



OT:ICEFALL

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

Jos Wetzels
Security Researcher, Forescout

- ▶ 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



The long climb ahead

- ▶ 10+ years ago, Digital Bond's Project Basecamp¹, 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, etc.
- ▶ OT:ICEFALL² (after next stop on Mt. Everest) aims to be quantitative **checkup of progress** made in **active production environments**
 - Evaluated systems selected based on customer asks to look into & support specific OT systems

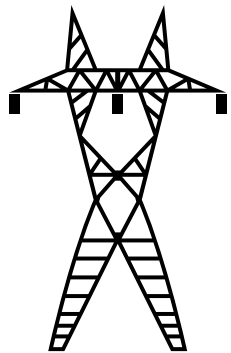
¹ <https://github.com/digitalbond/Basecamp>

² <https://www.forescout.com/resources/ot-icefall-report/>

Real-World Attackers Abusing Insecure-by-Design

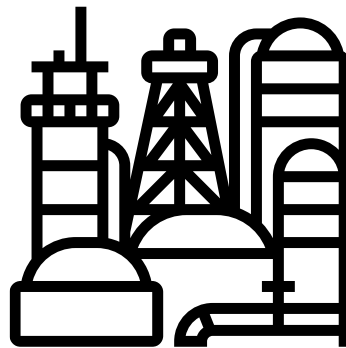
INDUSTROYER 1 & 2

- ▶ 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

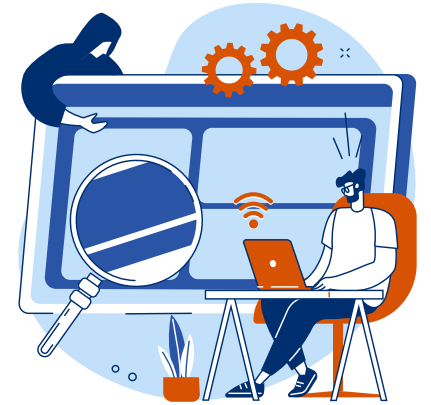


INCONTROLLER

- ▶ 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

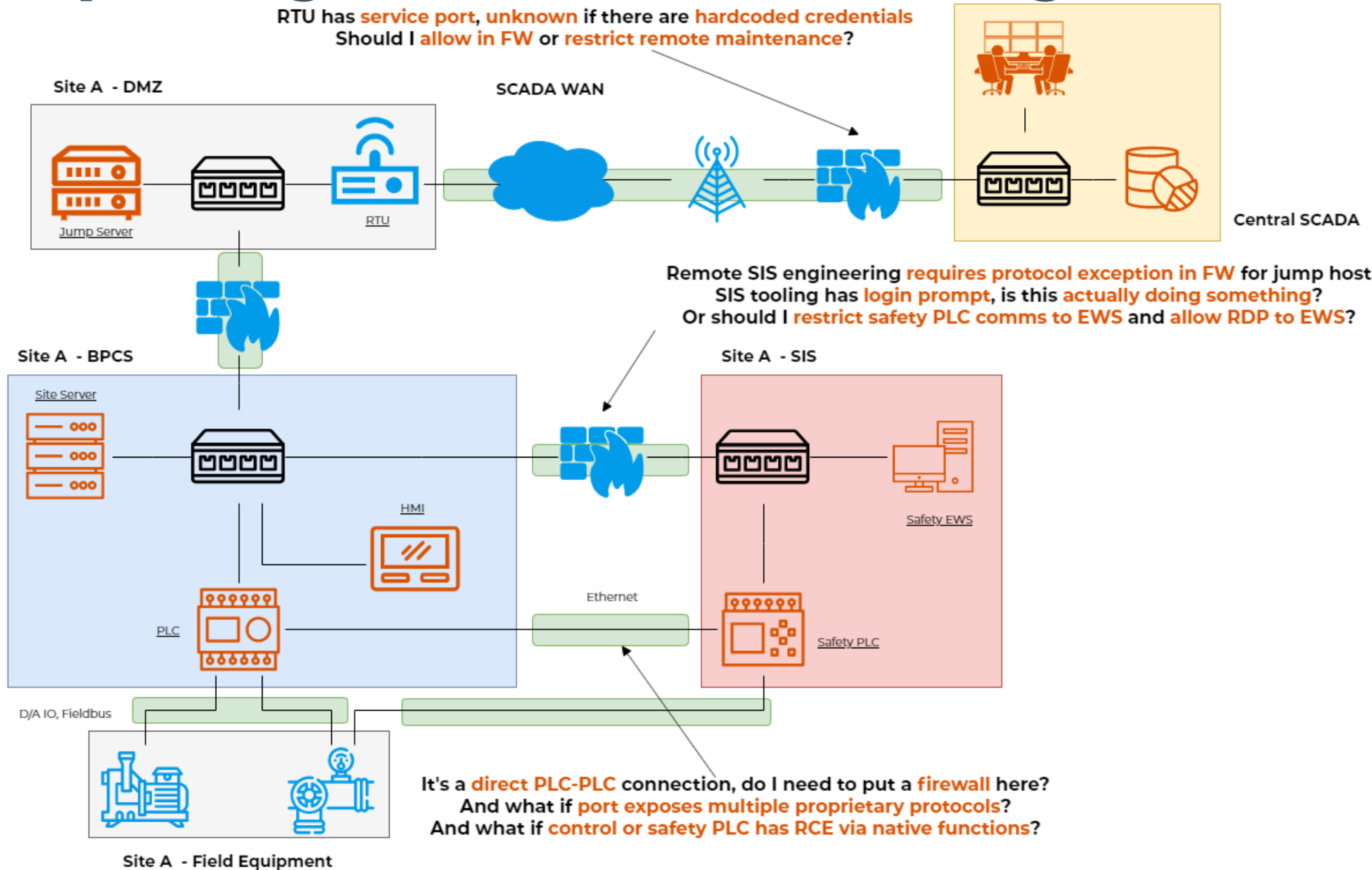
Insecure-by-design is a well-known issue, why revisit it?

- ▶ Risk management is complicated by opacity
 - Are we making **progress in install base**?
 - What's **under the hood** of those security controls?
- ▶ Cannot assume every **proprietary system** is & remains equally broken
 - Security mechanisms are sometimes **retrofitted**
 - Authentication implementations **change over time**
- ▶ Not enough to know thing is 'insecure', **need to know in what way**
 - Big difference between **changing setpoint** and RCE
 - Need to **justify compensating controls**
- ▶ Can't make **informed decisions** based on **speculation**



Example: Segmentation & Hardening

RTU has **service port, unknown** if there are **hardcoded credentials**
Should I **allow in FW** or **restrict remote maintenance**?

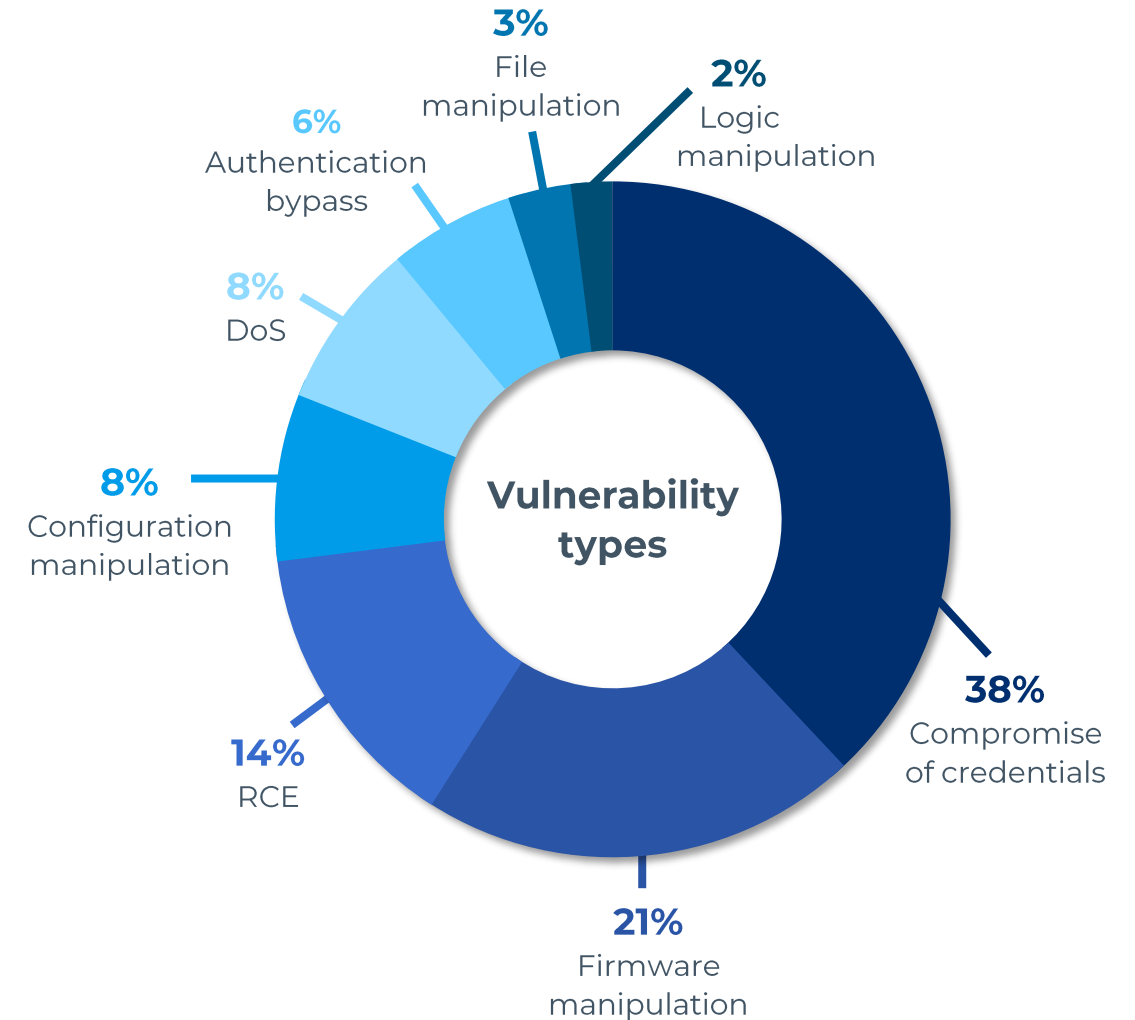


Overview

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/>



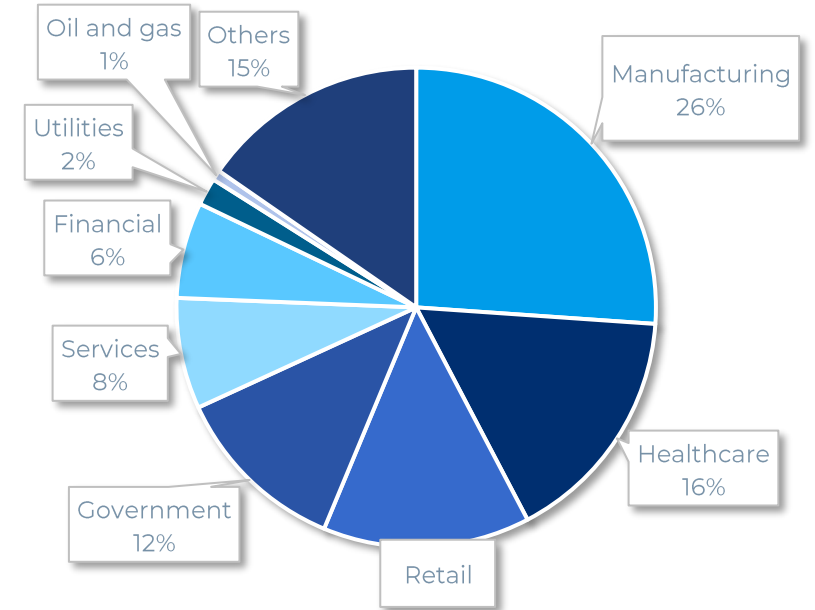
Disclosure

- ▶ Disclosed issues to CISA/vendors **90+ days ahead of publication**
 - Some vendors started in-depth investigation **very late**
 - Some issues and responses **still in disclosure**
 - Some vendors wanted details to be **restricted** to product bulletins
 - In some cases, **invigorated secure protocol development efforts**
- ▶ Affected versions & detailed mitigations in **CISA / vendor advisories**
 - <https://www.cisa.gov/uscert/ncas/current-activity/2022/06/22/cisa-releases-security-advisories-related-oticefall-insecure>
- ▶ Will not disclose full technical details

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

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**



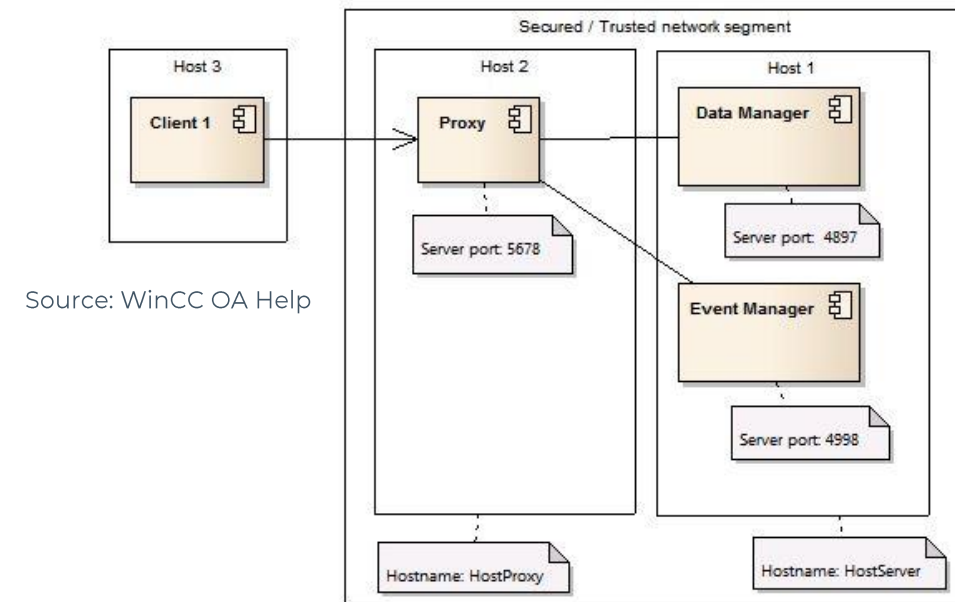
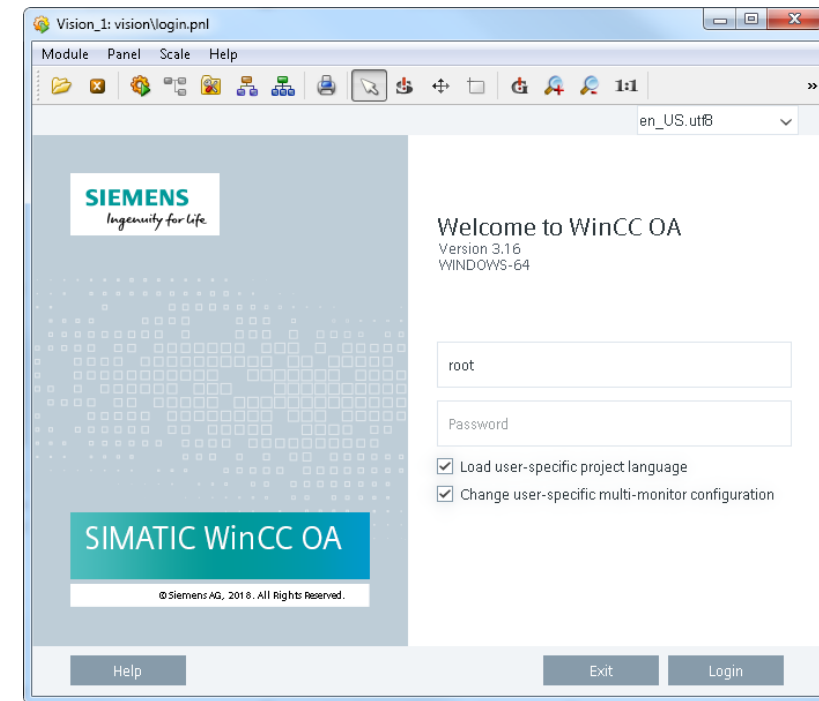
Certifications among affected product families

Advisories serve as reference for cert lab auditors without SME knowledge

Broken Authentication Schemes & Improper Fixes

Siemens WinCC OA SCADA (CVE-2022-33139)

- ▶ Operator UI talks to proxy
 - Proxy wraps **proprietary PVSS protocol** in TLS
- ▶ Authentication Modes
 - **Client-Side Authentication (CSA)**: default pre-3.17
 - Preferred for SSO integration
 - Server-Side Authentication (SSA): default 3.17+
 - Kerberos Authentication
- ▶ CSA stores creds as database points
- ▶ Client **sends PVSS request for creds, validates locally (e.g. against AD)**
 - Attacker can just write malicious client, no need for auth

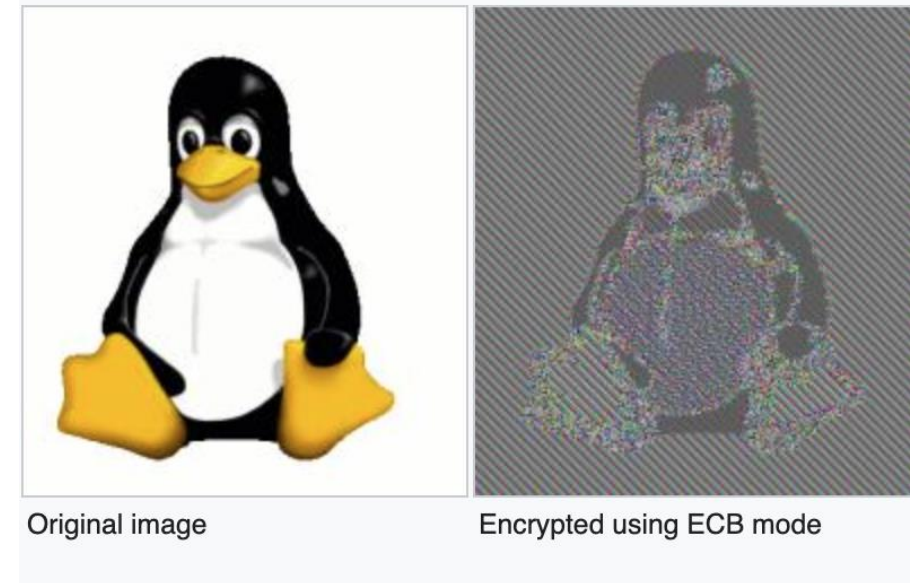
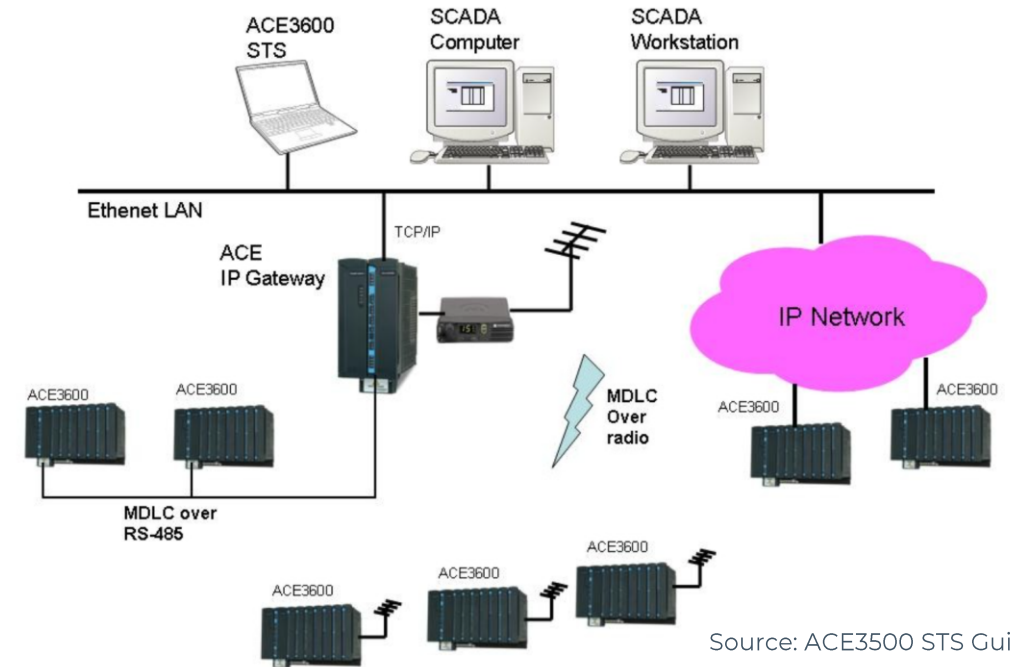


Motorola MDLC (CVE-2022-30273)

- ▶ SCADA ↔ RTU WAN protocol
 - (over IP, serial, radio, microwave, etc.)
- ▶ PSK-based Encryption Modes
 - **AES256**: default in newer RTUS (e.g. ACE3600)
 - **TEA-ECB**: default in older RTUs (e.g. MOSCAD/ACE1000)

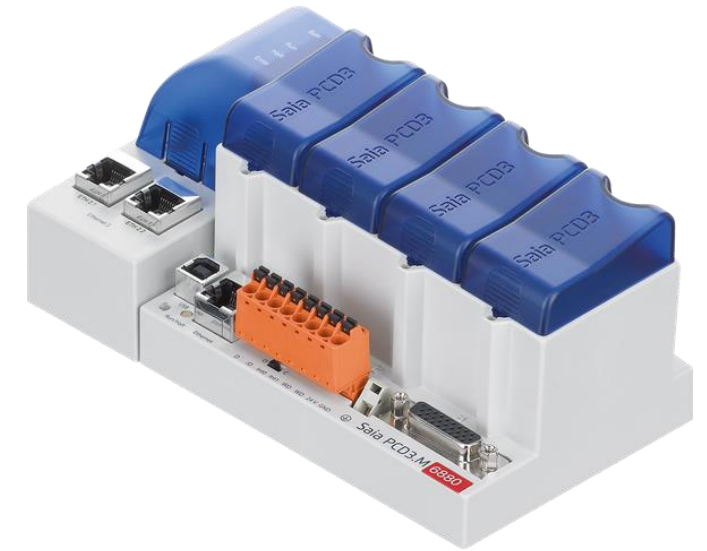
Supported by ACE3600 until 2022
(backward compatibility/mixed networks)

- **Notorious block cipher mode of operation**
- **Known plaintext attacks, block-swapping, etc.**



Saia Burgess PG5 PCD PLC (CVE-2022-30320)

- ▶ Uses **S-Bus** protocol (5050/UDP)
 - Master-slave protocol, historically RS485
- ▶ Password auth for engineering operations
 - S-Bus write to static address
 - 32-bit 'hash' derived from **CRC-16/XMODEM** over password **without nonce**
- ▶ Trivially insecure
 - Collisions
 - Replay
 - UDP with MAC/IP whitelist



```
public static uint PasswordToUInt32(string password)
{
    ushort crc1 = 0;
    foreach (char c in password)
    {
        if (!char.IsDigit(c) && !char.IsUpper(c))
            return 0;
        crc1 = SaiaLib.Crc16(crc1, Convert.ToByte(c));
    }
    ushort crc2 = crc1;
    foreach (char c in password)
    {
        if (!char.IsDigit(c) && !char.IsUpper(c))
            return 0;
        crc2 = SaiaLib.Crc16(crc2, Convert.ToByte(c));
    }
    return ((uint) crc2 << 16) + (uint) crc1;
}
```

Emerson ControlWave PLC/RTU

(CVE-2022-29954, CVE-2022-29955, CVE-2022-29956)



- ▶ Uses **BSAP/IP** protocol (1234/UDP)
 - Password auth for engineering operations
 - But: **UDP with MAC/IP whitelist**

- ▶ Authentication Modes
 - **Simple (legacy)**: 1-6 character plaintext password
 - **Secure (legacy)**: PLC sends 8-bit key K, EWS responds with E(pass, K)
 - **Secure 2 (undocumented, current)**: PLC sends 64-bit key K, EWS responds with E(pass, K)

- ▶ Bad design, 3 times over
 - **Can just decrypt the credentials**
 - Fundamental misunderstanding of challenge-response

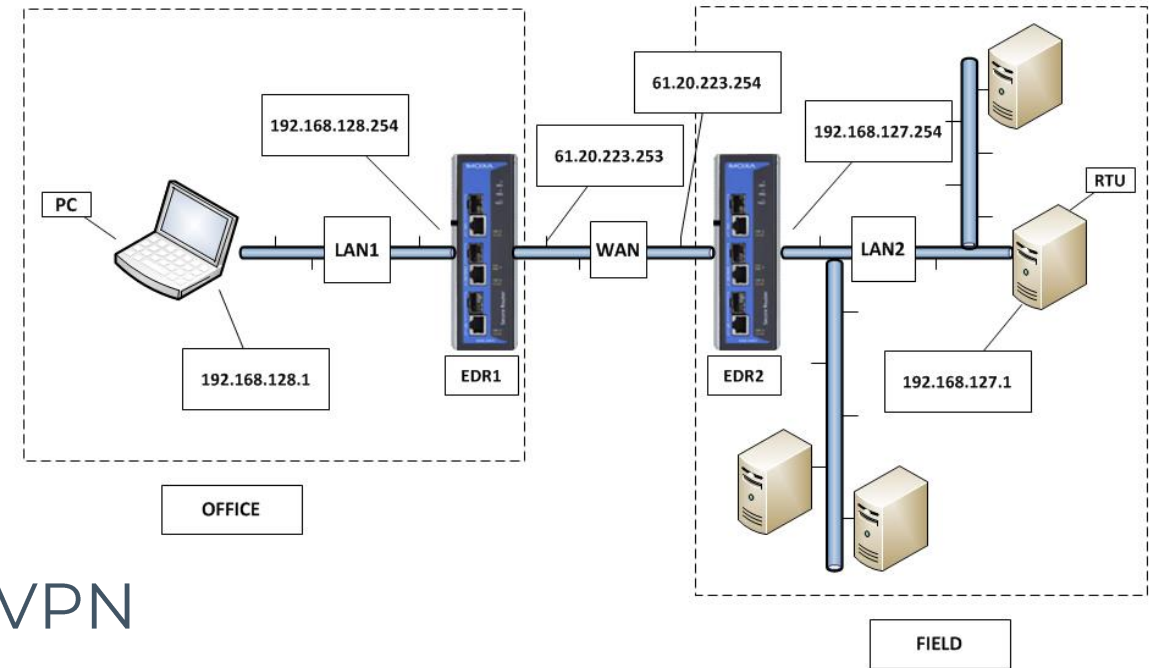
“Not a vulnerability” according to Emerson

- ▶ They feel this is adequately addressed by ControlWave manual
 - Basically: install VPN + firewall
 - “Enhanced security” implies existing controls offer “basic security”

1.8 Secure Gateway

For enhanced data security when using an IP/Ethernet connection, Emerson Remote Automation Solutions recommends adding an industrial router with VPN and firewall security. Recommended solutions include the MOXA EDR-810, the Hirschman Eagle One, or the Phoenix mGuard rs4000 (or equivalents). An example of how to install one of these devices to the RTU can be found in the Emerson Remote Automation Solutions *MOXA® Industrial Secure Router Installation Guide* (part number D301766X012). For further information, contact your Local Business Partner or the individual vendor’s website.

Source: ControlWave Micro Instruction Manual



Source: MOXA Industrial Secure Router Installation Guide (D301766X012)

- ▶ Reference recommends site-to-site VPN
 - No protection at site level

Yokogawa STARDOM PLC (CVE-2022-30997)



- ▶ **Hardcoded credentials** for **Telnet** maintenance interface
 - Duplex controllers only up to R4.31
- ▶ Multiple prior CVEs for hardcoded creds on *same* interface
 - CVE-2018-10592, CVE-2018-17896
- ▶ Indicates **bug-fixing is not followed up with variant-hunting**

```
strcpy(password, ██████████);  
password[9] = 0;  
*(_WORD *)&password[10] = 0;  
if ( loginUserVerify(██████████ password) )  
{  
    if ( !dword_593E58 && DuoLoginEncrypt(password, &s_encrypted) )  
        r
```

Emerson DeltaV DCS controllers

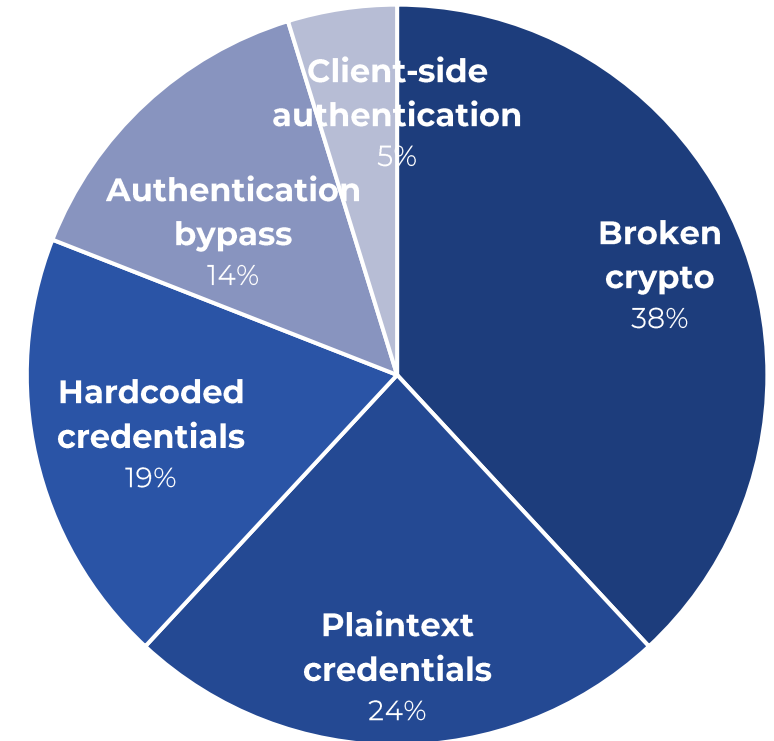
(CVE-2022-29962, CVE-2022-29963, CVE-2022-29964, CVE-2022-29965)

- ▶ “Read-only Telnet” (18550/TCP) **hardcoded creds**
 - S/P-controllers, CIOC, EIOC up to at least v14.3.1
 - Other hardcoded reported for “*disabled FTP/SSH*” but could be used for **LPE**
- ▶ Maintenance Telnet + shell access (23/TCP) **insecure auth algorithm**
 - M/S/P-controllers, SIS up to at least v14.3.1.7283
 - Silently patched some point after
 - **Homebrew** algorithm **without secret**, using **predictable seed** < 16 bits
- ▶ Not first time DeltaV suffered from these issues
 - CVE-2014-2350 (hardcoded creds on Telnet 706/TCP)
 - Again shows **bug-fixing without subsequent variant-hunting**



When is something 'secure-by-design'?

- ▶ Most standards specify functional requirement
 - Little detailed guidance on *robust design*
- ▶ 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
 - Bugfixes should address *root cause* and be followed by *variant-hunting*
 - Shouldn't certified SDLCs guarantee this...?



No more Potemkin security please

- ▶ Subpar controls can result in false sense of security that can be worse than clear sense of insecurity
- ▶ Secure-by-design + default can only work with
 - Clear, technically explicit minimum requirements
 - In-depth, independent validation beyond functional testing



Impact & Nuance

Nuance: Supply Chains & Collisions

- ▶ See more supply chain vulns **across tech stack**
 - RTOSes, SDKs and standard libraries¹
 - Protocol stacks²
 - IEC 61131-3 runtimes³
 - Remote access solutions⁴
- ▶ Vulns discovered in **particular product** rarely make their way ‘up & down the chain’ to **other affected products**
 - Discoverers **unaware** vuln is in 3rd party component
 - 3rd party vendor **don’t have complete overview of supply chain** (intermediate integrators, white label vendors, etc.)
- ▶ Leads to **vuln collisions & risk blindness**

¹ BadAlloc, uClibc DNS

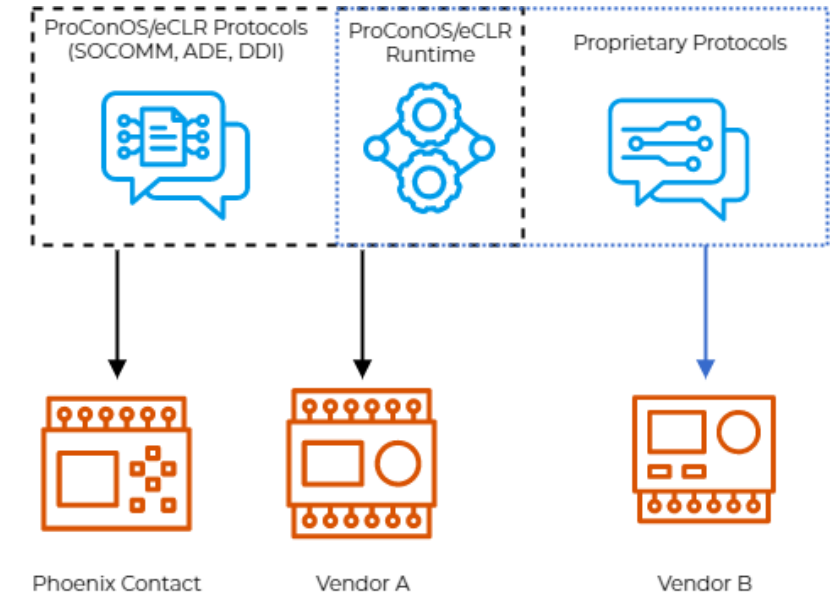
² Urgent/11, Ripple20, Amnesia:33, INFRA:HALT, NUCLEUS:13, RTA 499ES ENIP, Siemens PROFINET

³ CODESYS, ProConOS, ISaGRAF

⁴ Access:7

Example: ProConOS runtime

- ▶ IEC 61131-3 runtime by KW soft (now Phoenix Contact)
 - Used by **many** OEMs, integrators, white label vendors
 - Different integration conditions
 - **Runtime**: ProConOS vs eCLR
 - **Protocol**: SOCOMM vs ADE vs custom (eg Emerson ControlWave)
- ▶ History of vulns
 - **Unauthenticated protocols, RCE via unsigned logic**
 - CVE-2022-31800/1 **known** but **never assigned** CVEs
 - Other **CVEs only for Phoenix Contact products**
 - Public PoCs available for **years**
- ▶ **Lack of SBOMs** leads to **vuln rediscovery**
 - CVE-2014-9195 (Phoenix) == CVE-2016-4860 (Yokogawa)
- ▶ We identified additional affected parties
 - Unfortunately, info wasn't backpropagated to original CVEs as suggested



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

Nuance: Firmware Updates

- ▶ Malicious FW updates
 - Are *noisy*: controller reboot + process interrupt likely triggers alarms
 - But *powerful*: persist, mass-brick controllers, etc.
- ▶ Only 51% had update authentication, only 22% FW signing
- ▶ Majority of updates over Ethernet
 - But: some via SD/USB/serial ← risk reduced to compromised EWS / converters
- ▶ Caveat: if you sign, need to do it right
 - I.e.: end-to-end & asymmetric

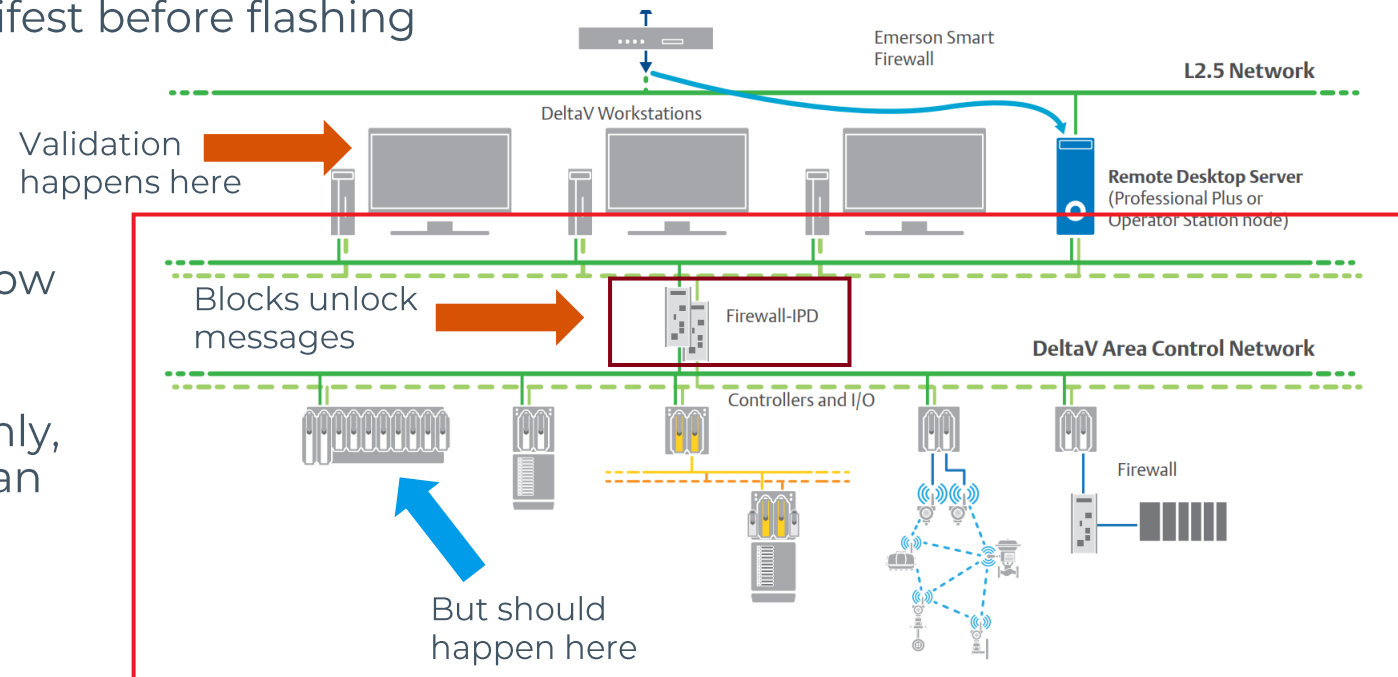
Example: Emerson DeltaV DCS



- ▶ Various **unauthenticated, proprietary protocols** (FW UPGD, PnP, SIS, Hawk SVC)
 - **Impact:** FW manipulation, config/strategy changes, service shutdown, etc.
- ▶ Controller firmwares are **unsigned** pre-14.3, only use CRC
- ▶ Emerson considers this *resolved* in 14.3 and *mitigated* elsewhere
 - 14.3+: **Update tool** validates sig in manifest before flashing
 - **Firewall-IPD** blocks unlock messages

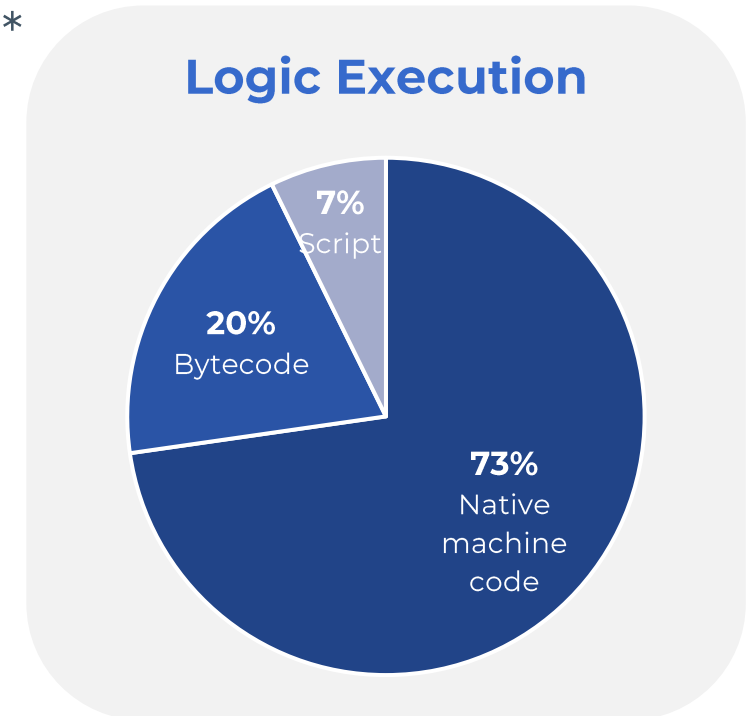
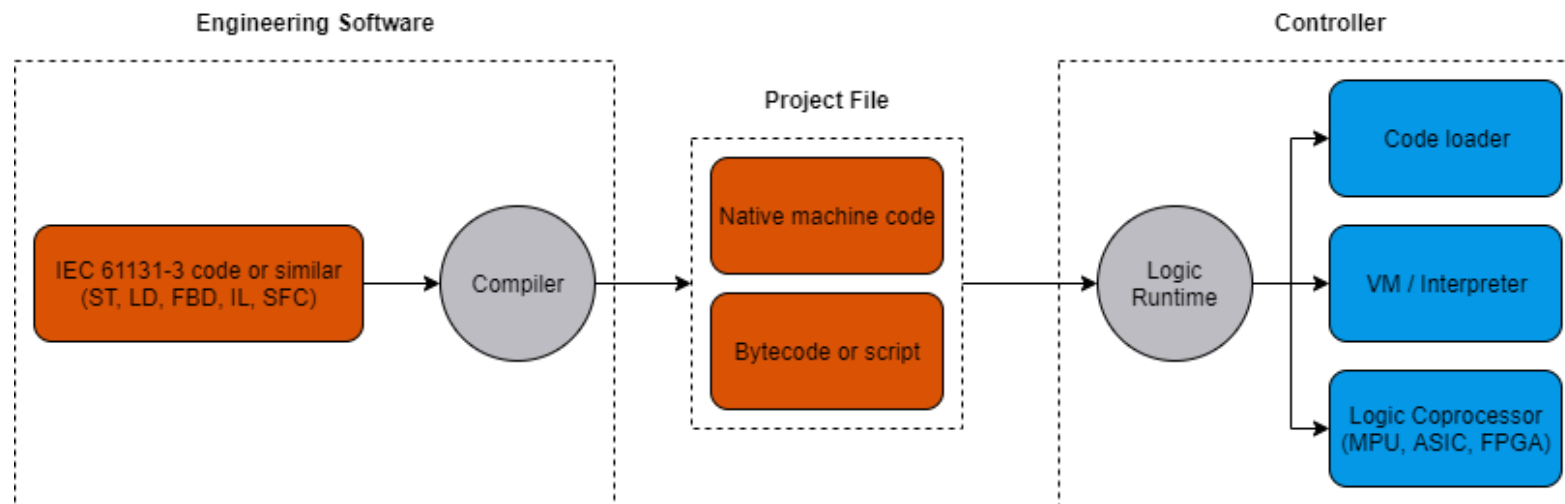
▶ But

- Attacker can target legit update window with own tooling
- In case IPD restricts comms to EWS only, attacker who can compromise EWS can still push malicious FW



Nuance: Logic Execution Model

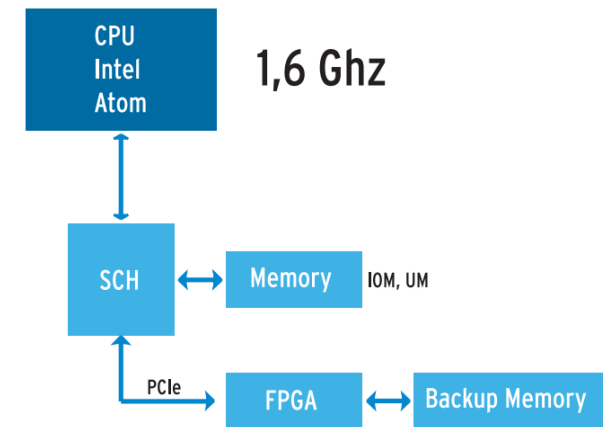
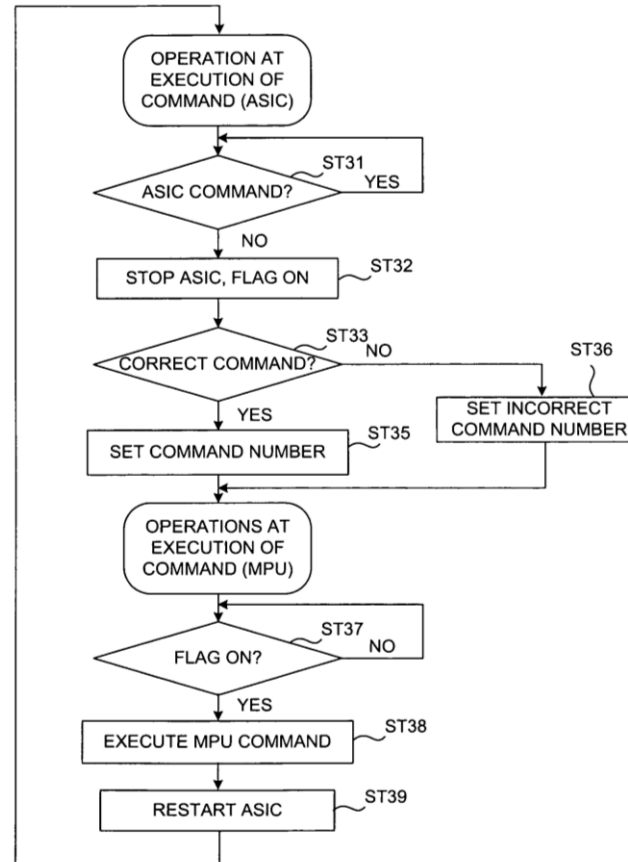
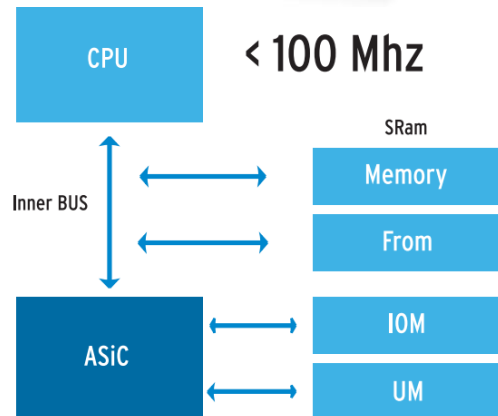
- ▶ Majority but not all logic is executed as **native machine code**
 - **No logic signing**, only handful used **sandboxing**
 - Often on PLCs **without RTOS/MMU support** for memory & privilege separation
 - Leads to *'execute my shellcode please'* scenarios
 - Bytecode VMs are bigger hurdle (see MC7P in S7-1200)*
 - Bytecode ASICs / FPGAs even more robust



* See: S. Brizinov - The Race to Native Code Execution in PLCs

Example: Omron SYSMAC CS/CJ/CP vs NJ/NX PLCs

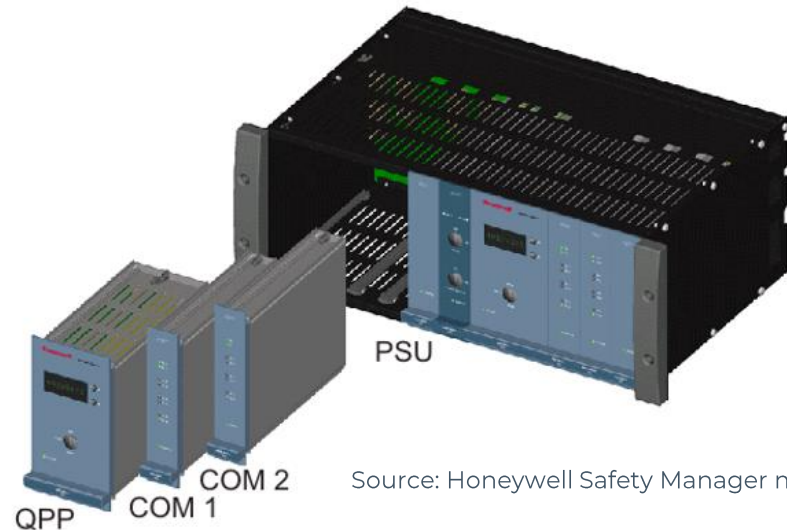
- ▶ Proprietary ASIC bytecode vs x86 machine code
 - Difference is **constrained** vs **unconstrained, low-level** access



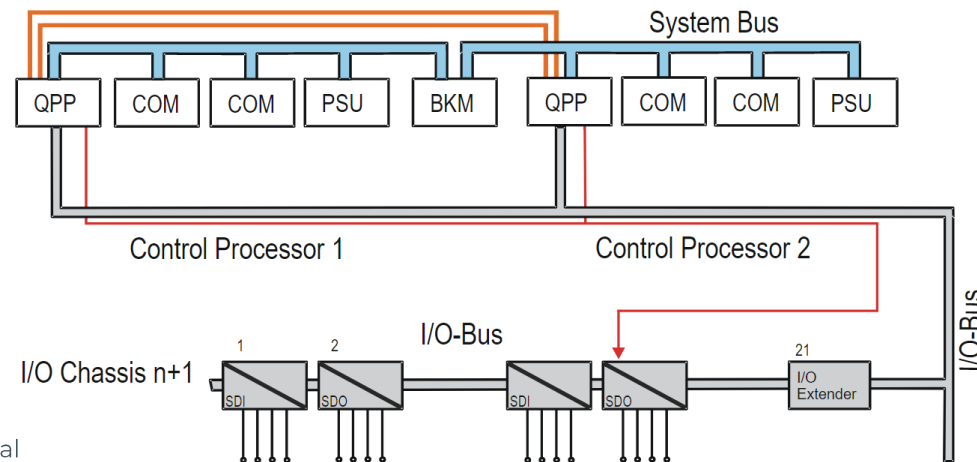
Example: Honeywell Safety Manager (SC) SIS

▶ Safety Manager

- Safety Station compiles SIF FLDs to **unsigned, native machine code**
- Downloads projects using **unauthenticated Safety Builder protocol**
- USI module sends logic via backplane to QPP CPU which **executes SIF logic**



Source: Honeywell Safety Manager manual

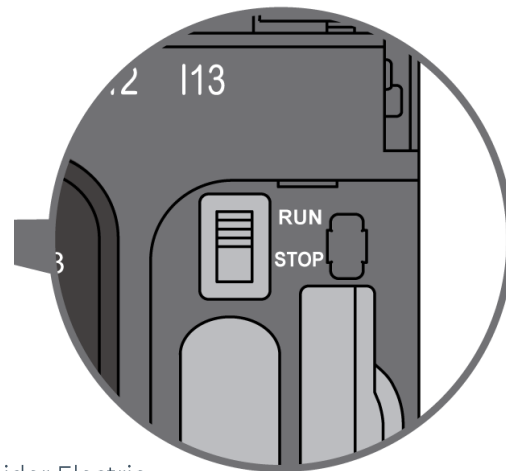


▶ Safety Manager SC (S300)

- SIF FLDs compiled to **mnemonic bytecode** instead

Nuance: Mode Switches

- ▶ ‘Traditional’ defense against logic downloads & FW updates
 - **Physical switch** to set RUN/REM/PROG/IDLE modes

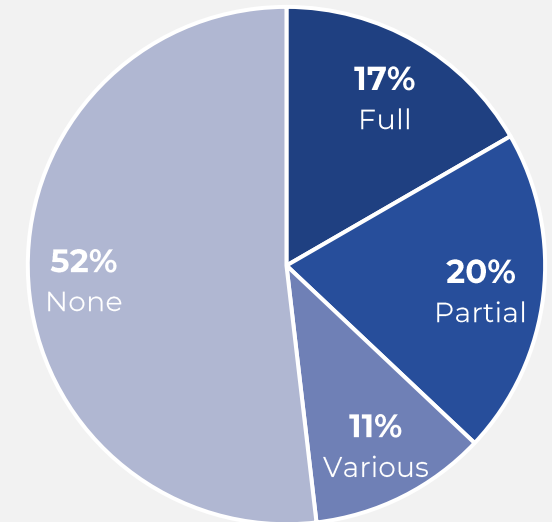


Source: Cyberark, Schneider Electric

▶ Pitfalls

- **Distinctness**: want **distinct** RUN / PROG modes
- **Virtual switches**: just a setting in EWS software
- **Exception modes**: instruct PLC to ignore switch settings
- **Defaults**: not all sensitive ops require switch settings by default

Mode Switch Support



Example: Emerson ControlWave PLC/RTU

- ▶ **Unsigned** firmware updates (CVE-2022-30262)
 - Troubling combined with **BSAP/IP auth bypasses**
- ▶ “*Not a vulnerability*” according to Emerson since
 - Keyswitch can be set to RUN, config setting can disable remote changes



<code>_APPLICATION_LOCKED</code>	<code>%MX 3.103.0 : BOOL</code>	4.50	When set TRUE, prevents external control changes to project via ControlWave Designer. Also prevents project downloads.
----------------------------------	---------------------------------	------	--

Source: ControlWave Micro Instruction Manual, ControlWave Designer Programmer's Handbook

- ▶ **However**
 - Keyswitch has **REMOTE** mode, Attacker can still **wait for legitimate window ...**
 - `_APPLICATION_LOCKED` **not set by default**, **prohibits all remote changes**

Example: Honeywell Safety Manager SIS

- ▶ QPP module keyswitch must be **IDLE** before logic download
- ▶ BKM **RESET** keyswitch must be triggered *after* logic download
- ▶ Except when “*remote load/reset*” are enabled!
 - Physical key needed to enable feature
 - But if enabled for historical reasons and not documented in ISMS or overlooked, **might lead to blind spot**

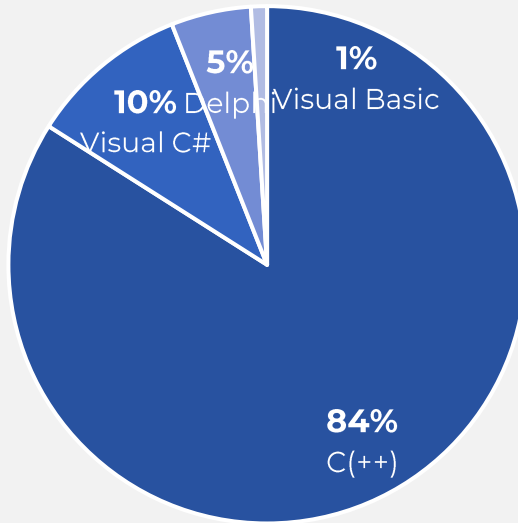


Reverse Engineering Effort

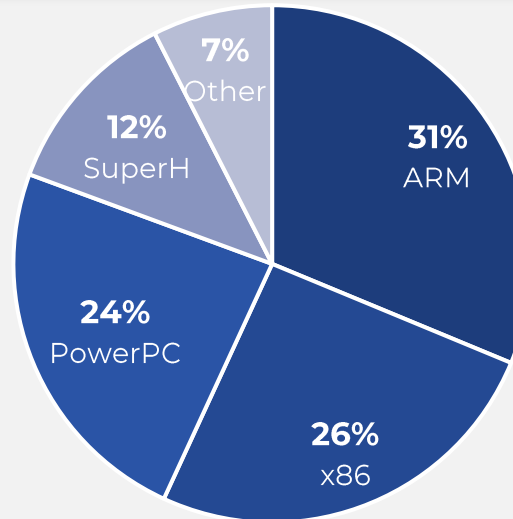
Reverse Engineering

For offensive OT capability development

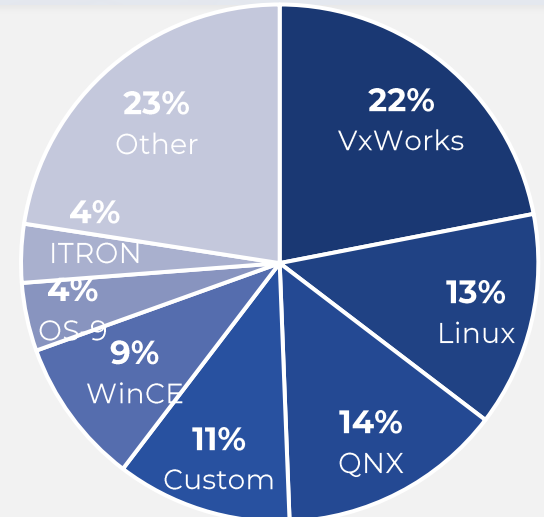
Dev. Languages



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)

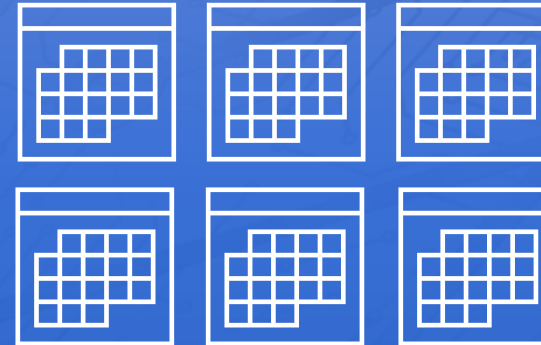
Offensive Capabilities are Feasible to Develop

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

Mitigations & Conclusions

Mitigations



Also see vendor & CISA guidance

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

Conclusions

- ▶ Insecure-by-design **continues to persist** in production install base despite decade+ of hardening efforts
- ▶ Need to get clearer on what *secure-by-design* **actually means**
 - Many security controls turn out to be **trivially broken**
 - Products with broken controls **continue to be certified**
 - Vulns sometimes **dismissed** “because VPN+FW”, even if risk **not fully controlled**
 - Security **retrofits sometimes miss the point** (e.g. IP ACL on UDP protocol)
 - Fixes frequently **don’t address root cause**
 - Lack of variant hunting suggests **immature SDLCs**
 - Should be **secure-by-default**, not “there’s options somewhere in the manual”

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

Thank you.

