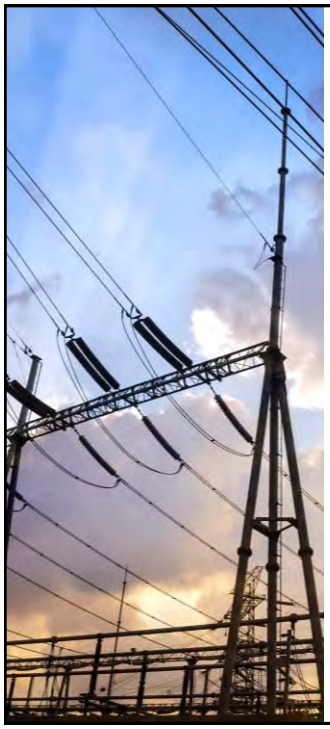


Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation

Mauricio Silveira, David Dolezilek, Jaya Yellajosula, and Scott Wenke
Schweitzer Engineering Laboratories, Inc.

Limited-vulnerability design methods create better understanding and specifications

Identify and investigate design gaps

↓

Recognize vulnerabilities associated with design gaps

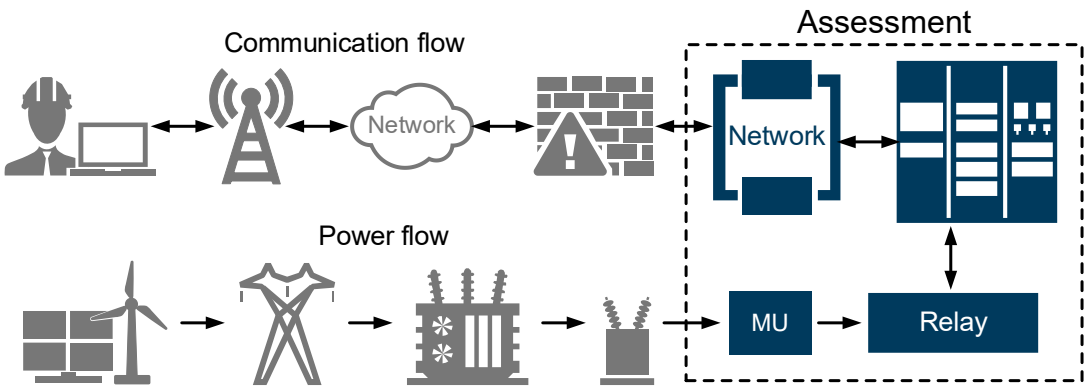
↓

Recognize risks associated with vulnerabilities

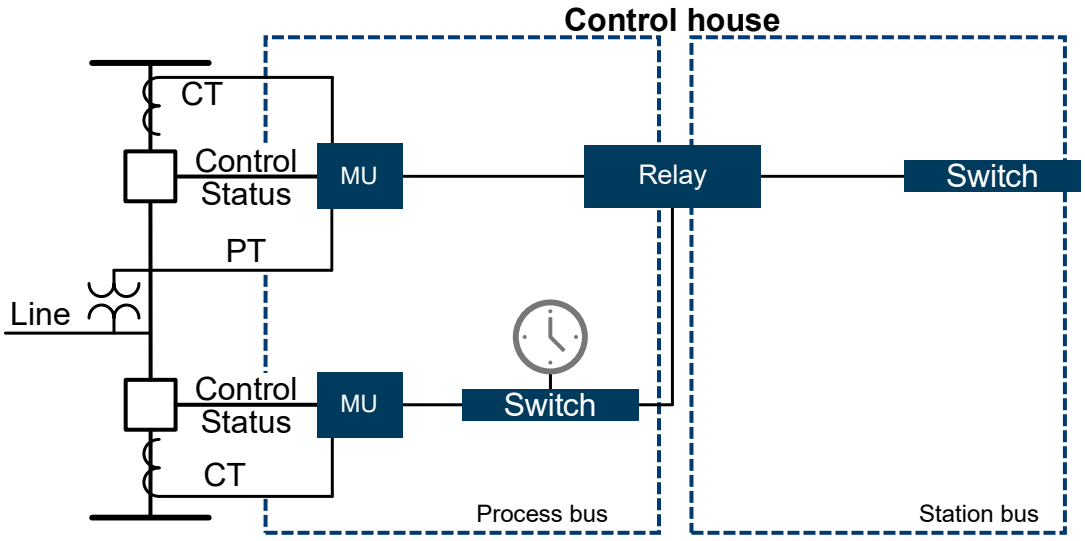
↓

Limit vulnerability based on cost, schedule, and performance design choices

Improve systems by assessing performance



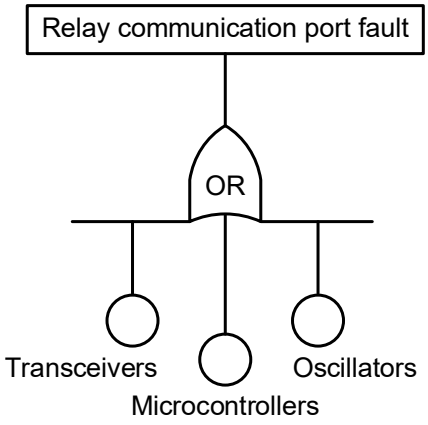
Digital secondary system



Event tree construction

IEC 60870 fault tree

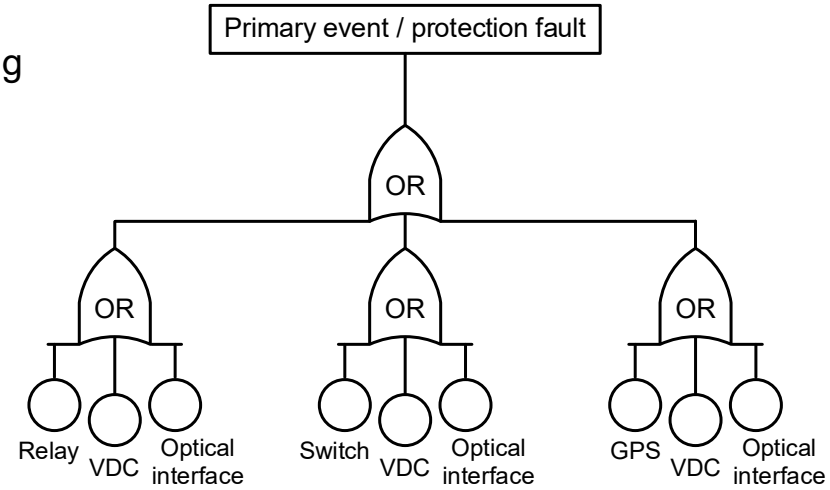
Failure analysis using system component unavailability



Event tree construction

IEC 60870 fault tree

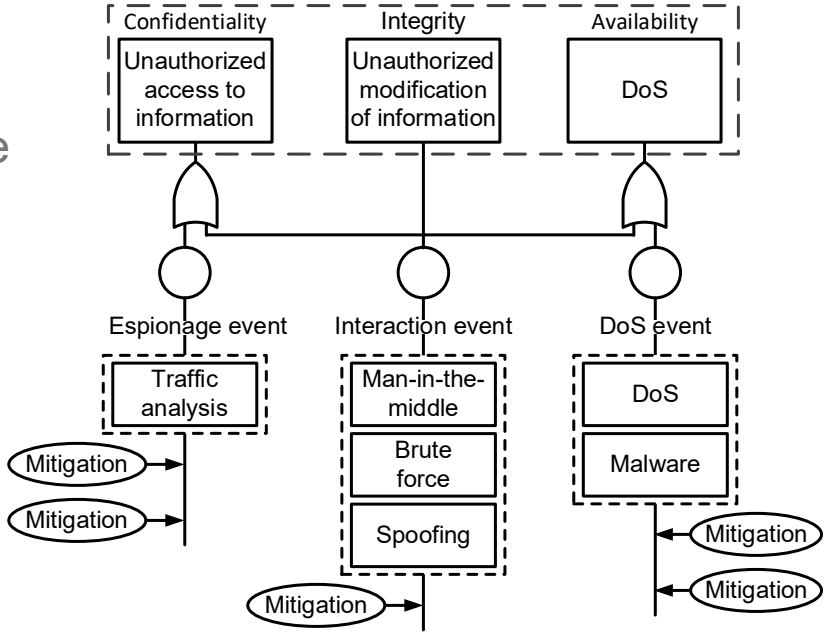
Failure analysis using system component unavailability



Event tree comparison

Cyber attack tree

Attack analysis using threat availability

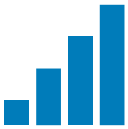


Understanding what to measure

Three major threats to consider for DSS applications

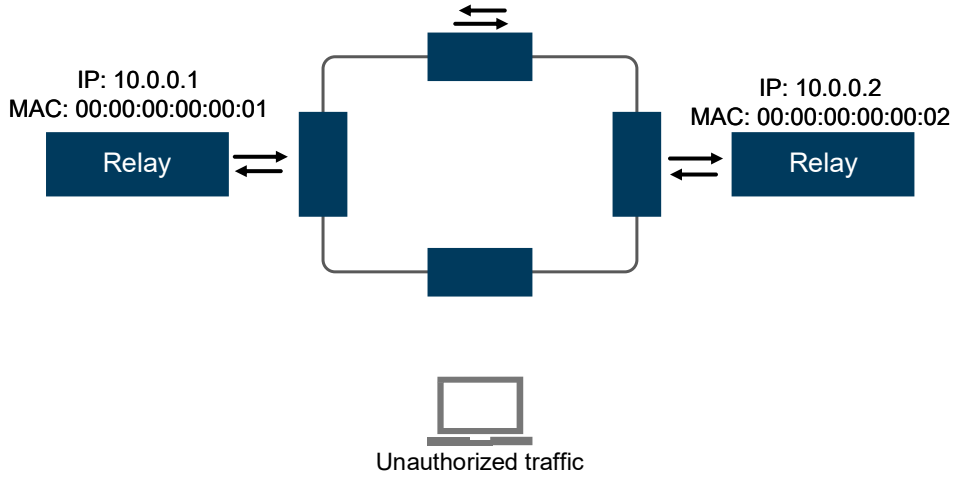
Confidentiality

Integrity

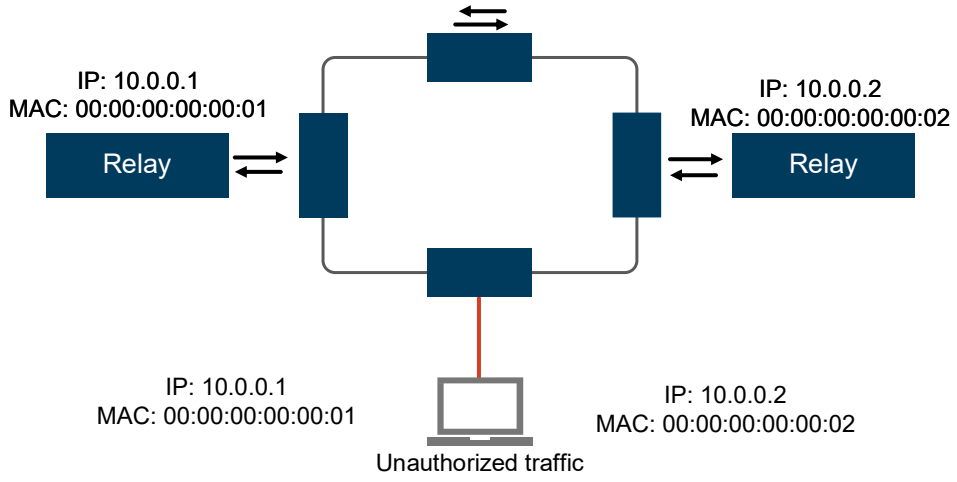


Availability

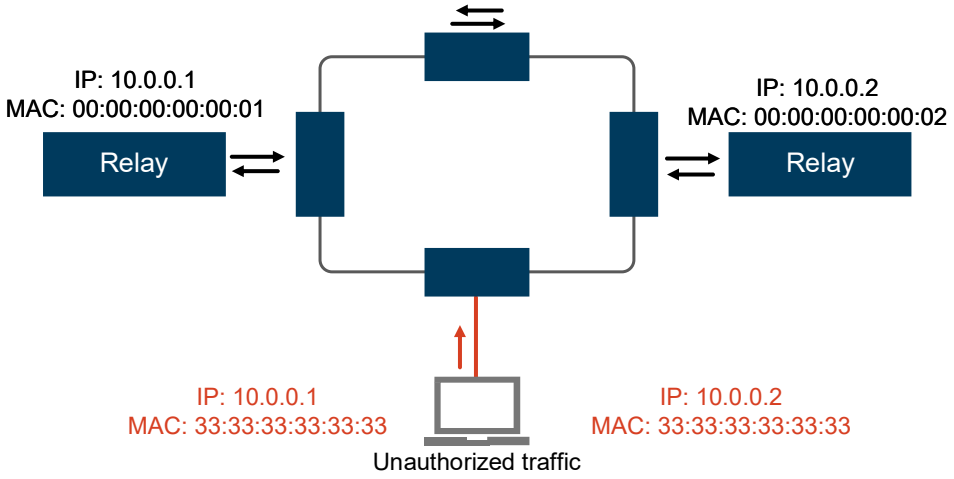
Event leaves: espionage, interaction, and DoS



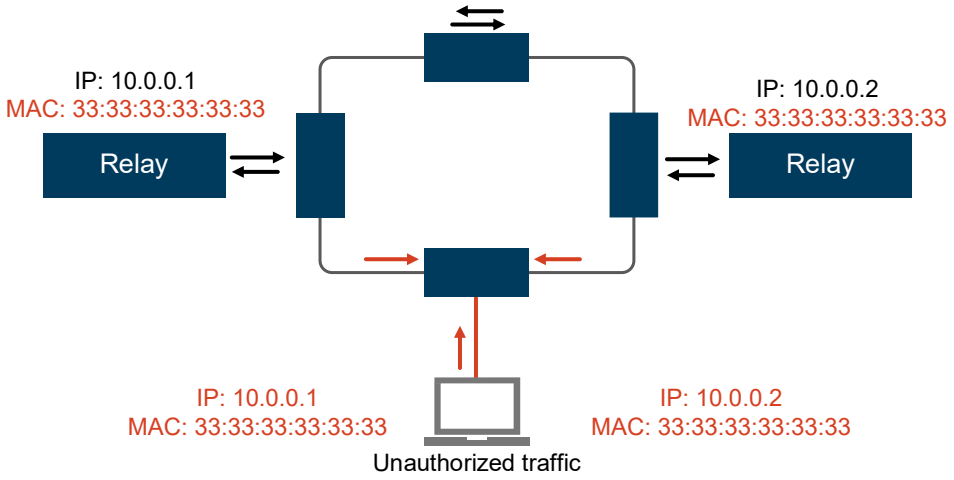
Event leaves: espionage, interaction, and DoS



Event leaves: espionage, interaction, and DoS

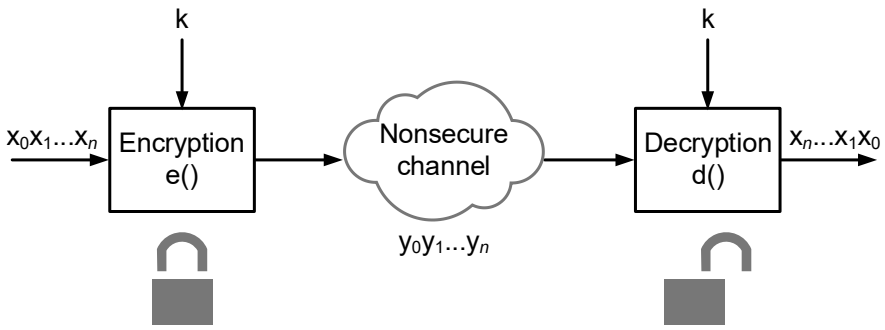


Event leaves: espionage, interaction, and DoS



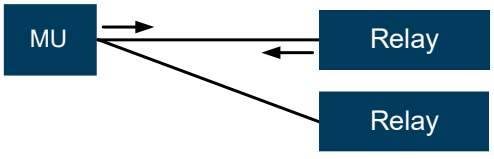
Mitigation leaves

- Cryptography



Mitigation leaves

- Cryptography
- Network architecture



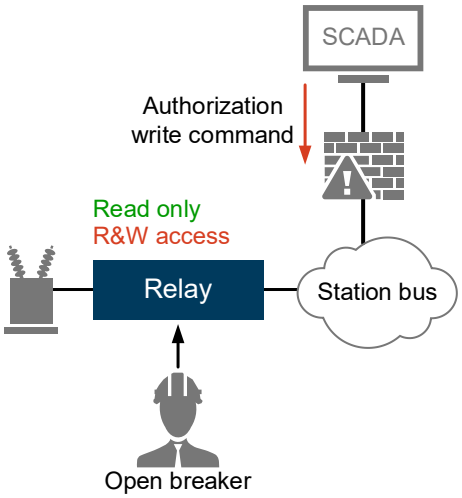
Not all cyber threats are created equal

$$\alpha_{total} = \textbf{Threat availability (TA)} = \sum_{i=1}^{n} \text{VS} + \sum_{i=1}^{n} \text{Power outage (hours)}$$

Espionage events	Communications bus	VS	Power outage (hours)	TA
Sniffing process bus network switched	Process	6.2	0	6.2
Sniffing OT-SDN process bus	Process	3.8	0	3.8
Sniffing process bus point-to-point architecture	Process	3.8	0	3.8

Low cybersecurity exposure in DSS

- Read / write access necessary about every 5 years
- Authentication transaction lasts seconds
- Most likely not via remote communication



Does solution address problem?

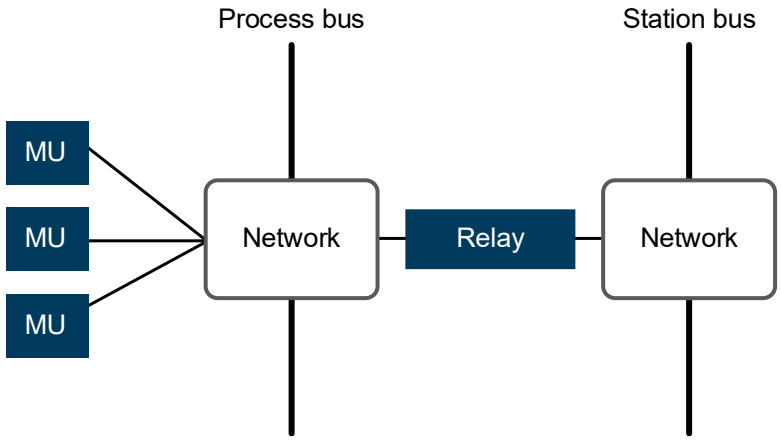
$$\Omega = \text{Resilience} - \text{Complexity}$$

Level	Value
Low	0–3
Medium	4–6
High	7–10

- Resilience
  - 0 = More vulnerable
  - 10 = Less vulnerable
- Complexity
  - 0 = Less complex
  - 10 = More complex

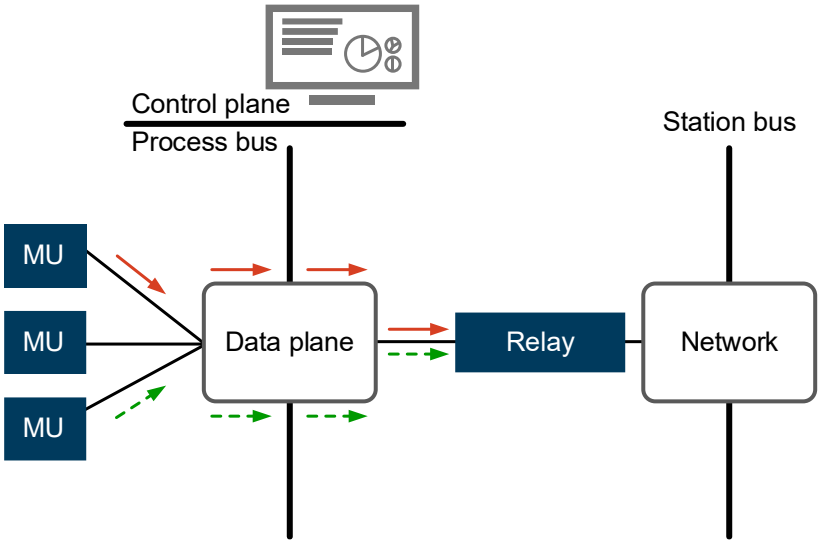
Security networks architectures for DSS

- Switched network



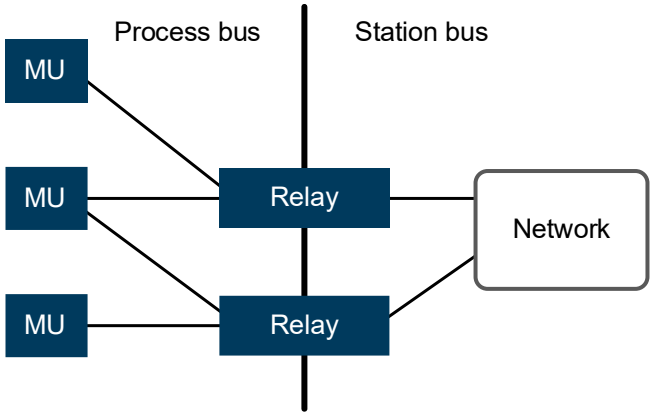
Security networks architectures for DSS

- Switched network
- Switched network OT-SDN



Security networks architectures for DSS

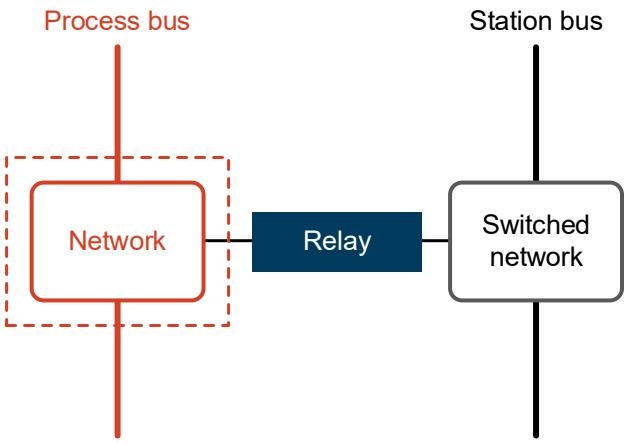
- Switched network
- Switched network OT-SDN
- Point-to-multipoint



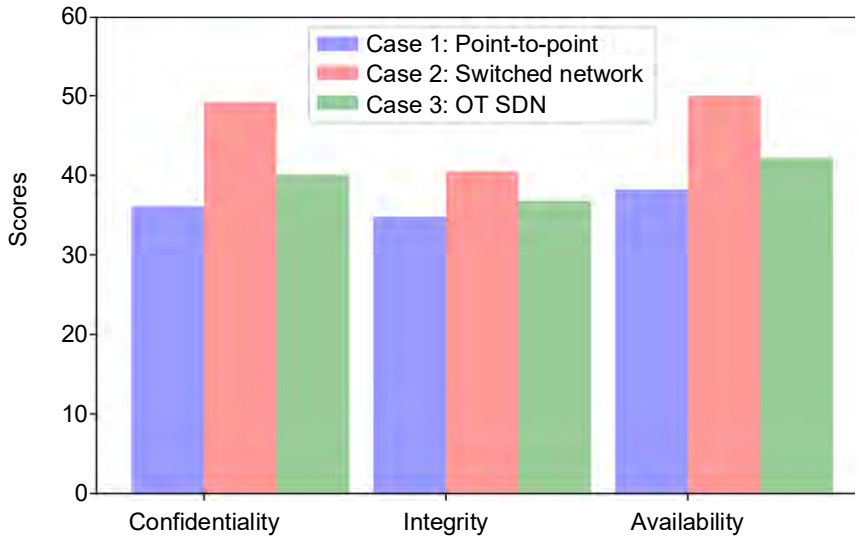
Comparing three process bus architectures

Three process bus scenarios

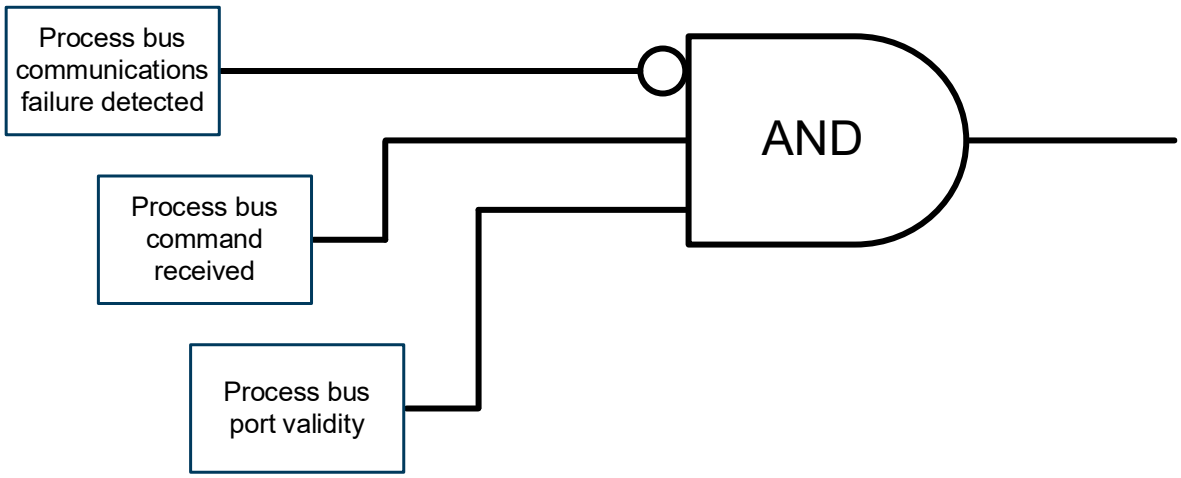
- Point-to-point
- Switched network - VLANs
- OT-SDN



Privacy is superior to secrecy



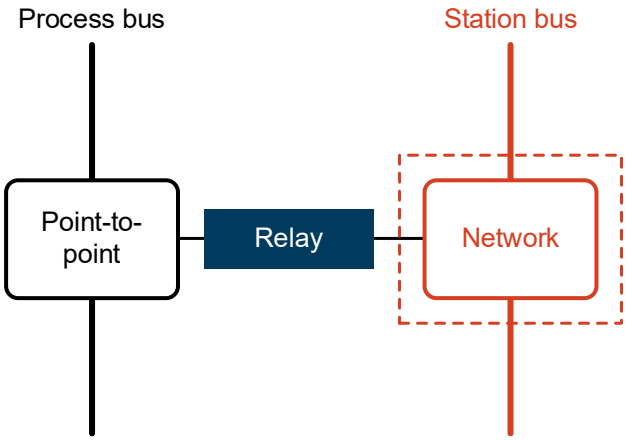
Attack on private connection is detectable



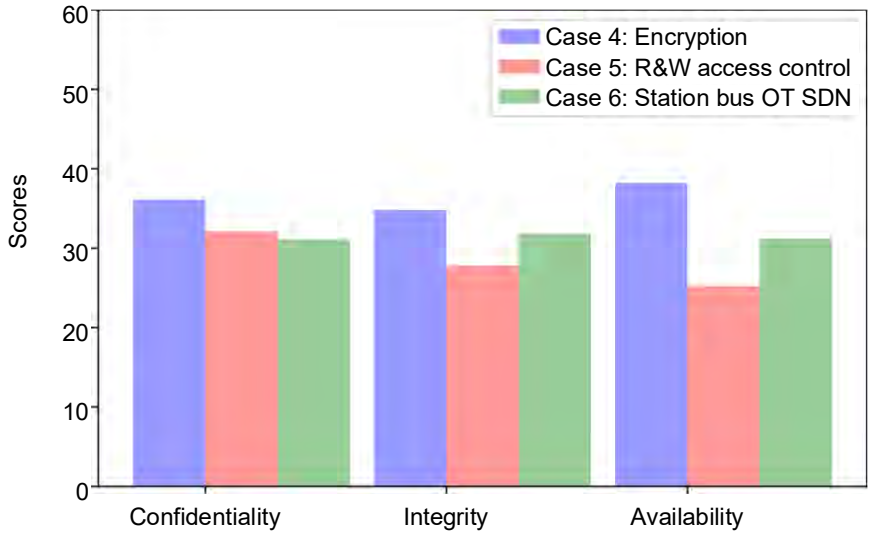
Station bus secrecy vs privacy

Three station bus variants

- Switched network with cryptography
- Switched network with R&W access control
- OT-SDN

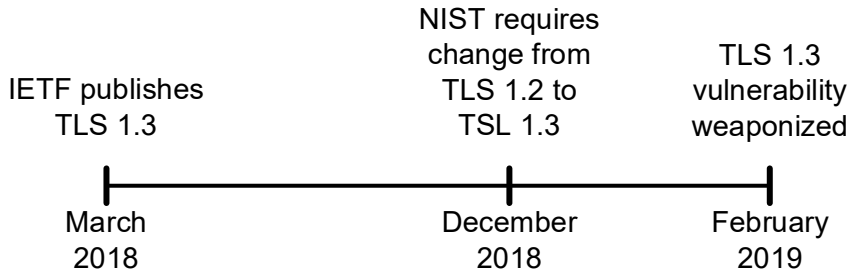


Privacy is superior to secrecy



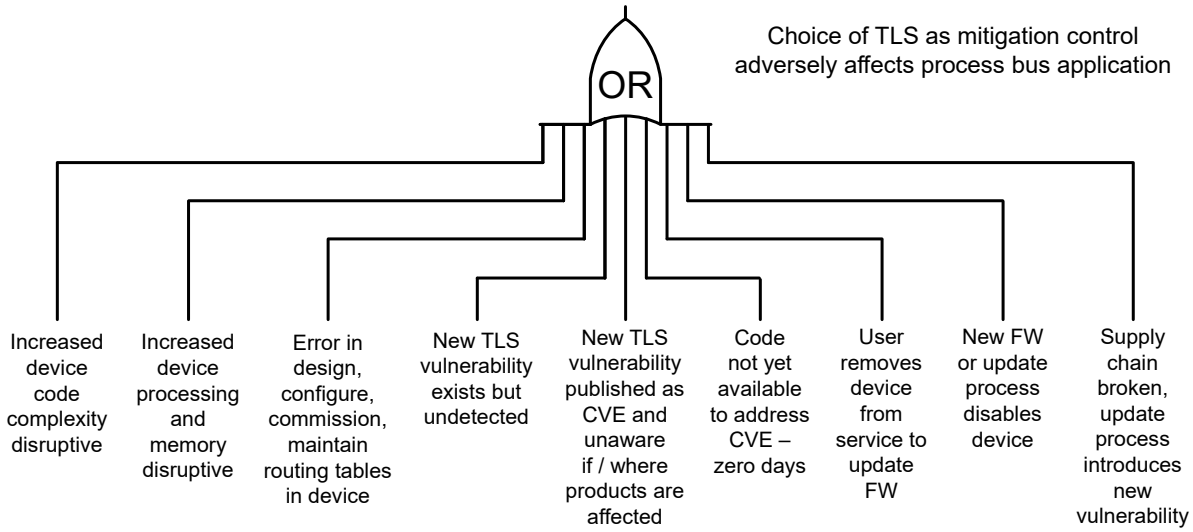
Recent weaponized vulnerabilities – TLS

"IT TLS doesn't belong in OT relays" –DARPA



IETF – Internet Engineering Task Force, defines internet standards

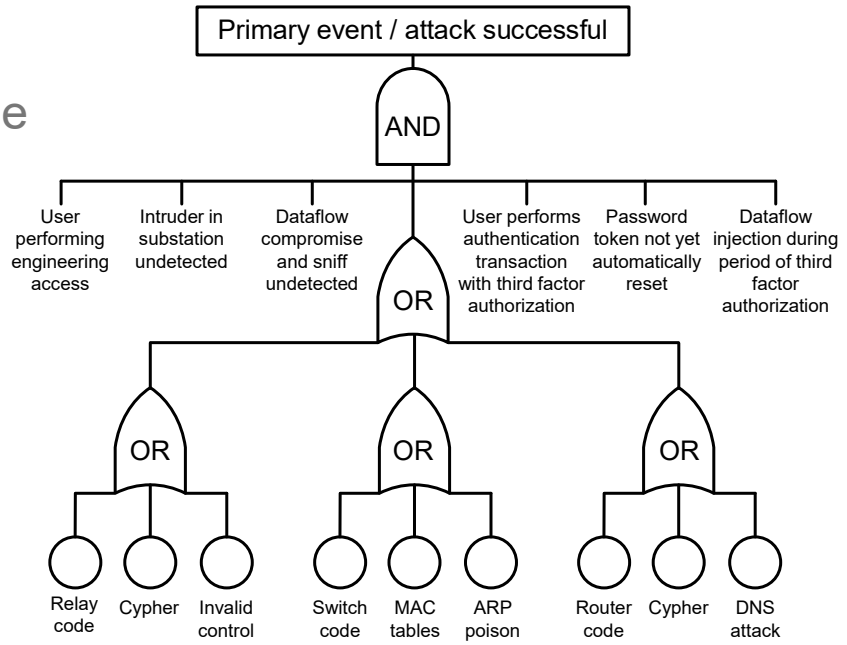
Vulnerability chain



Conclusion

Cyber attack tree

Attack analysis using threat availability



Questions?