VEDERE LABS

OT:ICEFALL

Revisiting a decade of insecure-by-design practices in OT

Jos Wetzels
Security Researcher, Forescout

Agenda

1. Background
2. Overview
3. Analysis
4. Example Findings
5. Conclusions

VEDERE LABS

- Part of Forescout
  - Visibility, Assessment & Control platform
  - Enterprise, OT, IoT, IoMT, etc.

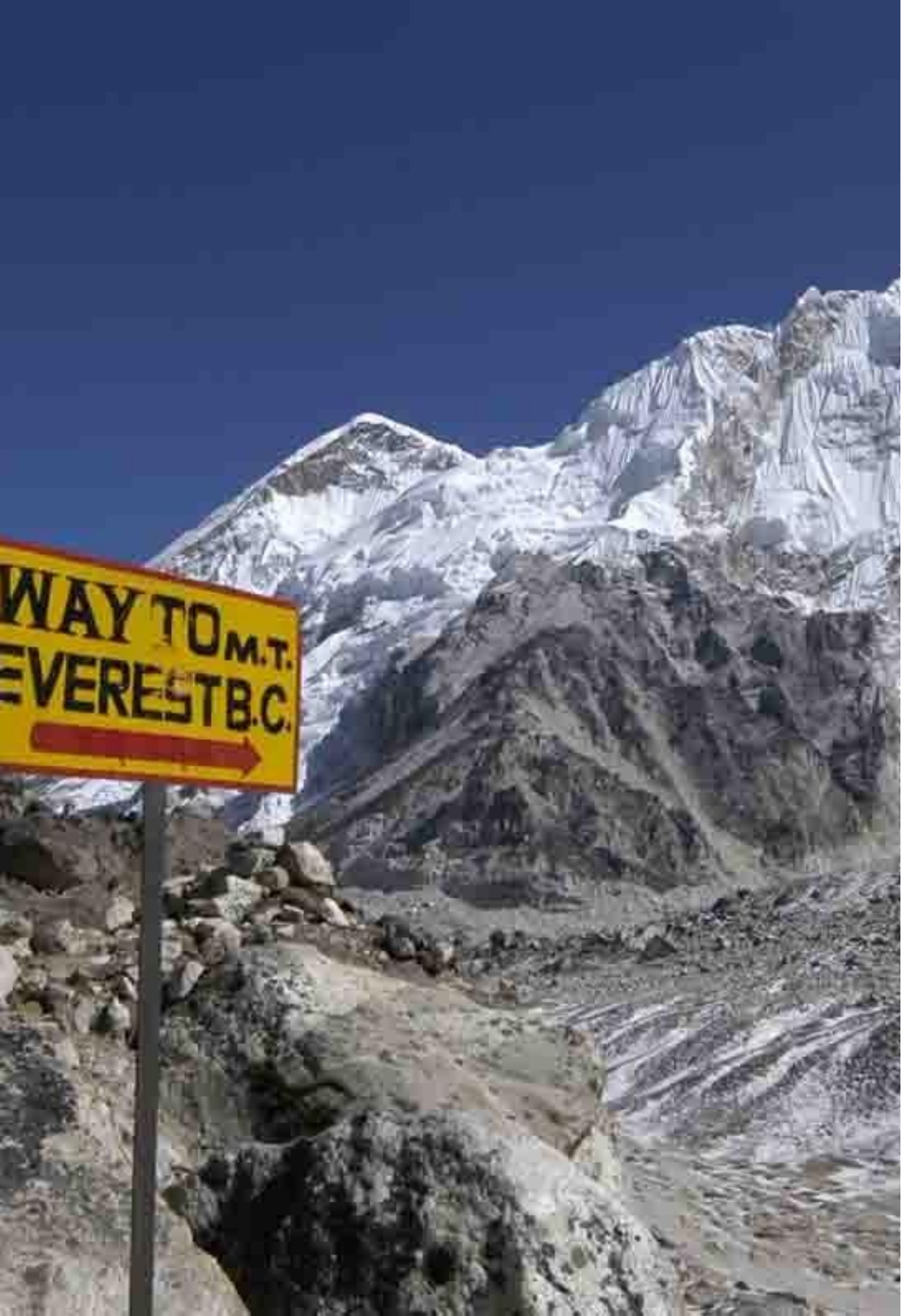
- Threat Intelligence & Vulnerability Research

- Project Memoria
  - 100+ vulnerabilities in 14 TCP/IP stacks affecting 500+ vendors and millions of devices

- Access:7
  - Medical Supply Chain vulnerabilities

- R4IoT
  - Ransomware PoC for IoT & OT

https://www.forescout.com/research-labs/



The long climb ahead

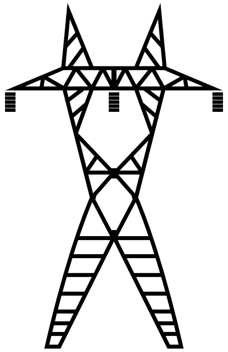
- 10+ years ago, Digital Bond's Project Basecamp[1], modeled after Firesheep, showed pervasiveness of **insecure-by-design** in ICS equipment
- Lack of basic security controls → historical deployment in trusted, air-gapped networks
- Advent of standards-driven security efforts
  - IEC 62443
  - NERC CIP
  - NIST SP 800-82
  - IEC 51408/CC
  - Etc.
- OT:ICEFALL[2] (after next stop on Mt. Everest) aims to be **checkup of progress** made & **diagnose impact**

[1] https://github.com/digitalbond/Basecamp
[2] https://www.forescout.com/resources/ot-icefall-report/

Real-World Attackers Abusing Insecure-by-Design

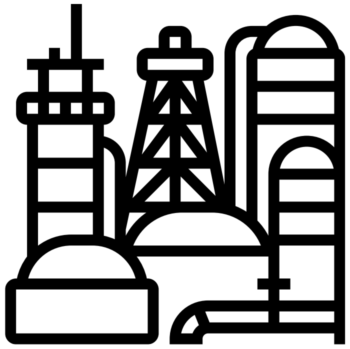
INDUSTROYER 1 & 2

- OT protocol capabilities
  - IEC-101/104
  - IEC-61850
  - OPC DA
- Attack on UA TSO in 2016
- Attempted attack on UA energy CI in 2022



TRITON

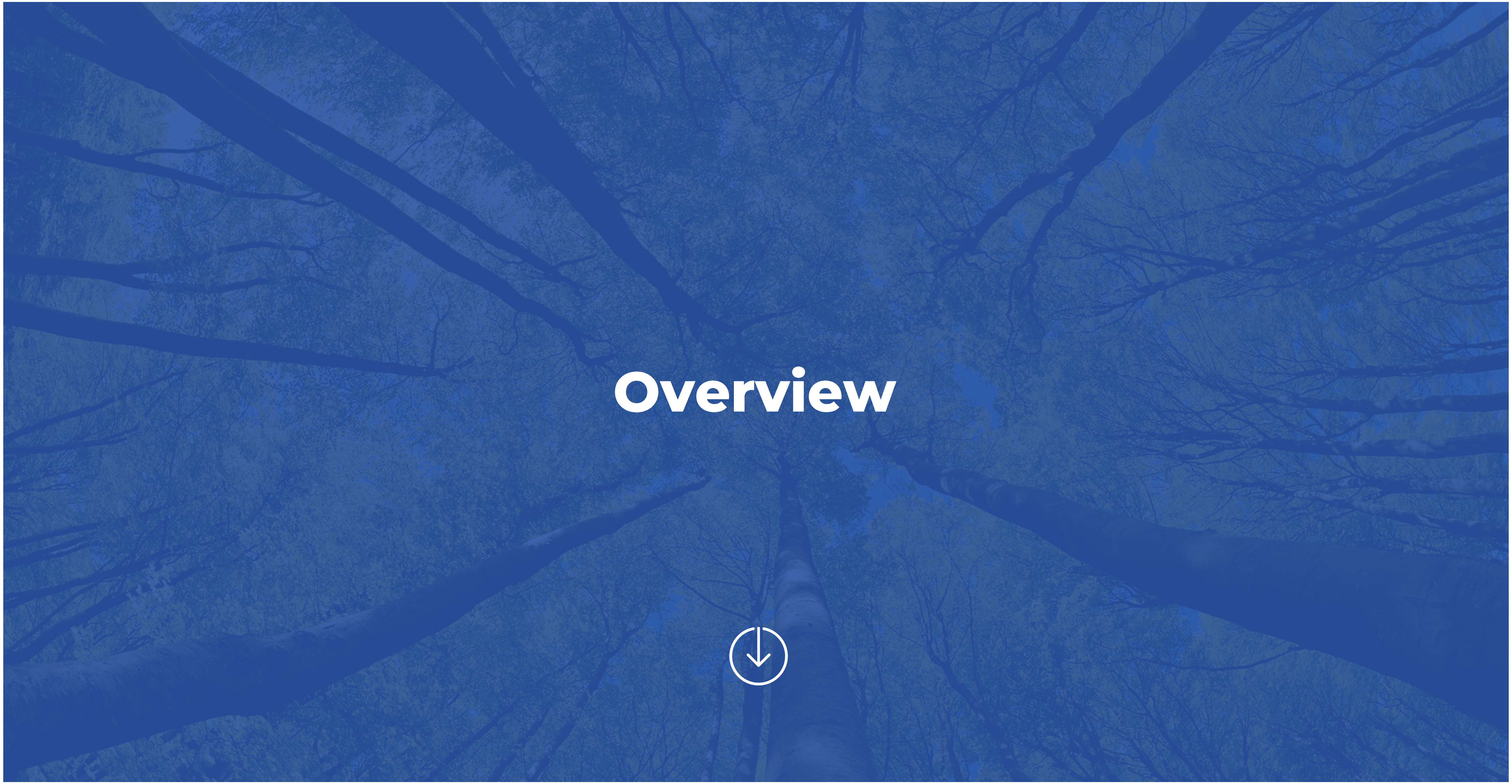
- OT protocol capabilities
  - SE TriStation
- OT implant capabilities
  - SE Triconex SIS
- Attack on SA petrochemical facility in 2017



INCONTROLLER

- OT protocol capabilities
  - Machine Expert Discovery
  - CODESYS V3
  - Modbus TCP
  - Omron FINS
  - OPC UA
- OT attack capabilities
  - SE Machine Expert PLCs
  - Omron SYSMAC N* PLCs
- Discovered in 2022 before deployment, rumored to target LNG & energy CI facilities

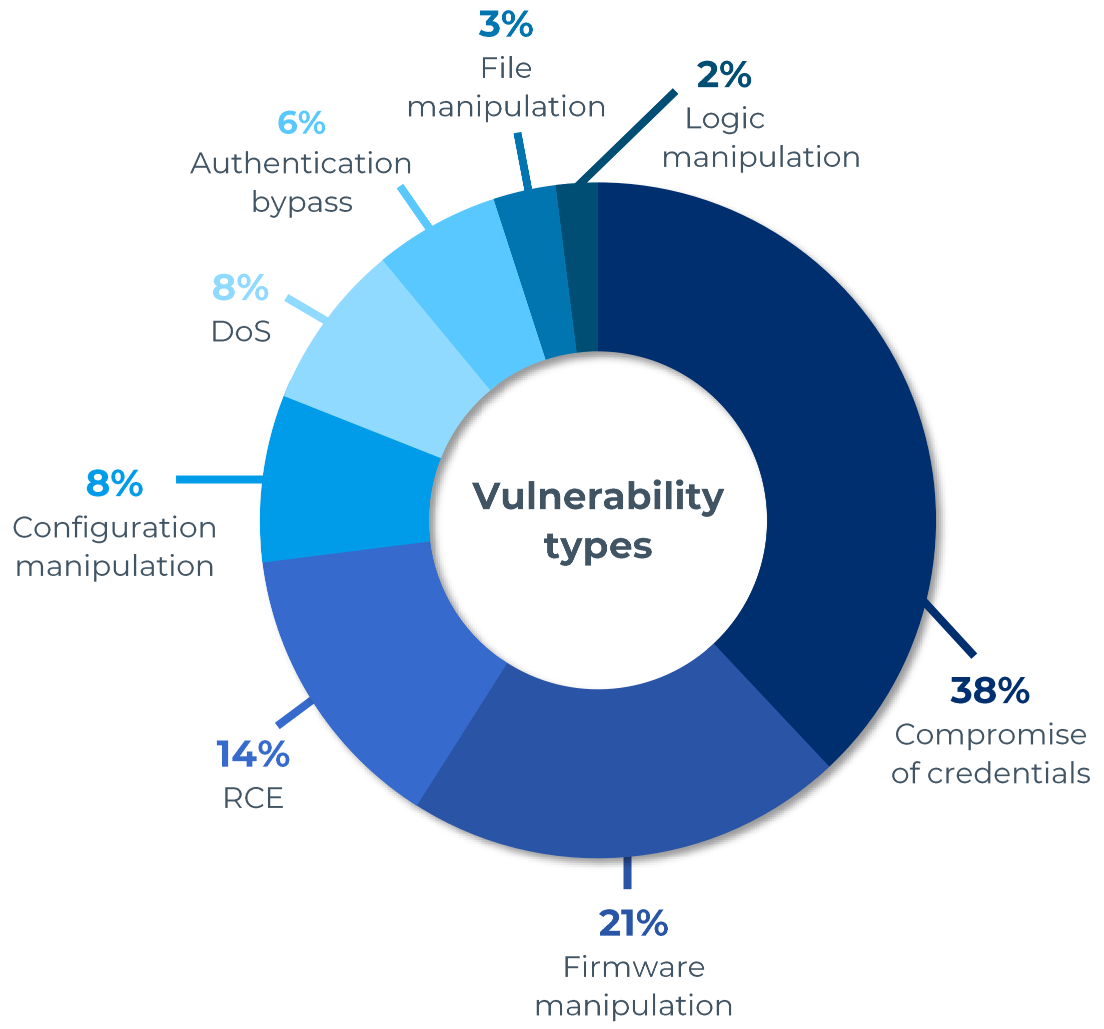
Overview



56 CVEs affecting 10+ vendors

Vendor	Model	Type
Bently Nevada	3700 / TDI	Condition Monitoring
Emerson	DeltaV	DCS
Emerson	Ovation	DCS
Emerson	OpenBSI	Engineering Workstation
Emerson	ControlWave, ROC	RTU
Emerson	FANUC / PACsystems	PLC
Honeywell	Trend IQ	Building Controller
Honeywell	Safety Manager / FSC	SIS
Honeywell	Experion LX	DCS
Honeywell	ControlEdge	RTU
Honeywell	Saia Burgess PCD	PLC
JTEKT	Toyopuc	PLC
Motorola	MOSCAD IP Gateway	Gateway
Motorola	MDLC	Protocol
Motorola	ACE1000	RTU
Motorola	MOSCAD Toolbox	Engineering Workstation
Omron	SYSMAC Cx/Nx	PLC
Phoenix Contact	ProConOS/eCLR	Runtime
Siemens	WinCC OA	SCADA
Yokogawa	STARDOM	PLC

Full overview: https://www.forescout.com/research-labs/ot-icefall/



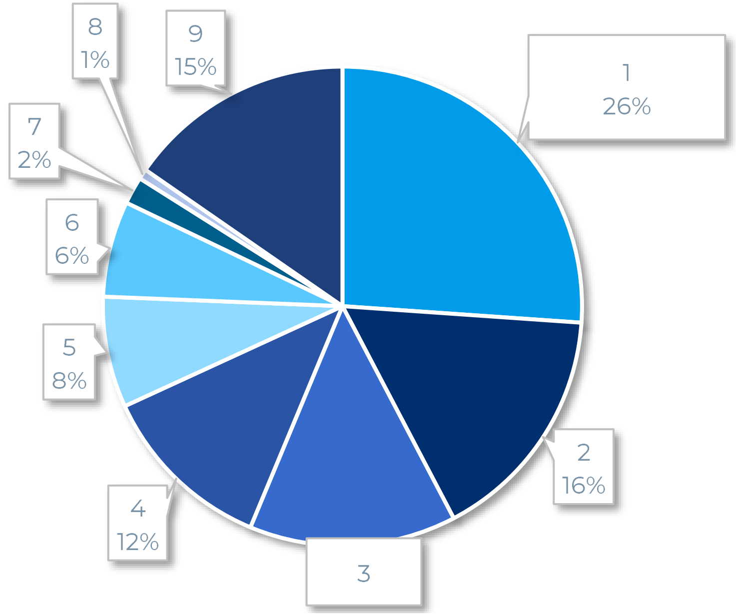
Disclosure

- Disclosed issues to CISA/vendors 90+ days ahead of publication
- Will not disclose full technical details
  - 'Unpatchable' issues → Compensating controls / Migrations can take long
  - Sensitive systems
- Affected versions & detailed mitigations
  - Coordinated with CISA & vendors: https://www.cisa.gov/uscert/ics/advisories
  - Overview: https://www.forescout.com/research-labs/ot-icefall/
- Some issues and responses still in disclosure

Impact

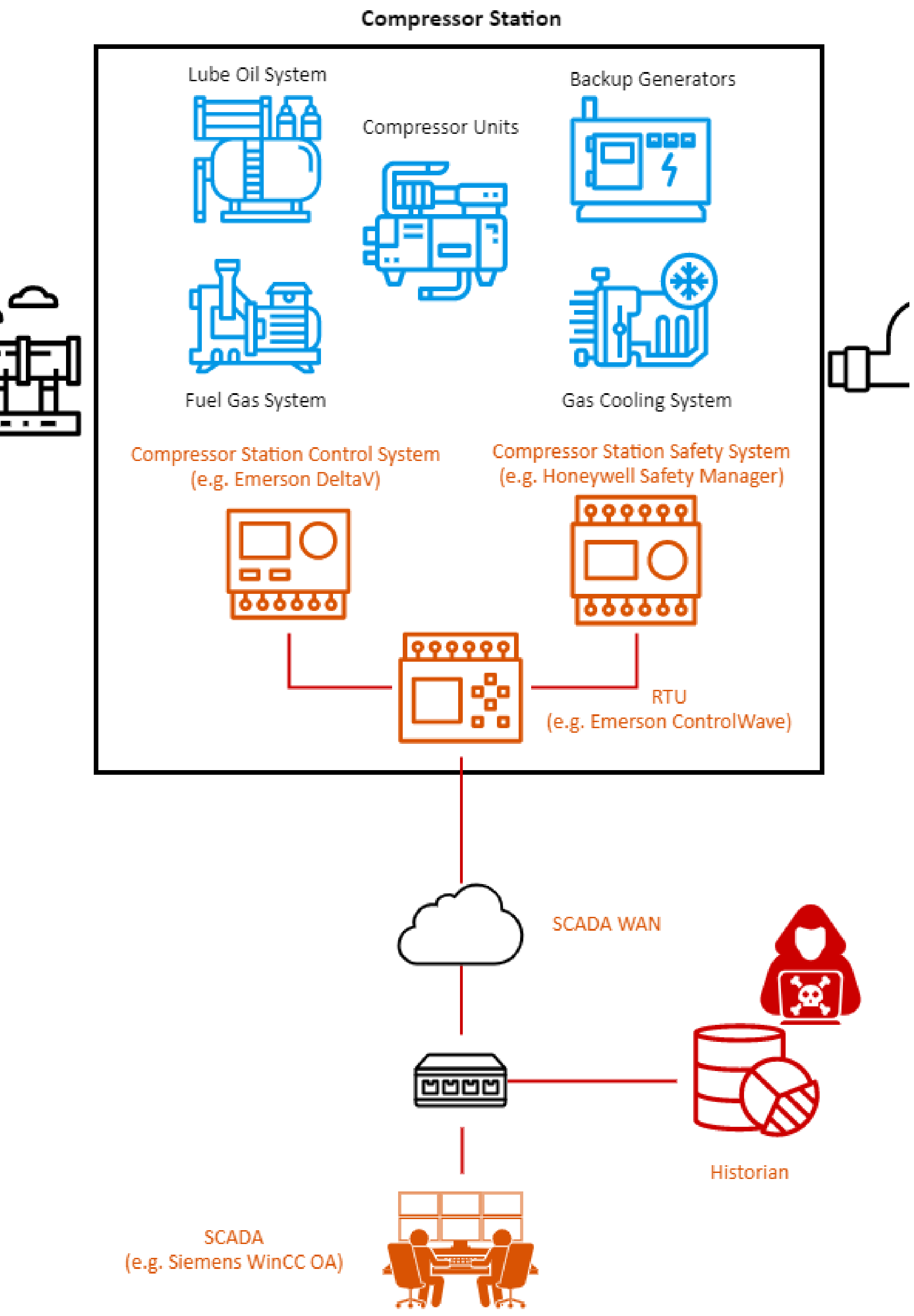
Vendor/Device	Shodan Query	#Results	Top 3 Countries
Honeywell Saia Burgess	http.favicon.hash:-1547576879	2924	Italy (954) Germany (326) Switzerland (263)
Omron	port:9600 response code	1305	Spain (321) Canada (113) France (110)
Phoenix Contact DDI	port:1962 PLC	705	Italy (285) Germany (104) India (68)
ProConOS SOCOMM	port:20547 PLC	236	China (65) US (60) Germany (10)
Honeywell Trend Controls	“trend control”	162	France (74) Denmark (27) Italy (16)
Emerson Fanuc / PACSystems	port:18245,18246 product:"general electric"	60	US (22) Canada (5) Poland (4)
Stardom	“stardom”	5	Thailand (2) Egypt (1)
Siemens WinCC OA	"WinCC OA"	1	Austria (1)
Motorola MOSCAD	“moscad”	1	Korea (1)

Number of vulnerable devices on Forescout Device Cloud



Estimate impact of OT: ICEFALL

- Three main sources:
  1. **Open-source intelligence**
  2. **Shodan queries =** >5k devices exposed
  3. **Forescout Device Cloud =** >30k devices on Device Cloud



Scenario: Natural Gas Transport

- Gas periodically repressurized along pipeline route

- Attack on SCADA subnet
  - CVE-2022-33139: Auth bypass on WinCC OA → Manipulate setpoints & monitoring values

- Downstream hacking
  - CVE-2022-29961: **Auth bypass** on ControlWave RTU
    - Issue commands to **deny control and view**
  - CVE-2022-31801: **RCE** → gain **access to station network**
    - Move to DCS Area Control Network (ACN) [depending on segmentation]
  - CVE-2022-29957: Manipulate DCS via **unauthenticated protocols**
    - **Manipulate** suction pressure, lubrication/cooling, close discharge valves, disable anti-surge protection, etc.
  - CVE-2022-30313: Manipulate SIS via **unauthenticated protocols**
    - **Manipulate** ESD, F&G

Analysis

Risk management is complicated by opacity

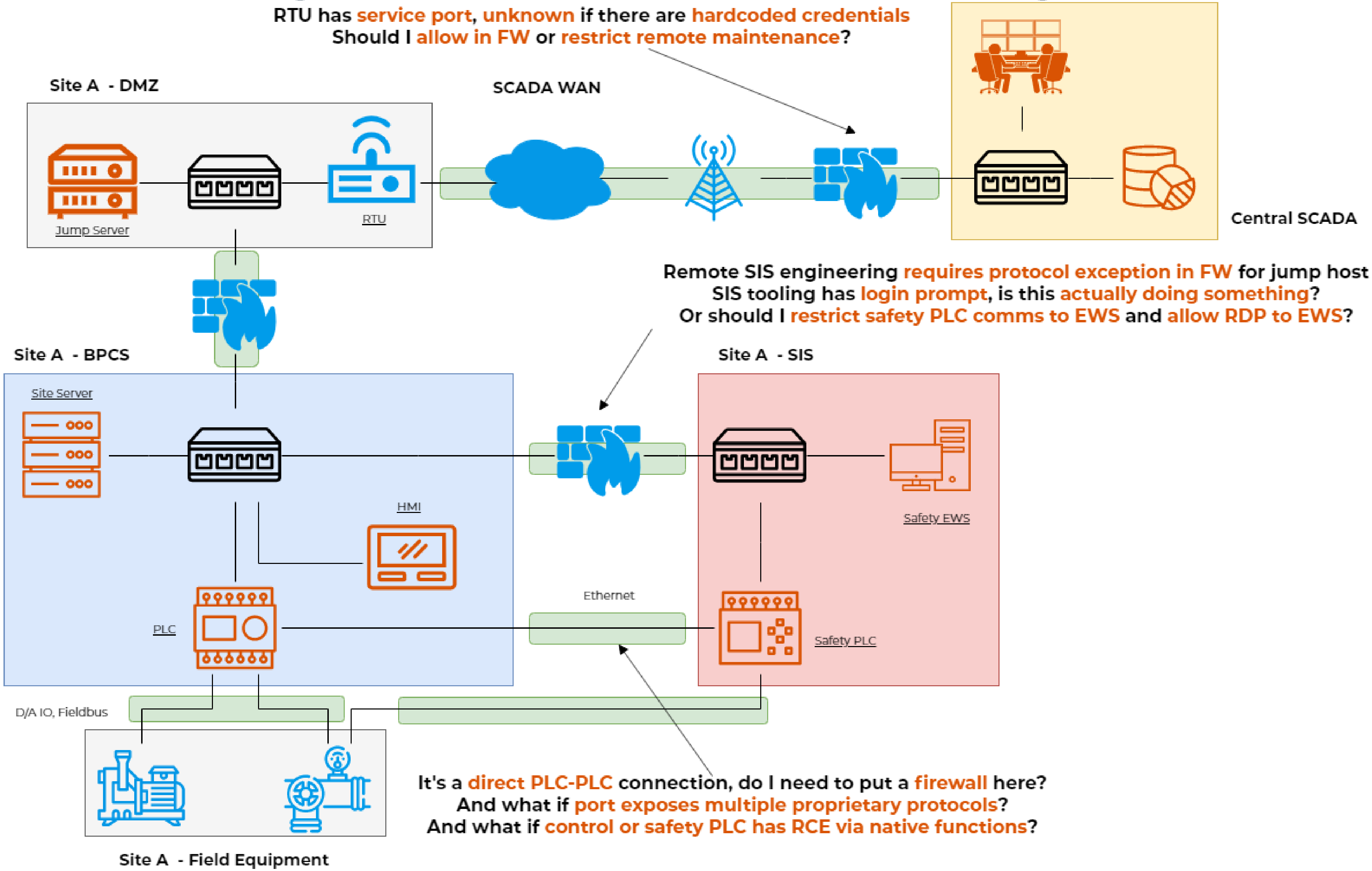
- Insecure-by-design is well-known issue, why revisit it?

1. Unless we default to defeatism, need to revisit status quo
   - How do we know if proprietary protocol has (new) security features?
   - Do we just assume security mechanisms are broken by default?

2. Not enough to know thing is insecure, need to know in what way
   - Big difference between changing a setpoint and getting RCE

- Can't make informed decisions based on speculation

Example: Segmentation & Hardening



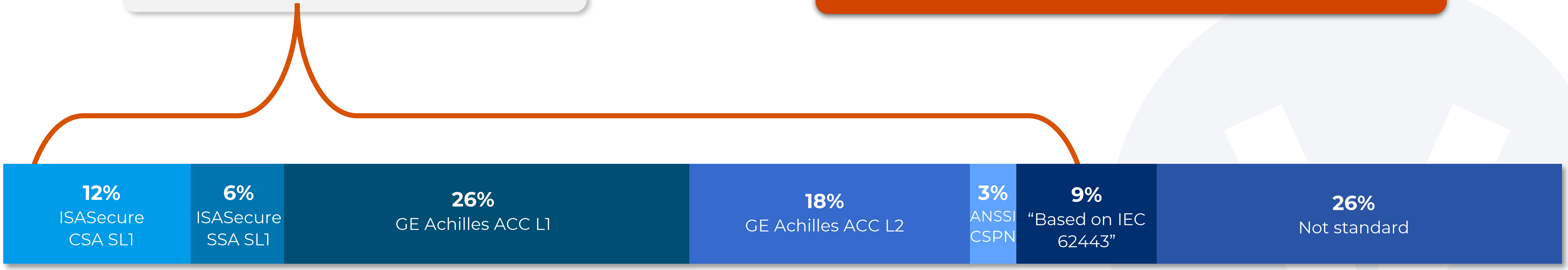
Vulnerable products are often certified

74%

of the product families affected by the found vulnerabilities have some form of security certification

Factors contributing to this problem include:

- (Re)certification effort
- Limited targets for evaluations
- Opaque security definitions
- Focus on **functional testing**



Certifications among affected product families

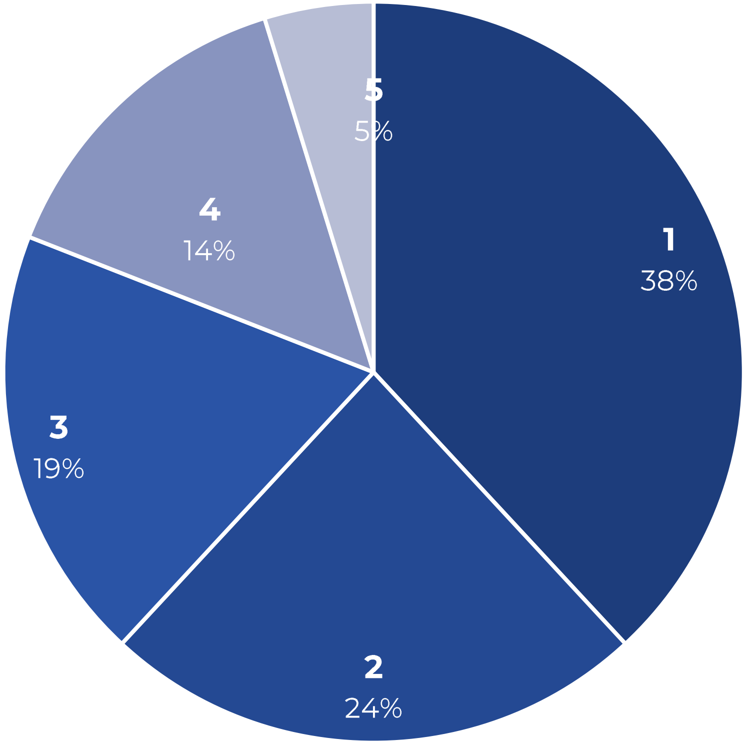
Advisories serve as reference for cert lab auditors without SME knowledge

When is something 'secure-by-design'?

- Most standards specify functional requirement
  - Little detailed guidance on *robust design*
  - Once met, holds for subsequent SLs

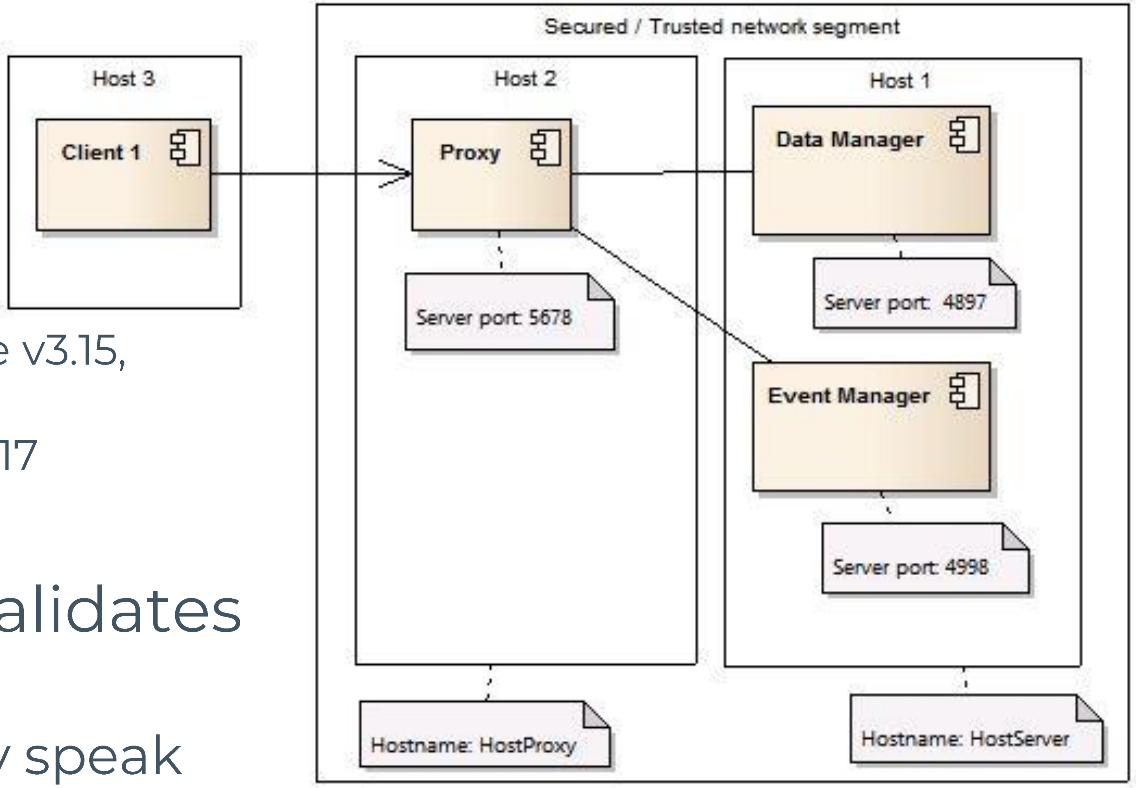
- 22 CVEs in OT:ICEFALL related to broken auth
- 28 CVEs in prior work (last 5 years) on *different* products with similar root causes

- Secure-by-design is not enough
  - Need secure-by-default, not 'how to harden' guidance somewhere in manual
  - Don't give integrators enough rope to hang themselves!



Example: Client-Side Authentication

- CVE-2022-33139: Siemens WinCC OA SCADA
  - Operator Interface talks to proxy
    - Wraps proprietary, unauthenticated PVSS in TLS
  - Auth schemes
    - Kerberos Authentication
    - Server-Side Authentication (SSA) ← available since v3.15, default since v3.17
    - Client-Side Authentication (CSA) ← default pre v3.17
- CSA fetches credentials from server, validates locally
  - Malicious client can simply ignore, directly speak protocol



Example: Broken Authentication #1

- Emerson ControlWave: Hybrid RTU/PLC
  - Popular in Oil & Gas, Water/Wastewater
- Proprietary automation & engineering protocol: BSAP/IP
  - Serial protocol transposed onto IP
  - Authentication capabilities, but
- CVE-2022-29961: Auth is based on MAC/IP whitelisting and protocol is UDP
- CVE-2022-29954/5/6: 3 different auth modes
  - Simple: 1-6 character plaintext password
  - Secure: challenge-response with 8-bit secret
  - Secure 2: response holds credentials, encrypted with challenge-based key

Example: Broken Authentication #2

- CVE-2022-29965: Emerson DeltaV controllers
  - Major DCS, big in Oil & Gas
- TCP-based maintenance interface
- Privileged operations (incl. shell access) require utility password
- Generated using insecure algorithm with predictable seed (no secrets)
- Silently patched few releases ago
  - But we know OT patching times…

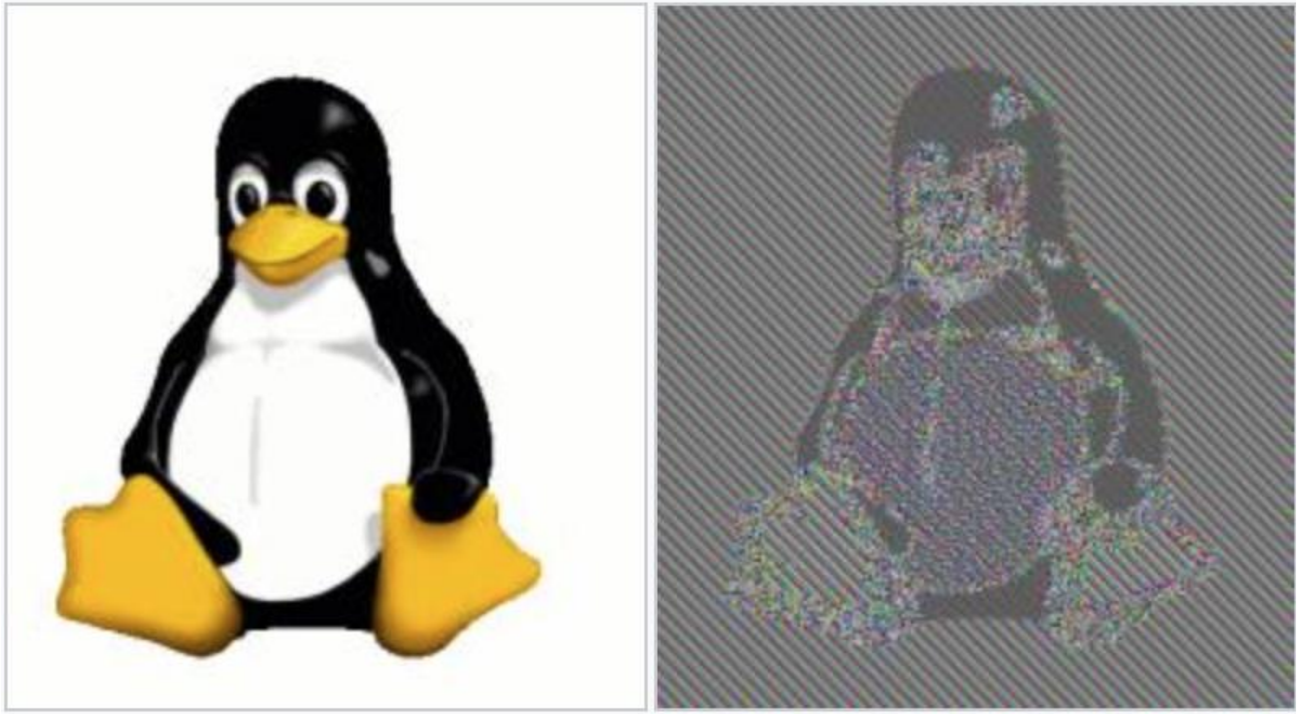
Example: Broken Crypto

- CVE-2022-30273: Motorola MDLC protocol
  - SCADA ↔ RTU WAN L7 protocol (over IP, serial, radio, microwave, etc.)

- Encryption modes
  - AES256: default in newer RTUS (e.g. ACE3600)
  - Legacy: used by older RTUs (e.g. MOSCAD/ACE1000)

    Supported in new ones until 2022 (backward compatibility)

- Legacy: TEA in ECB mode



Original image — Encrypted using ECB mode

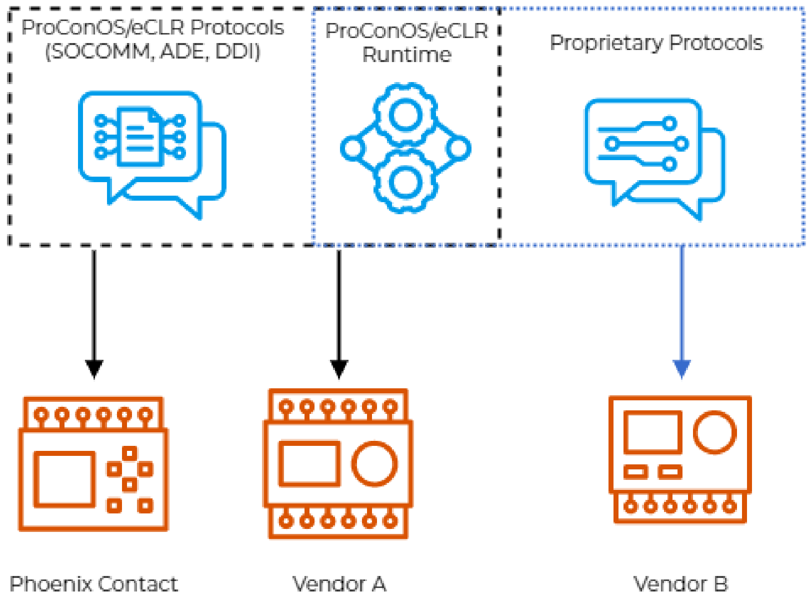
No more Potemkin Security

- Fake villages built for Empress Catherine II during official visits
  - Subpar controls are less intentional but result in similar false sense of security

- Secure-by-design+default can only work with clear, technically explicit minimum requirements on controls and in-depth independent validation

Supply Chains & SBOMs

- ProConOS IEC 61131-3 runtime
  - Similar to CODESYS, ISaGRAF
  - KW-Software, acquired by Phoenix Contact
  - Used by many OEMs, integrators
- Different integration conditions
  - ProConOS vs ProConOS/eCLR runtimes
  - SOCOMM vs ADE vs proprietary protocols
- Lack of SBOMs leads to vuln rediscovery
  - CVE-2014-9195 (PC) == CVE-2016-4860 (Yokogawa)
  - CVE-2022-31800/1 known but never assigned CVEs
- Public PoCs available for years

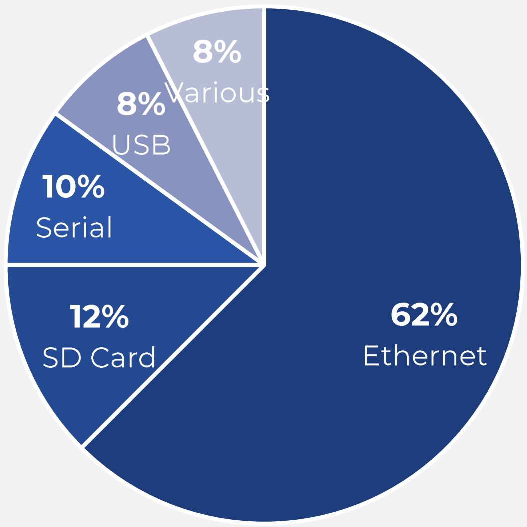


Vendor	Product
Phoenix Contact	AXC, ILC, RFC, FC
Emerson	ControlWave
ABB	RTU 520/540/560
Advantech	ADAM, APAX, AMAX, UNO
KUKA	KUKA.PLC
ICP DAS	KinCon-8xxx
Yaskawa	Mpiec
Schleicher	XCx
Hilscher	netPLC
Luetze	DIOLINE PLC
Delta	DMXC
ISH	SIS, SIC, uPLC
Yokogawa	STARDOM

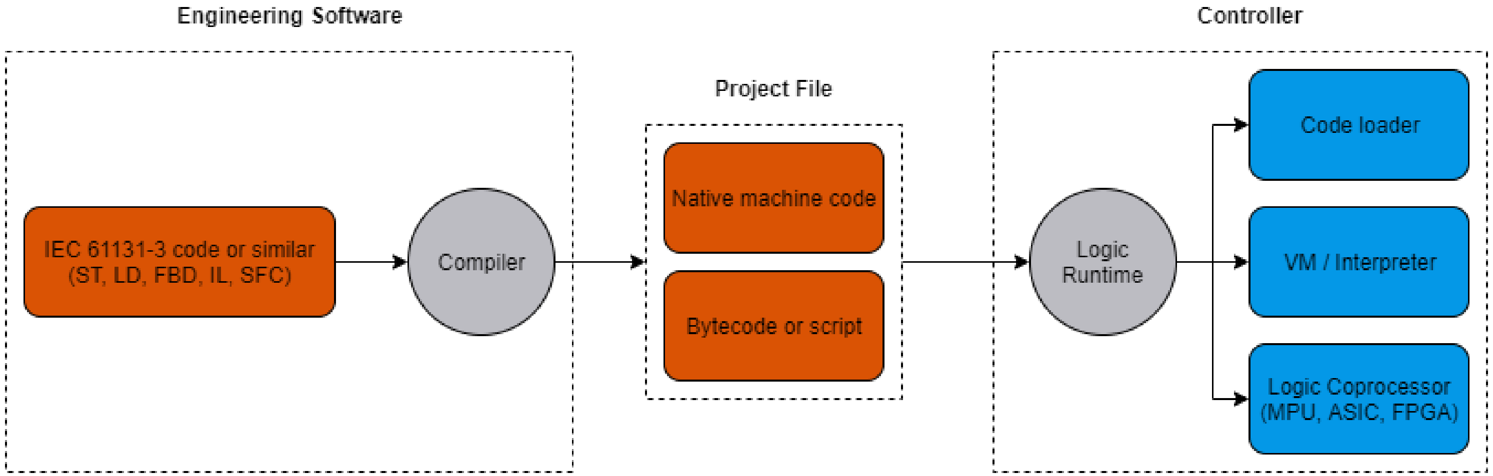
Shades of insecurity: Firmware updates

- Only 51% had some sort of FW update authentication
- Only 22% did some sort of FW signing
- Majority of updates over Ethernet
- SD/USB/Serial channels less at-risk but
  - Compromised EWS
  - Ethernet media converters

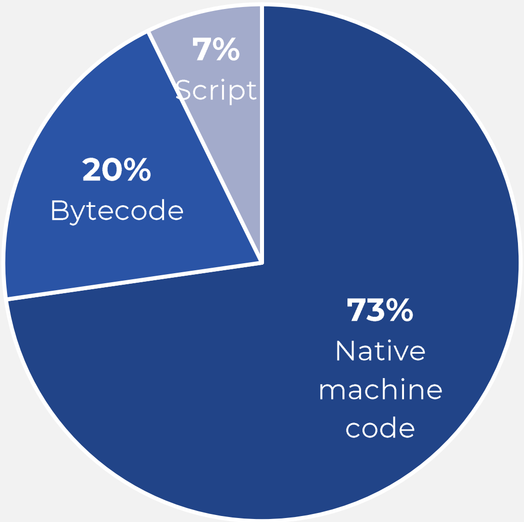
FW Update Channels



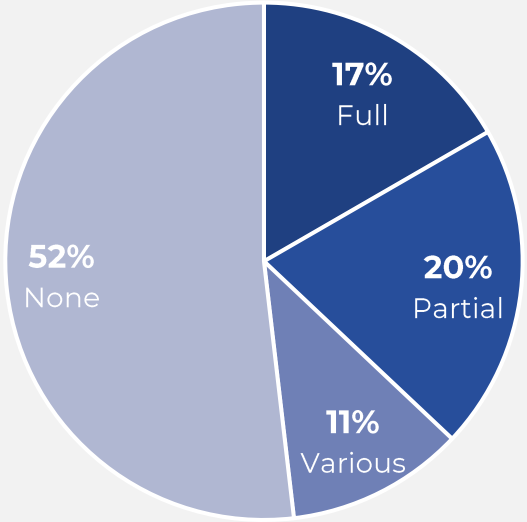
Shades of insecurity: Logic downloads



Logic Execution



Mode Switch Support



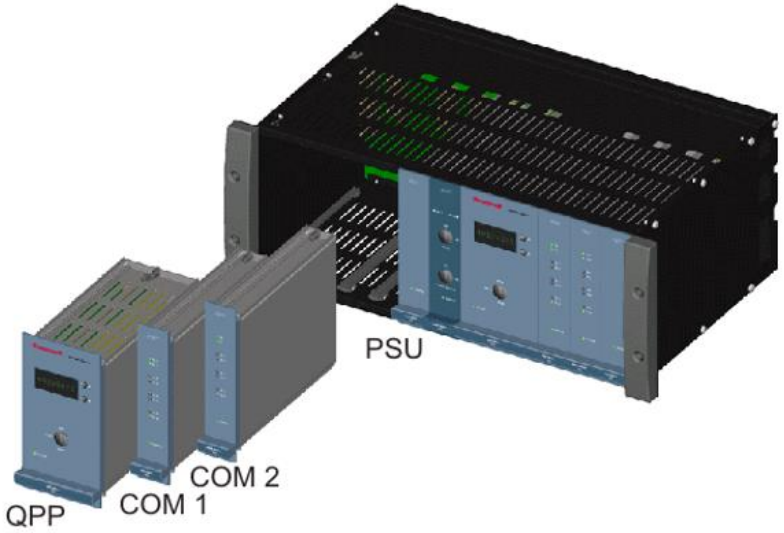
Example: Honeywell Safety Manager RCE

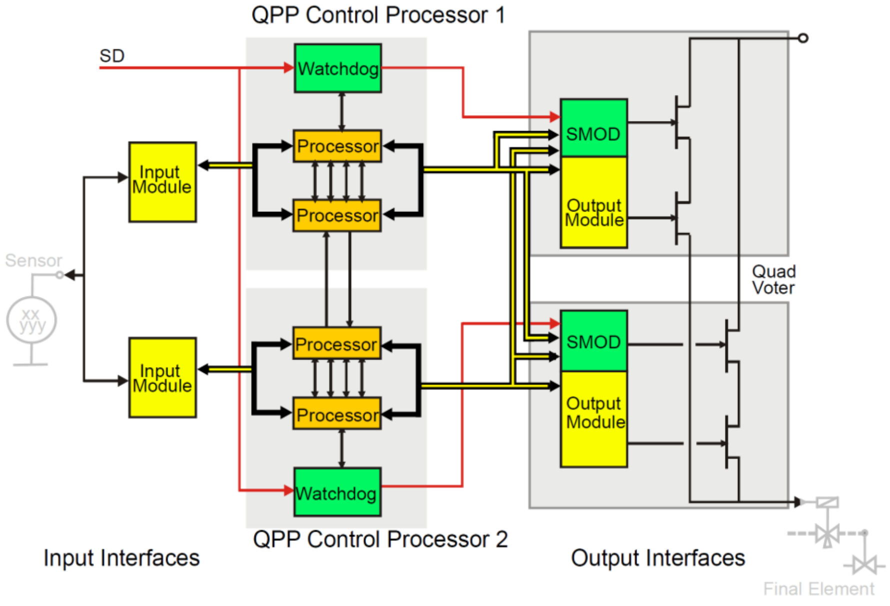
- SIL-3 SIS for ESD, PSD, F&G
  - Part of Experion PKS DCS or standalone
  - Similar to Schneider Triconex

- Many critical use-cases
  - Floating Production, Storage and Offloading (FPSO)
  - Wellhead platforms
  - Gas pipelines
  - LNG plants
  - Ethylene plants
  - Etc.

Example: Honeywell Safety Manager RCE

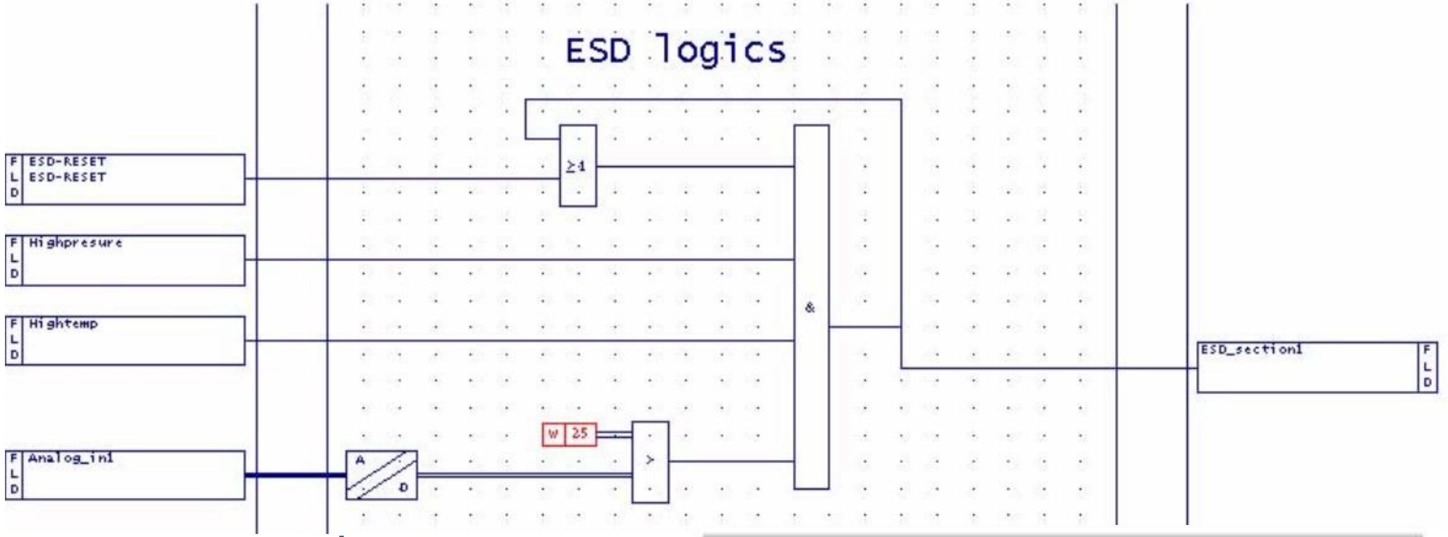
- Quad Processor Pack (QPP)
  - QMR CPU module
  - Executes SIF logic
- Universal Safety Interface (USI)
  - Ethernet/Serial comms module
  - Transfers recv'd logic to QPP over backplane
  - Insecure proprietary OT protocols
    - Safety Builder Protocol
    - Honeywell Modbus
- Battery & Keyswitch Module (BKM)





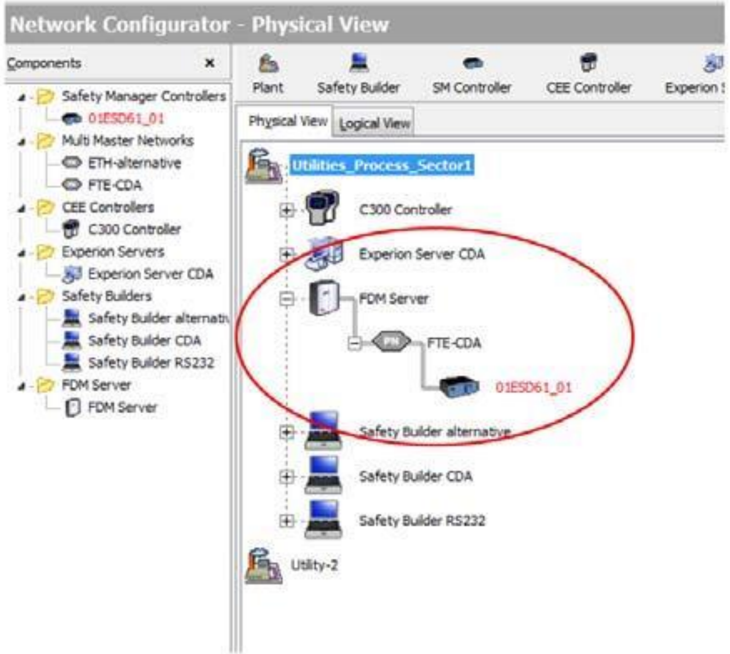
Example: Honeywell Safety Manager RCE

- Safety Station (EWS)
  - Manage & configure SM
  - Design SIFs in FLD
  - Download logic to QPP



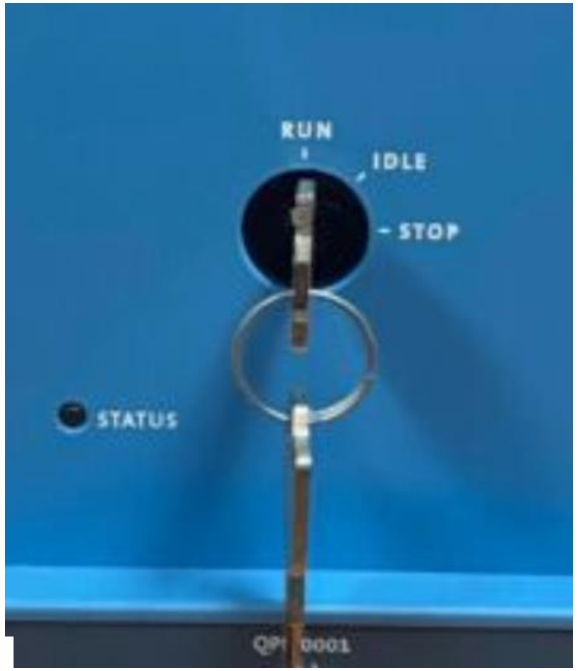
- CVE-2022-30313: Safety Builder protocol
  - Unauthenticated
  - Start/Stop, file read, logic download/upload

- CVE-2022-30315: FLDs compiled to machine code
  - No signing, no authentication
  - 'Execute my packet please' ← Like TRITON!



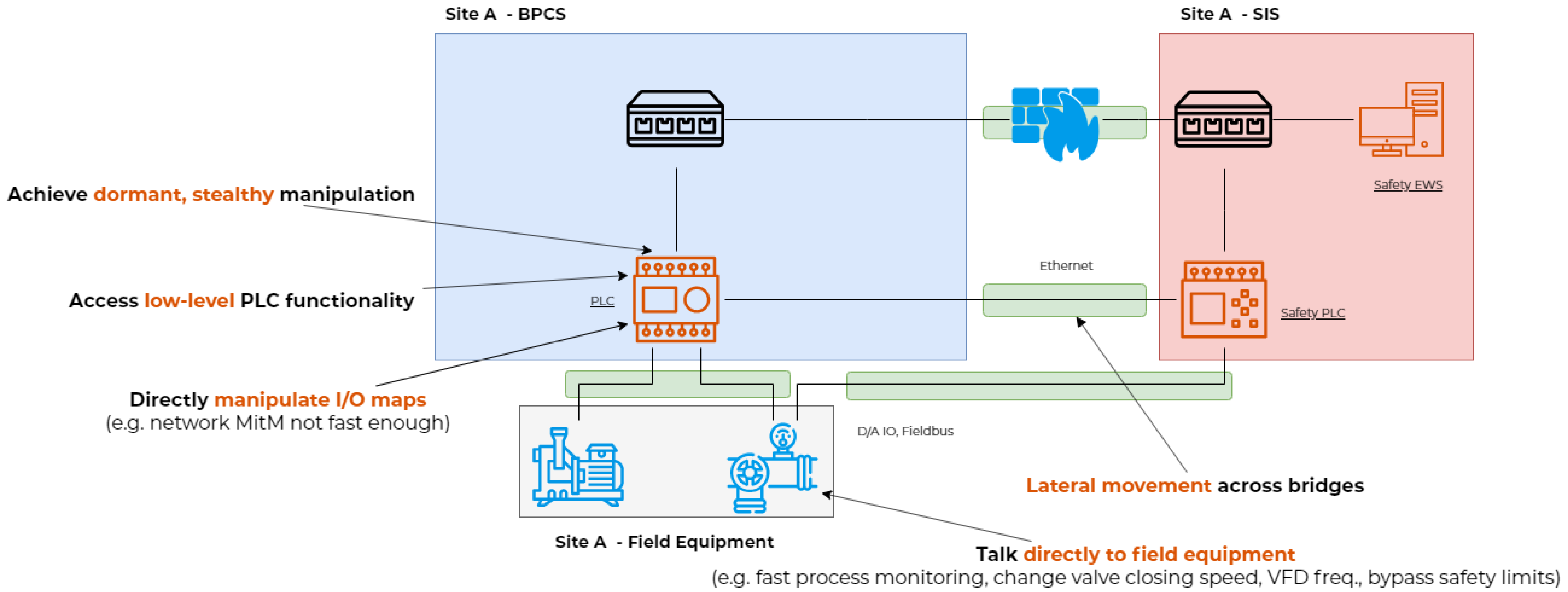
Example: Honeywell Safety Manager RCE

- Mitigating factors!
  - QPP keyswitch cannot be in RUN mode
  - BKM reset keyswitch after download
- <u>Except</u> when remote load/reset is enabled!
  - **Document this in your ISMS!**
- Additional compensating controls
  - Segmentation (OT-aware FW)
  - Monitoring (OT-aware IDS)
  - Restrict & secure access (VPN, IPSEC)
  - Migrate to S300 (FLD compiled to bytecode)



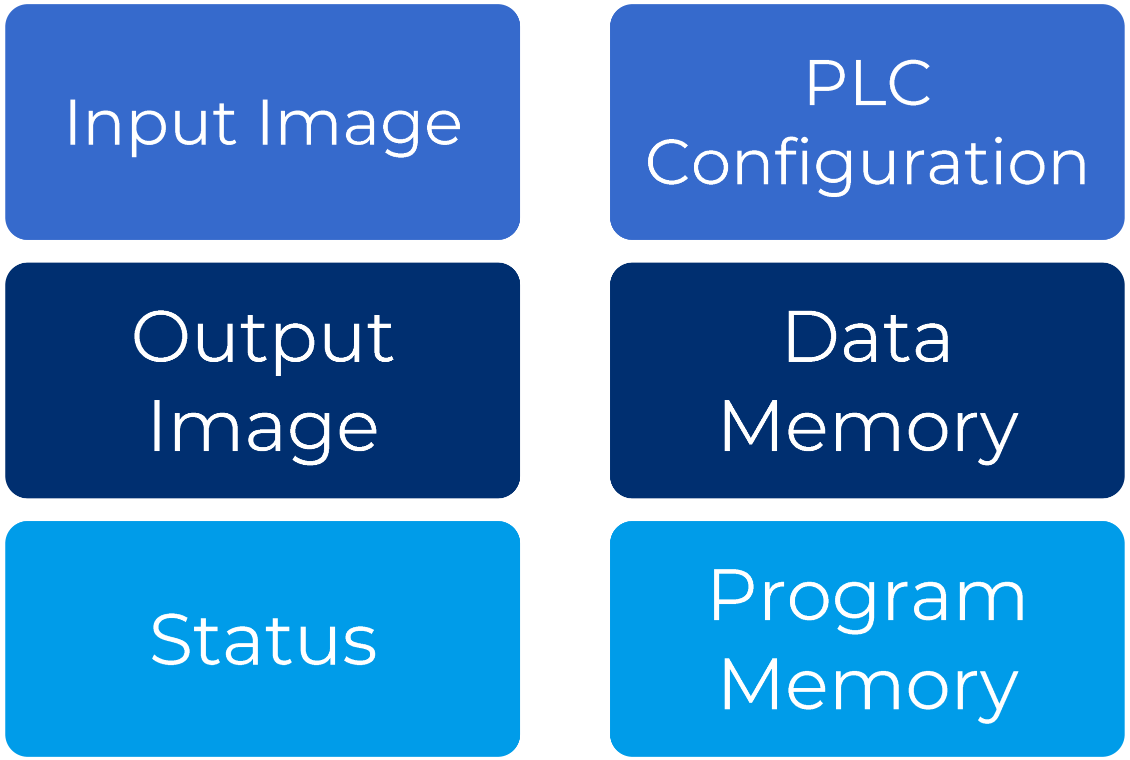
What's the big deal with RCE?

Why bother if I can modify a setpoint or logic?



Shades of insecurity: Memory Reads / Writes

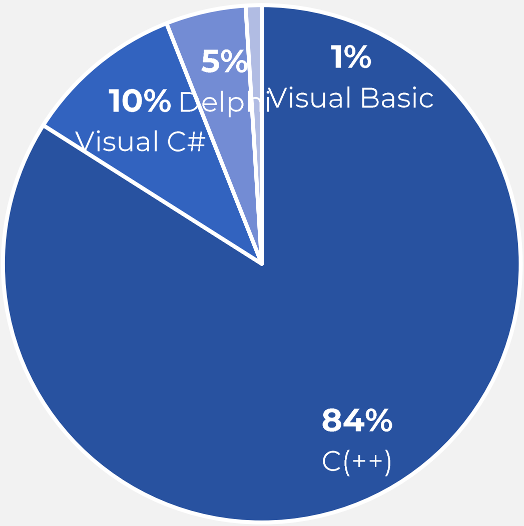
- PLC memory typically organized in dedicated *areas* and *blocks*
- Can read/write using engineering protocols
  - Often no bounds checks or ACL
  - Sometimes no HW/OS support for memory protection & privilege separation
- Basic operations often remain unauthenticated (unlike logic downloads/uploads)
- Impacts vary
  - OOB-read to get password from memory
  - OOB-write for RCE



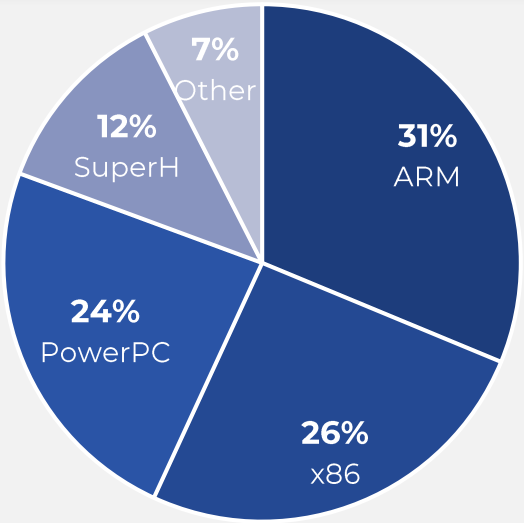
Reverse Engineering

For offensive OT capability development

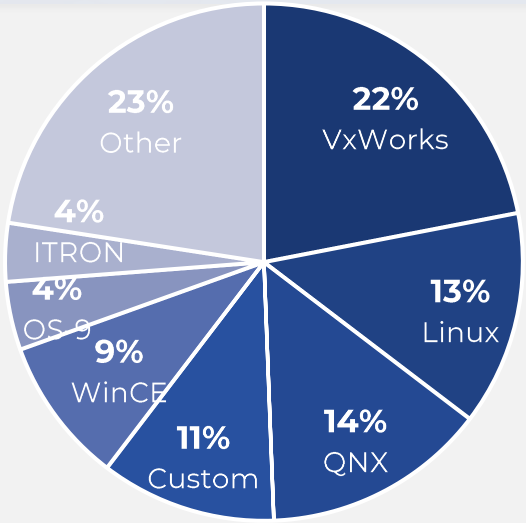
Dev. Languages



CPU Architectures



RTOSes



- Windows software packages are typically huge (GBs) & complex
  - 100s of DLLs, MFC, ATL, COM, RPC, Qt
- Devices match typical non-consumer embedded systems
  - Regional outliers (OS-9/ITRON + SuperH in Asia)

Offensive Capabilities are Feasible to Develop

Reverse engineering a single proprietary protocol

- Took between 1 day and 2 man-weeks

Reverse engineering a complex, multi-protocol system

- Took 5 to 6 man-months

- Basic offensive cyber capabilities leading to the development of OT-focused malware or cyberattacks could be developed by a small but skilled team at a reasonable cost

Conclusions

Mitigation

Mitigation recommendations

Discover and inventory vulnerable devices

Work toward consequence reduction by following Cyber-PHA and CCE methodologies

Enforce segmentation controls and proper network hygiene

Make use of native hardening capabilities

Monitor progressive patches released by affected device vendors

Actively procure for secure-by-design products

Monitor all network traffic for suspicious activity

Also see vendor & CISA guidance
https://www.forescout.com/research-labs/ot-icefall/

Conclusion

Based on quantitative analysis of our research:

- Small but skilled teams can develop OT Offensive Cyber Capabilities at surprisingly reasonable cost

- Insecure-by-design practices are still the norm
- Subpar security controls

- Products with insecure-by-design features and broken security controls continue to be certified

- Issues invisible and unactionable leading to unnecessary risk blindness

CTA

- **Device manufacturers** – Properly secure OT devices and protocols
- **Asset owners** – Actively procure for secure-by-design products
- Wider **security community** – Ensure that security controls are robust

https://www.forescout.com/research-labs/ot-icefall/

Thank you.

VEDERE LABS