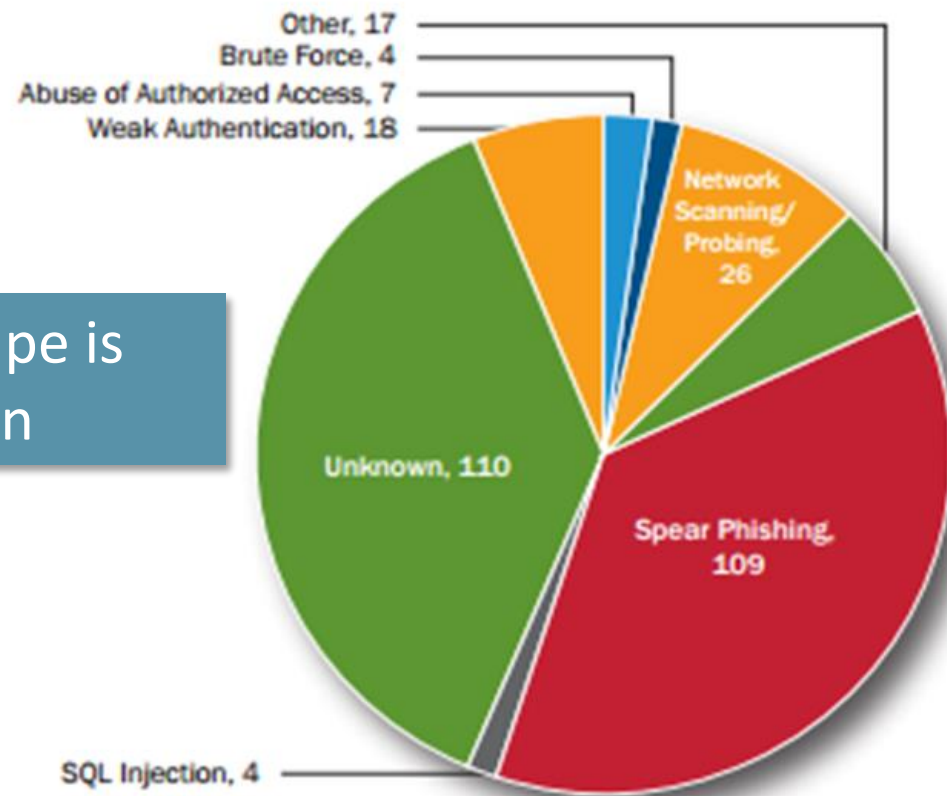
The Unknown Threat Landscape

Few People Know How to Protect the ICS that Run Our World

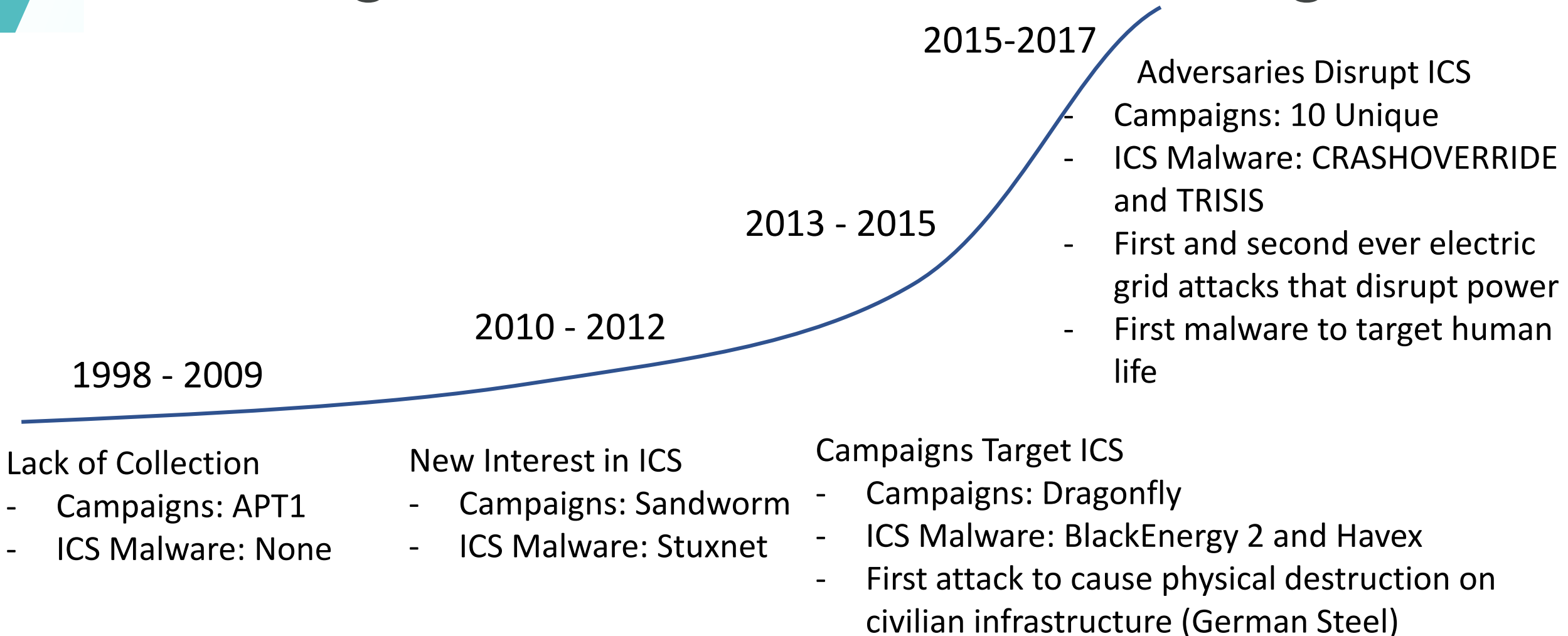


The Threat Landscape is Mostly Unknown

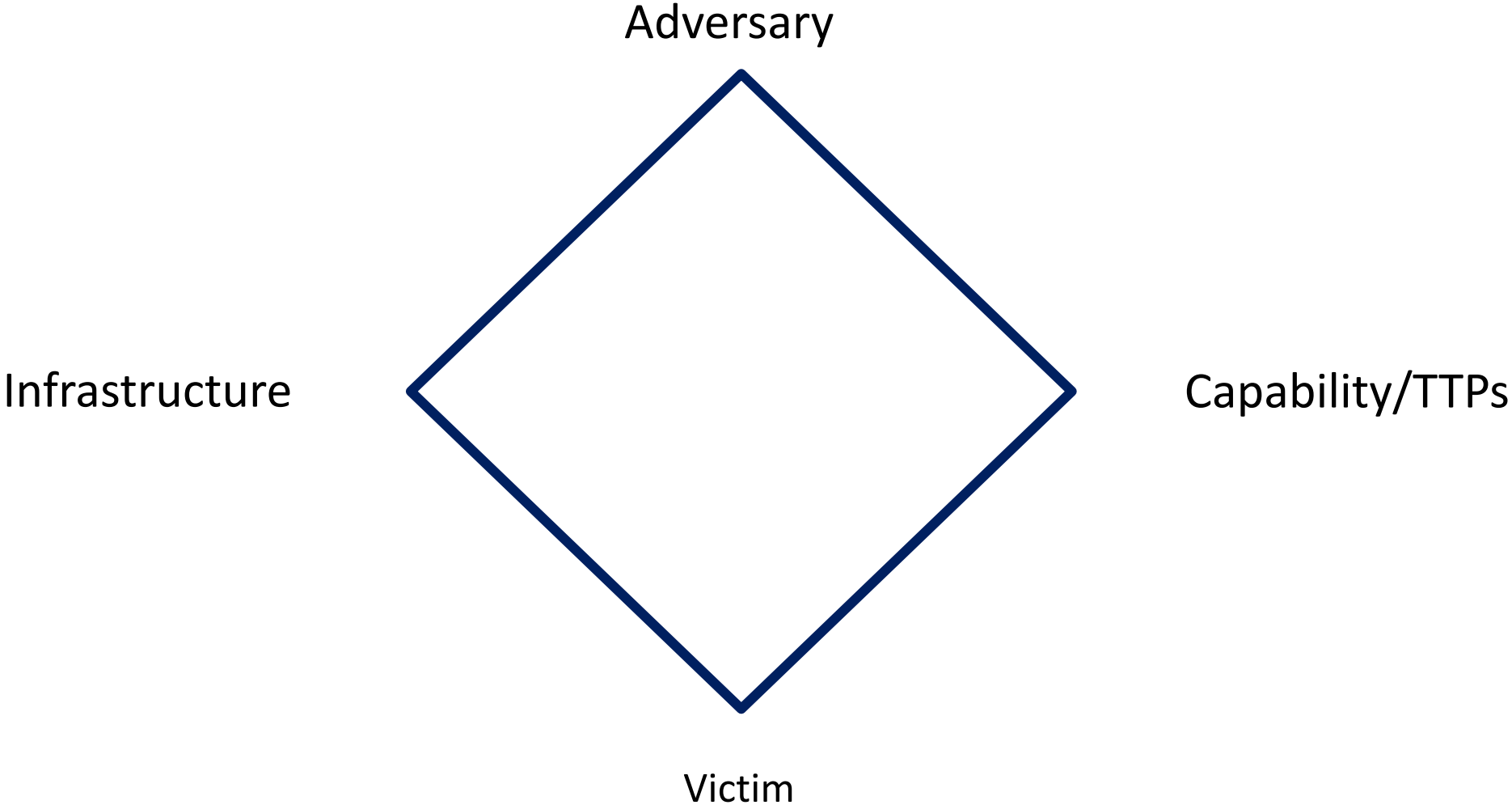
FY 2015 Incidents by Infection Vector (295 total)



Finding More and More Occurring

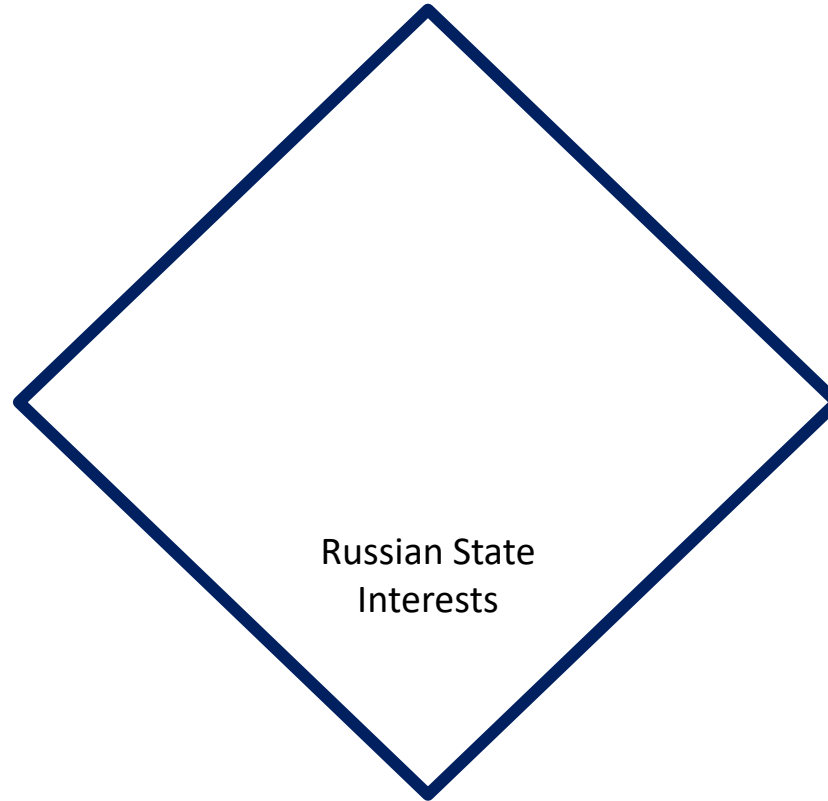


The Diamond Model





ELECTRUM

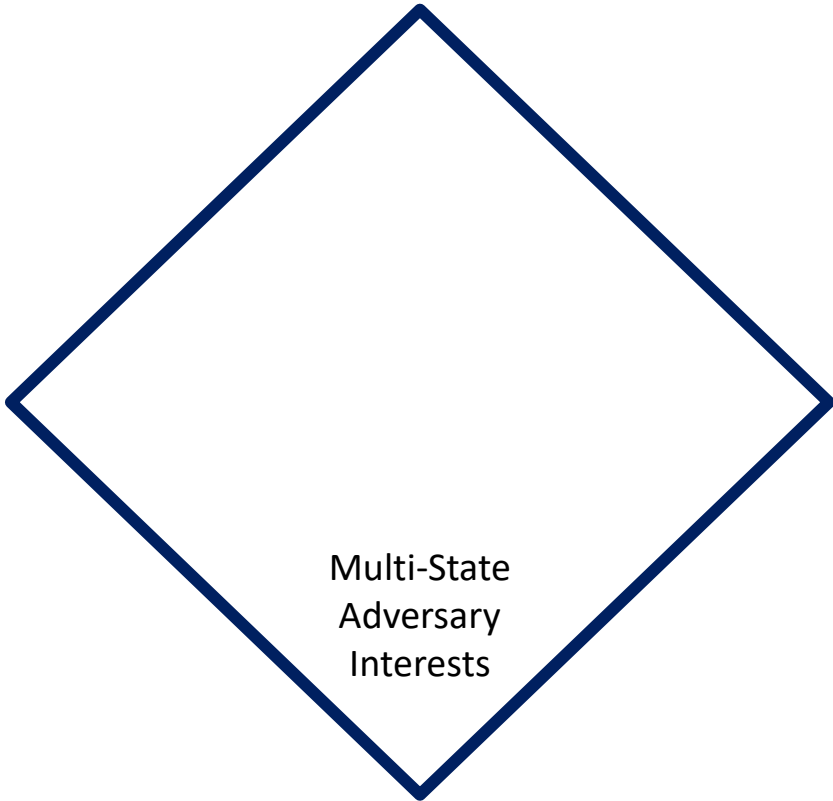


- Dual-use infrastructure such as TOR to host C2
- Internal proxies setup

- Long term access to ICS
- CRASHOVERRIDE
- ICS Specific Modules
- Operations Knowledge

- Ukrainian Utility Companies
 - Electric
 - Water

DYMALLOY

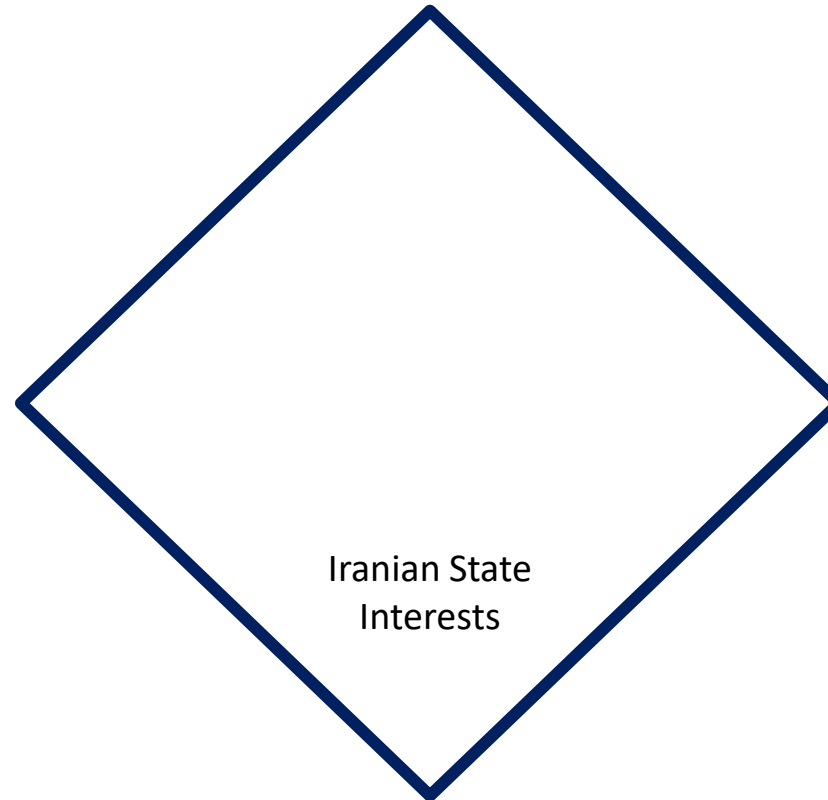


- Compromise ISP IPs
- Compromised business connections for initial infection and subsequent implants

- Malicious docs w/ credential harvesting via external SMB connections
- RATs from publicly available toolkits
- Custom-developed information theft toolkits built on public tools
- One non-public toolkit

- North American electric operators
- Turkish energy providers
- Western Europe electric operators

CHRYSENE

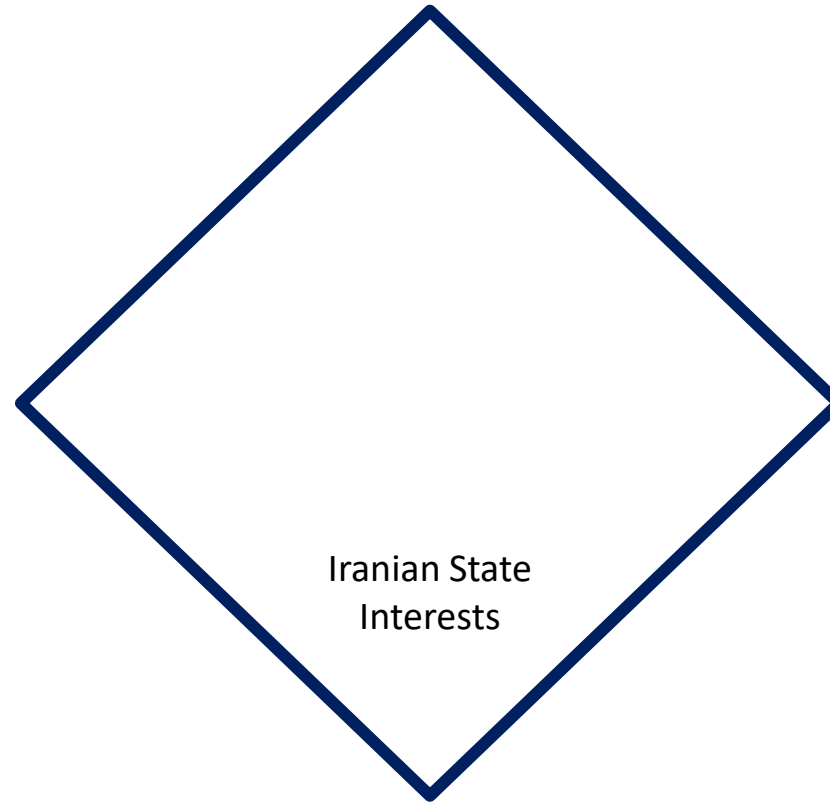


- Actor owned infrastructure
- Domain patterns after legitimate resources
- Custom DNS server as authoritative for the domain to enable C2

- 64-bit malware using DNS for C2
- Greenbug malware with HTTP C2
- OilRig as evolution of Greenbug
- Unique DNS C2 system
 - Initial beacon AAAA request
 - IPv6 encoded commands

- Arabian gulf region
- Saudi Arabia petrochemical focus
- Oil/gas, petro, and electric generation

MAGNALIUM



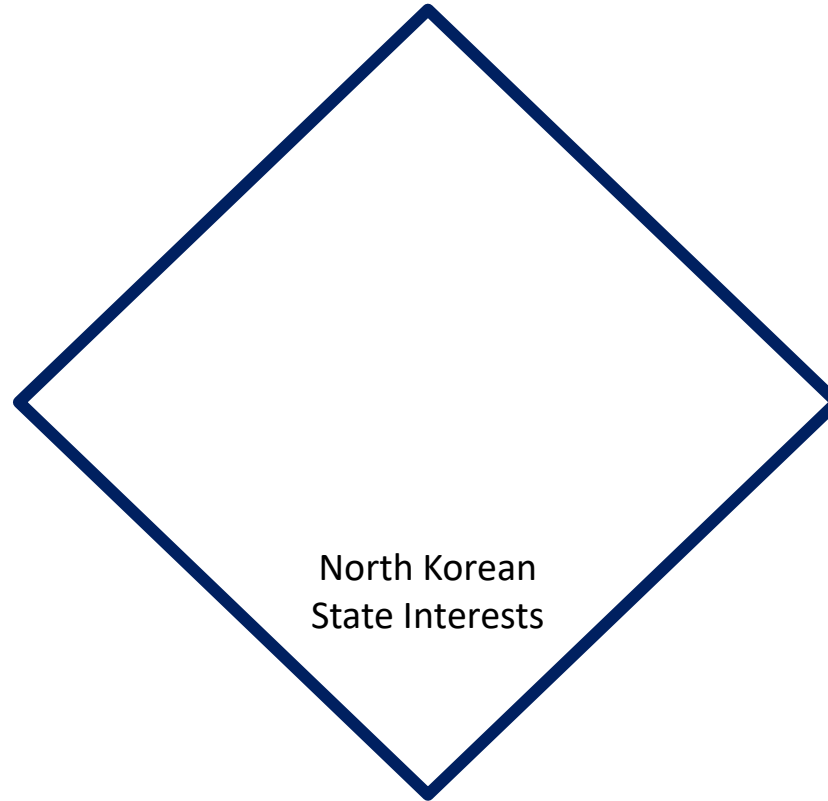
- Spoofed domains of relevance to victim
- Dynamic DNS for C2
- IT services and aerospace themed

- Commodity and non-public malware combination
- Publicly available crimeware
- Specific malware encoding routine

- Saudi Arabian petrochemical
- Aerospace companies
- North America and South Korean targets only with Saudi business



COVELLITE



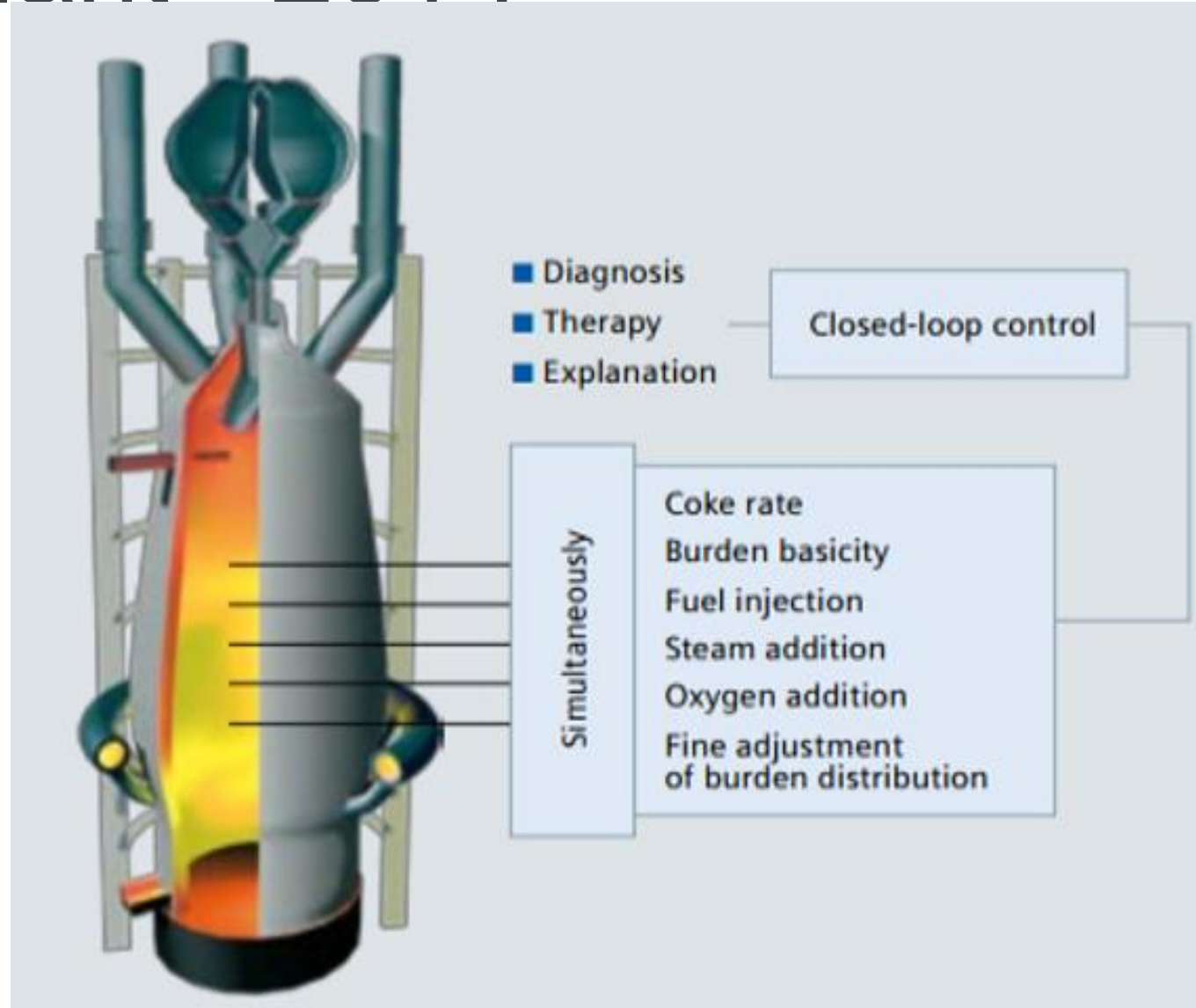
- Legitimate infrastructure
- University IPs for C2

- Sophisticated implant with secure communication channels
- Similar features to malware used against South Korean targets
- Specific session key used for payload and second encrypted layer
- 41 minute and 30 second sleep

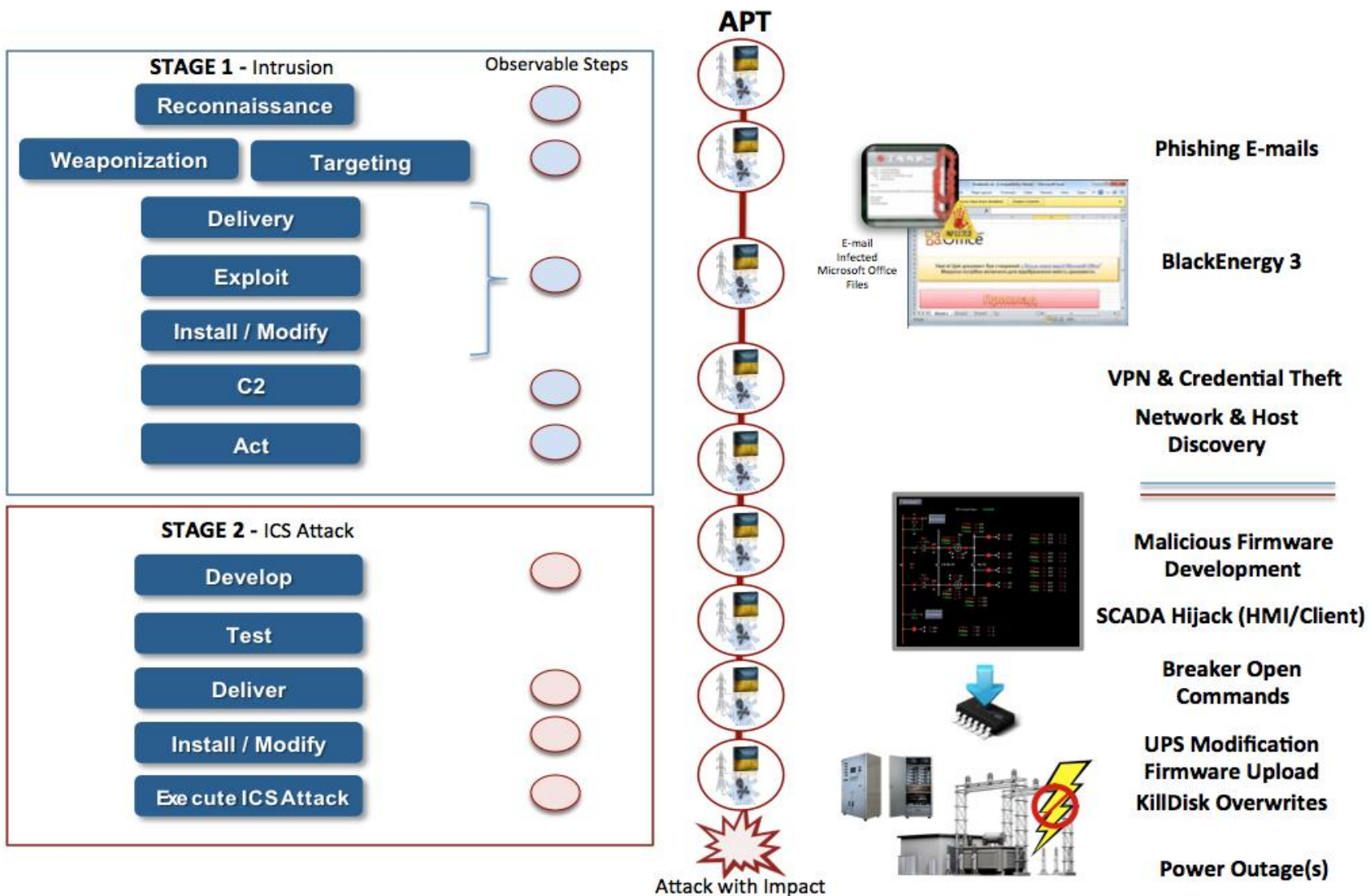
- Electric utility companies in the United States

German Steel Plant - 2014

- Dec 18, 2014 German Government's BSI released annual report highlighting incidents
- Identified "massive damage" in a steel facility due to a cyber attack
- 2nd publicly known case of physical damage to control systems from cyber attacks

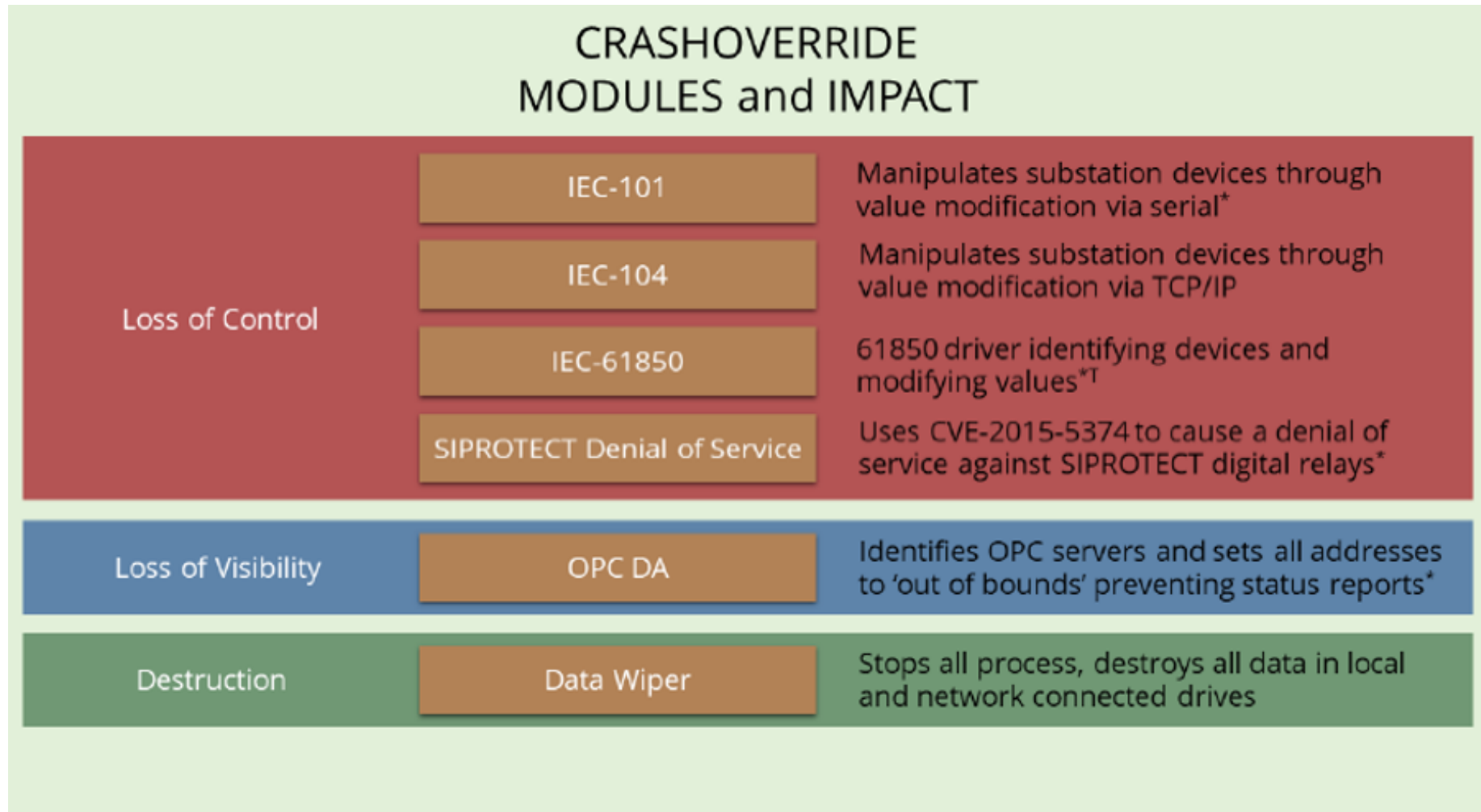


Ukraine 2015

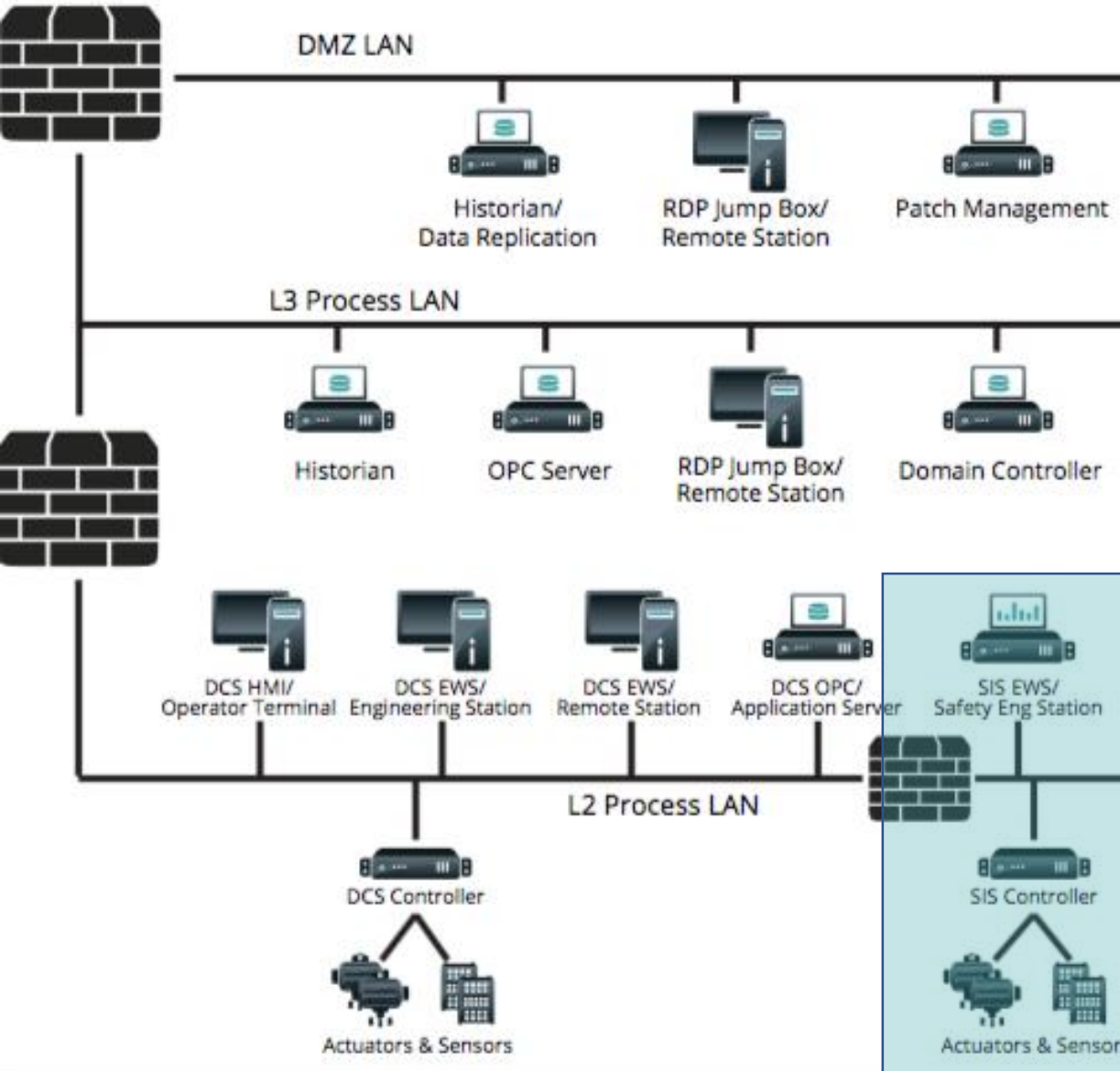


- 1st Ever cyber attack on a power grid to lead to outages
- 3 power companies across Ukraine
- SCADA Hijack scenario by a well funded team

Ukraine 2016 - CRASHOVERRIDE



Middle East 2017 - TRISIS



- TRISIS was delivered into a petrochemical facility in the Middle East by a well funded attack team
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- 1st malware to specifically target human life

You Cannot Just Patch Away the Problem

Dragos' 2017 in Review reports revealed that for ICS vulnerabilities:

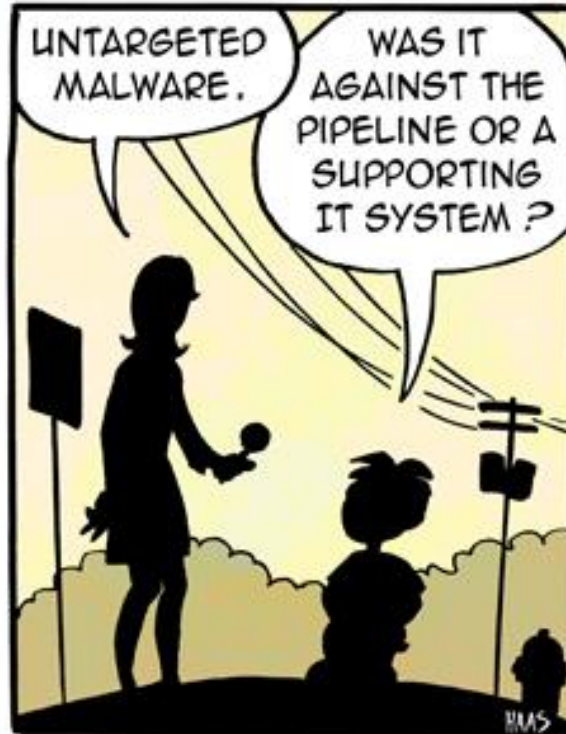
- 64% of all vulns didn't eliminate the risk
- 72% provided no alternate mitigation to the patch
- Only 15% could be leveraged to gain initial access



Where We're Heading

LITTLE BOBBY

by Robert M. Lee and Jeff Haas



ICS Incidental Impact vs. ICS-Tailored

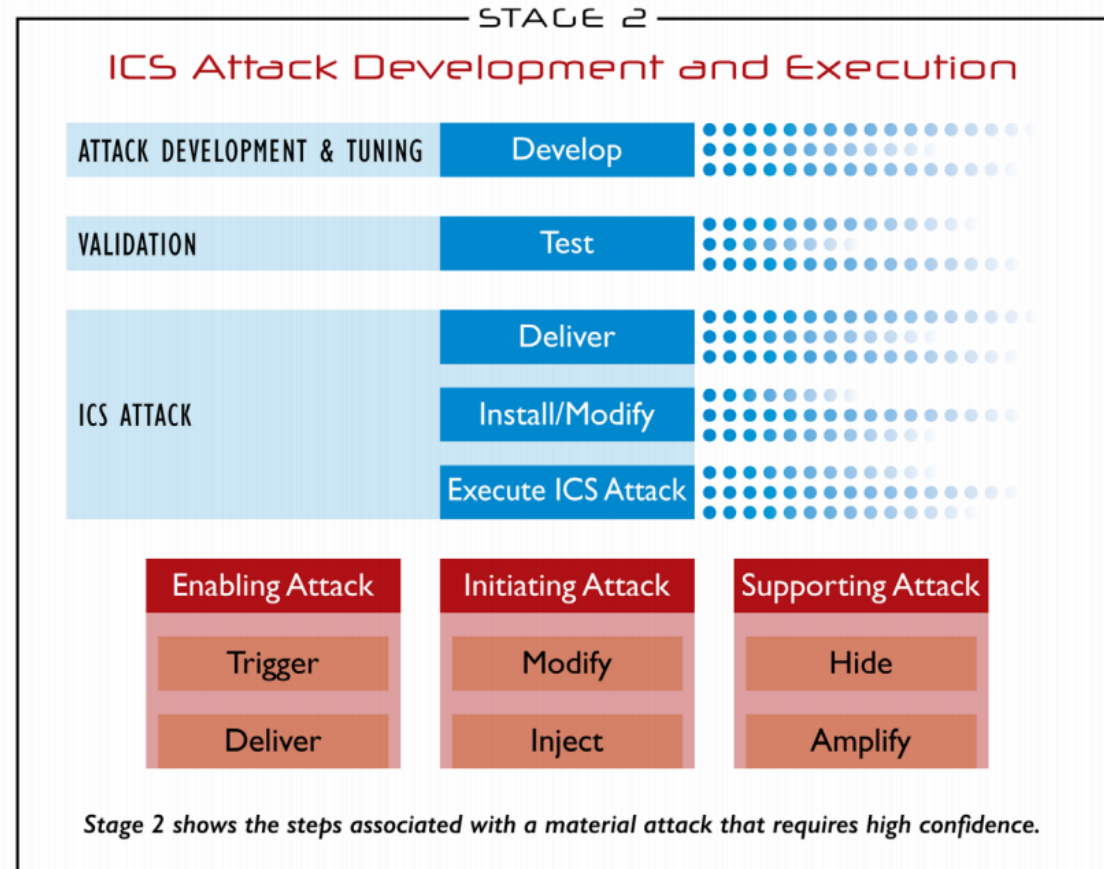
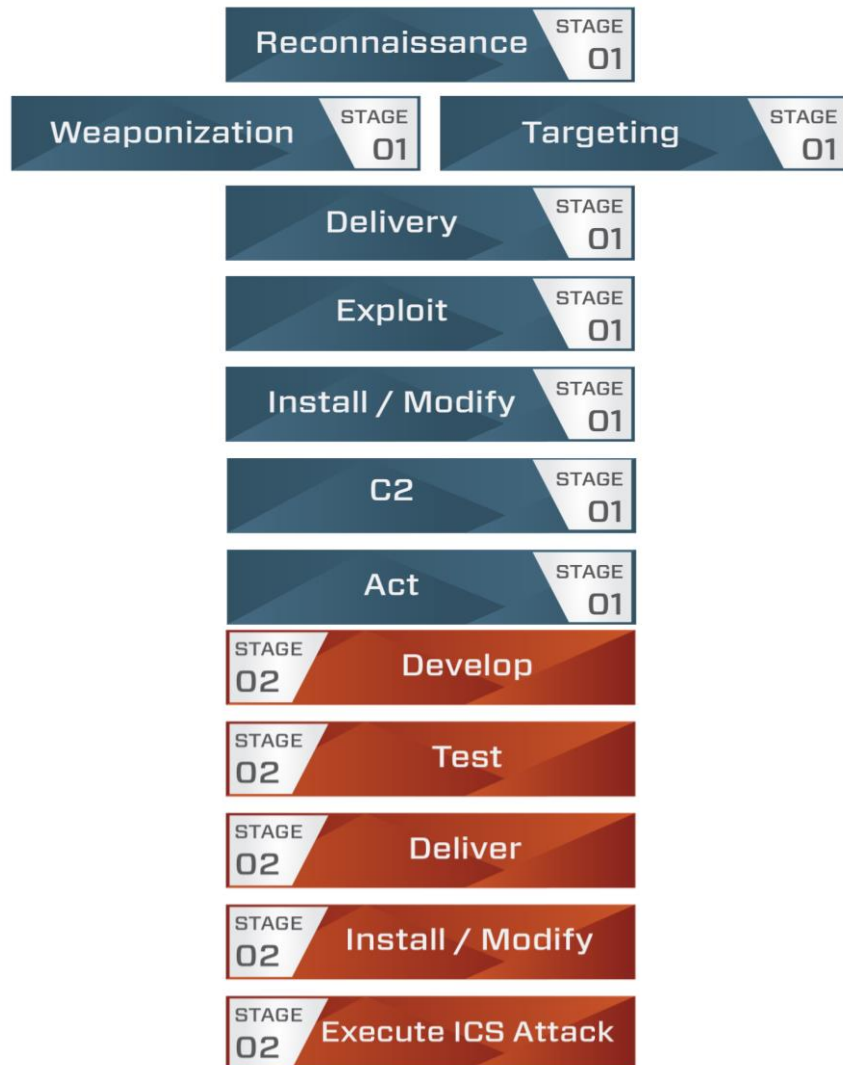
ICS Incidental Impact

- Resource Usage
- Destructive
- Wormable

ICS-Tailored

- Protocol Knowledge
- System Knowledge
- Process Knowledge

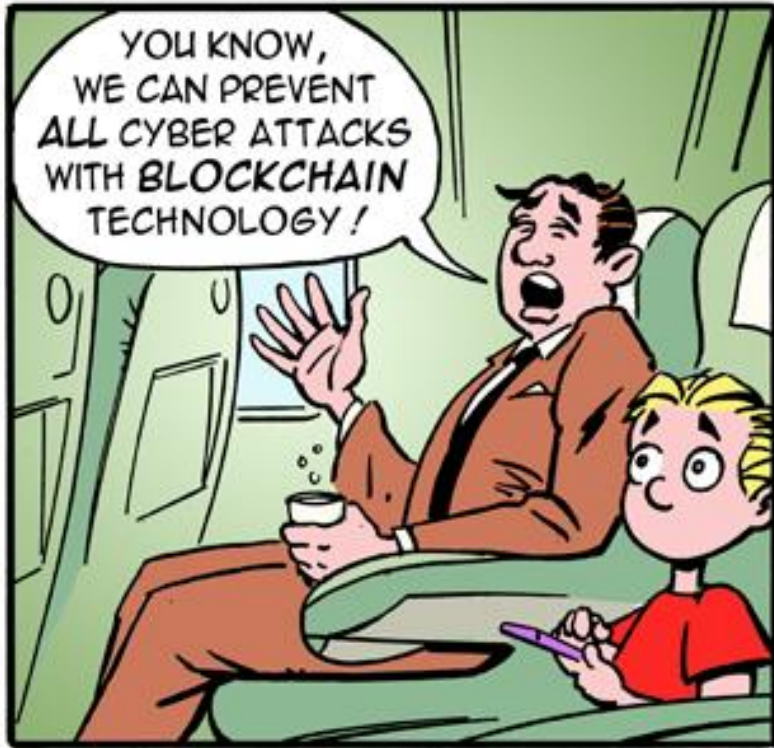
Multi-Phase Attacks



Ref: <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>

Research Ideas

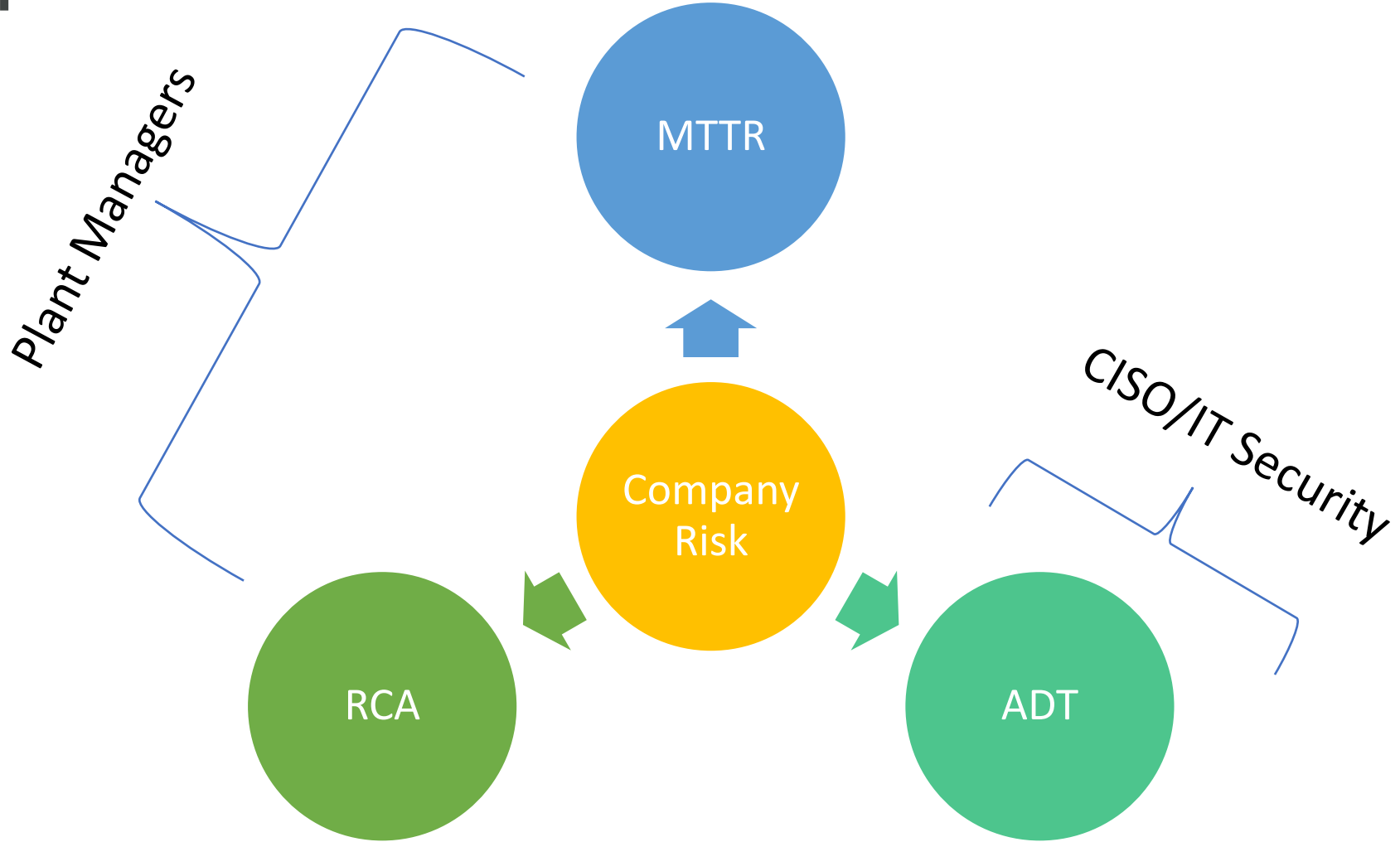
LITTLE BOBBY



by Robert M. Lee and Jeff Haas



Your Goal – Satisfy the Right Requirements





Problems



Problem: Rush for Sensors



Problem: Over-Focus on Malware, Vulns, and Exploits



Problem: Over-Focus on ML/AI Models



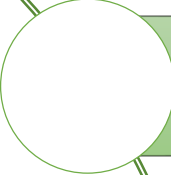
Problem: Need to Scale Knowledge/Workforce



Problem: Big Architecture Changes



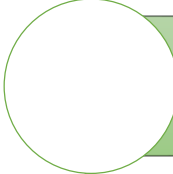
Ideas



Idea: Common, Robust, Dynamic Sensor



Idea: Limiting of Impact Outside Scope



Idea: Intelligence-Driven Approach



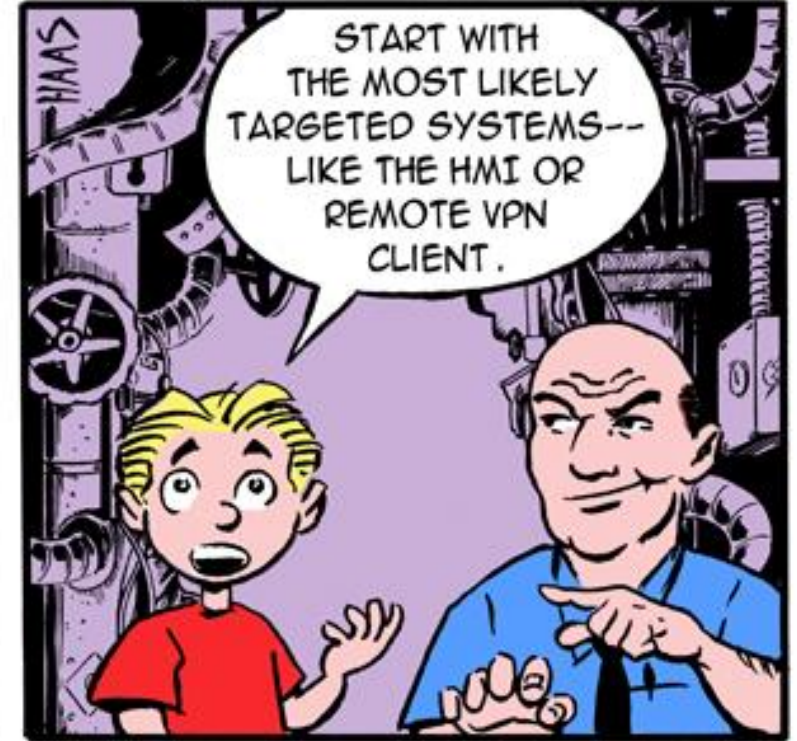
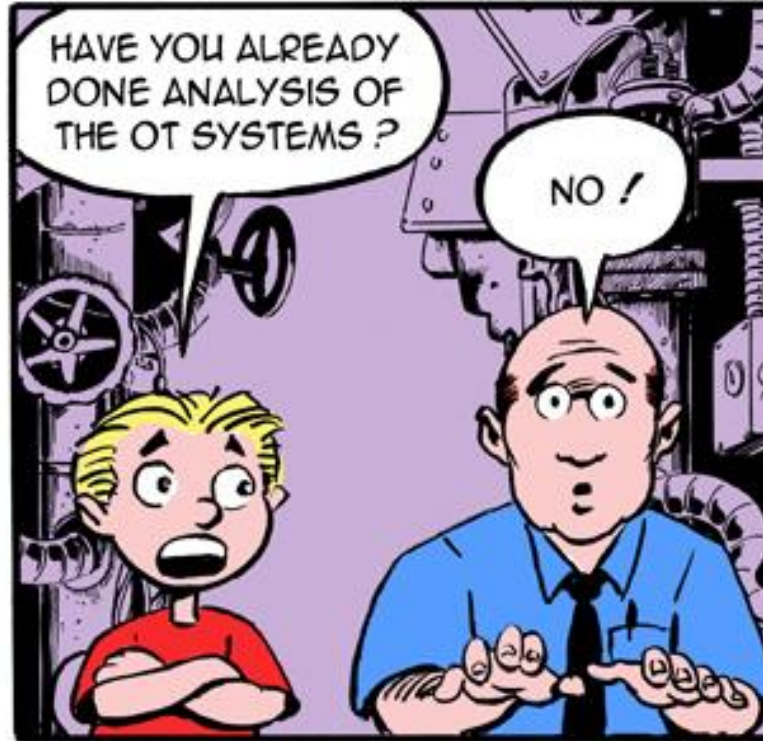
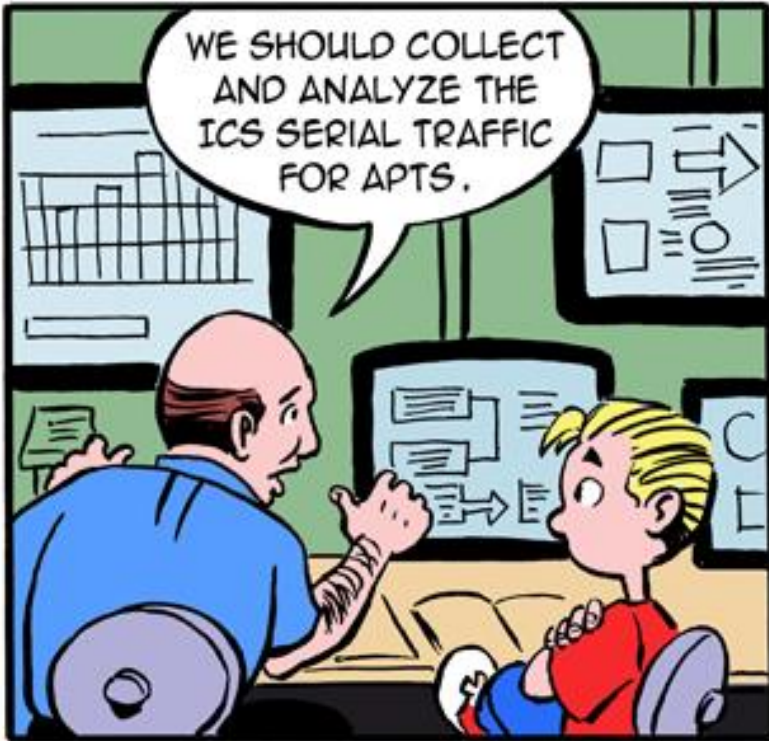
Idea: Enabling/Scaling Human Knowledge



Idea: Common Logging/API in OEM Gear

Questions?

LITTLE BOBBY



by Robert M. Lee and Jeff Haas