ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

# Considerations for securing the Industrial Network

MARCH, 2019

IEEE802.1 PLENARY, VANCOUVER, BC.

JORDON WOODS

LEI POO

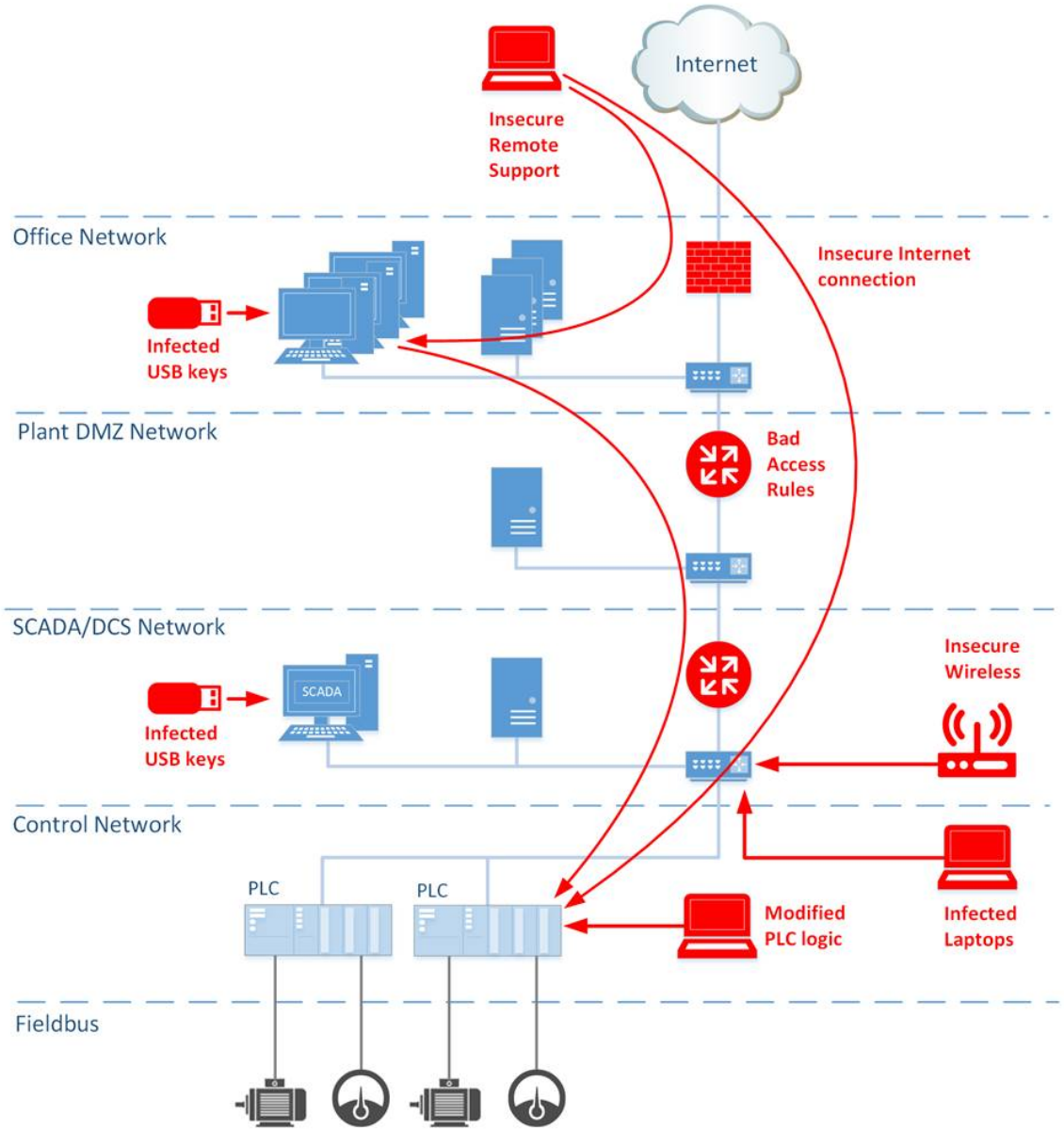
# Agenda

- The need
  - What's in the current draft?
  - What should the profile cover in terms of security
- What should we worry about?
  - What threats models have we seen in the market?
- What are the trade-offs?
  - Likelihood of an Attack versus Impact of an Attack
- Next Steps

# The Need

- What's in the current draft?
  - The security section of D1.0 contains references to MACsec and associated amendments, Secure Device Identity, and port-based access control.
  - All cited specifications are optional.
  - This contributor is aware of no industrial use cases requirement for layer 2 security.
- Developers, providers, vendors, and users of networking services and components for industrial automation equipment require some guidance regarding security measures for these products.
  - Which threat models are appropriate?
  - What vulnerabilities do those threats imply?
  - What mitigations are appropriate?
  - For high performance applications, what are the trade-offs between security and performance?
- Is P60802 the appropriate vehicle to provide these guidelines?

# Threat Landscape for ICAS

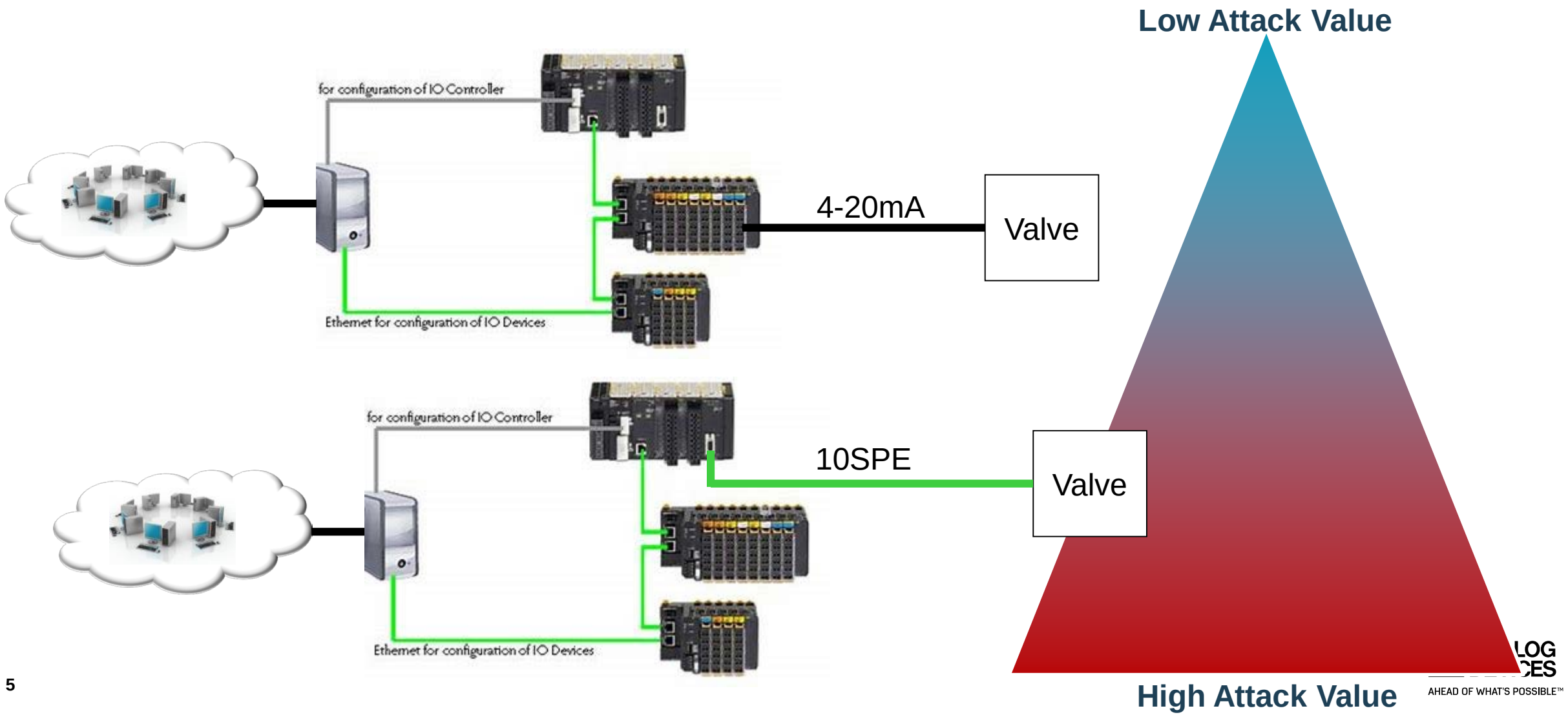



https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

**Attack vectors of concern:**

- introduce **malware** to the control system either remotely or through unsecured ports
- **pass information to unauthorized locations** external to the control system
- introduce **excessive network loading** that can be used to create security problems or launch attacks on the control system
- **physical attacks** causing Denial-of-Service downtime or undetectable spoofing

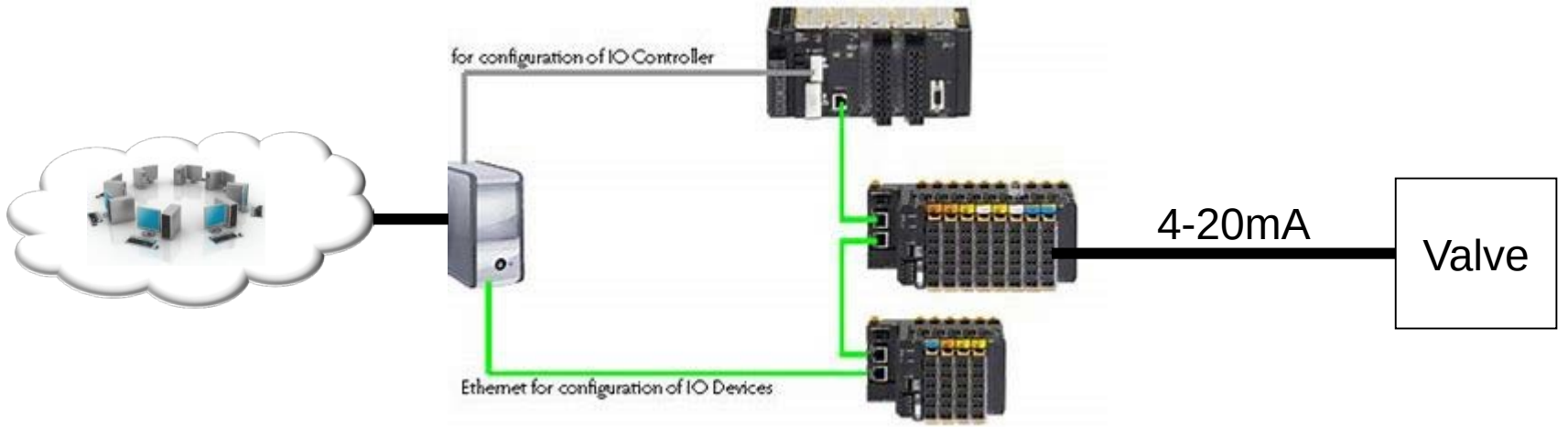
# Likelihood of an Attack versus Impact of an Attack

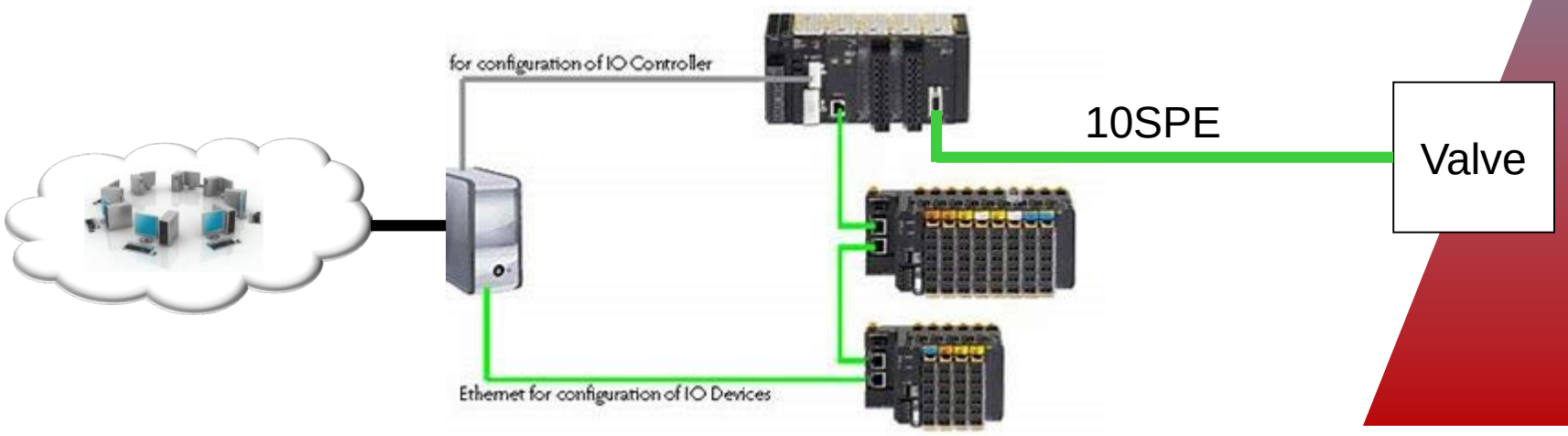


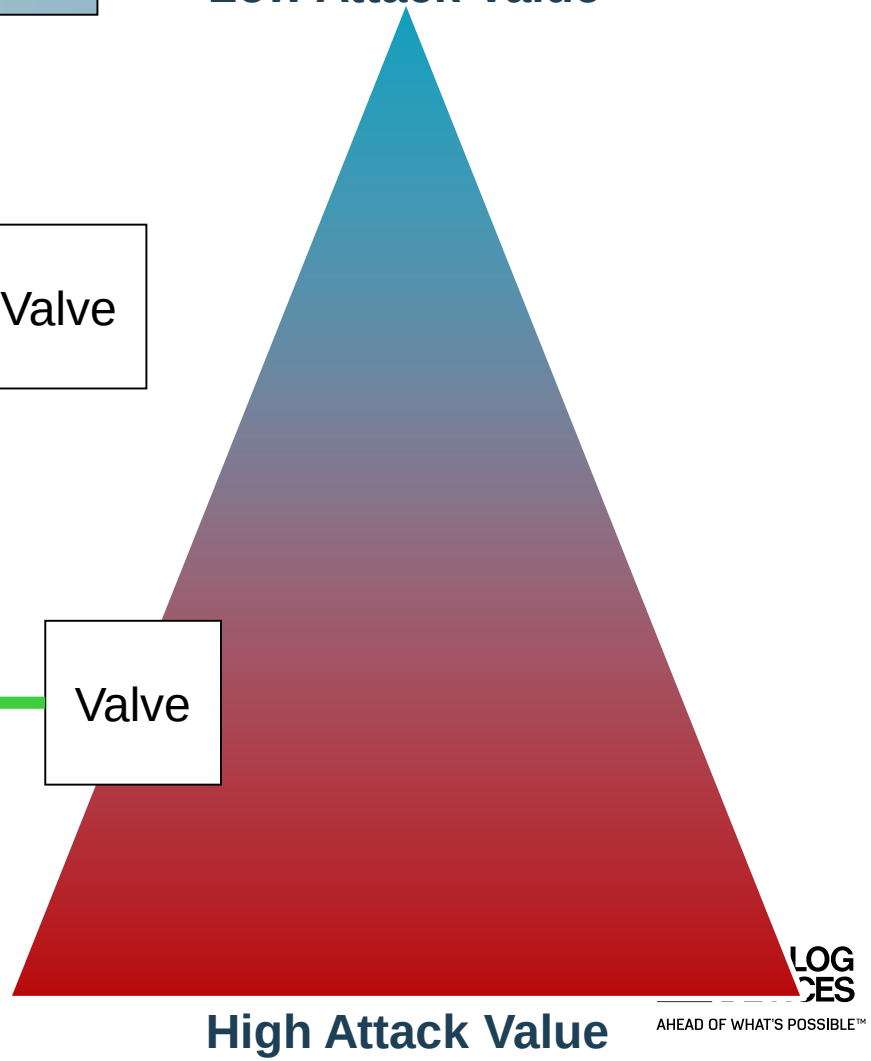
# Likelihood of an Attack versus Impact of an Attack

- Likelihood increases with ease
- Impact is the amount of damage

Low Attack Value means little return for amount of work



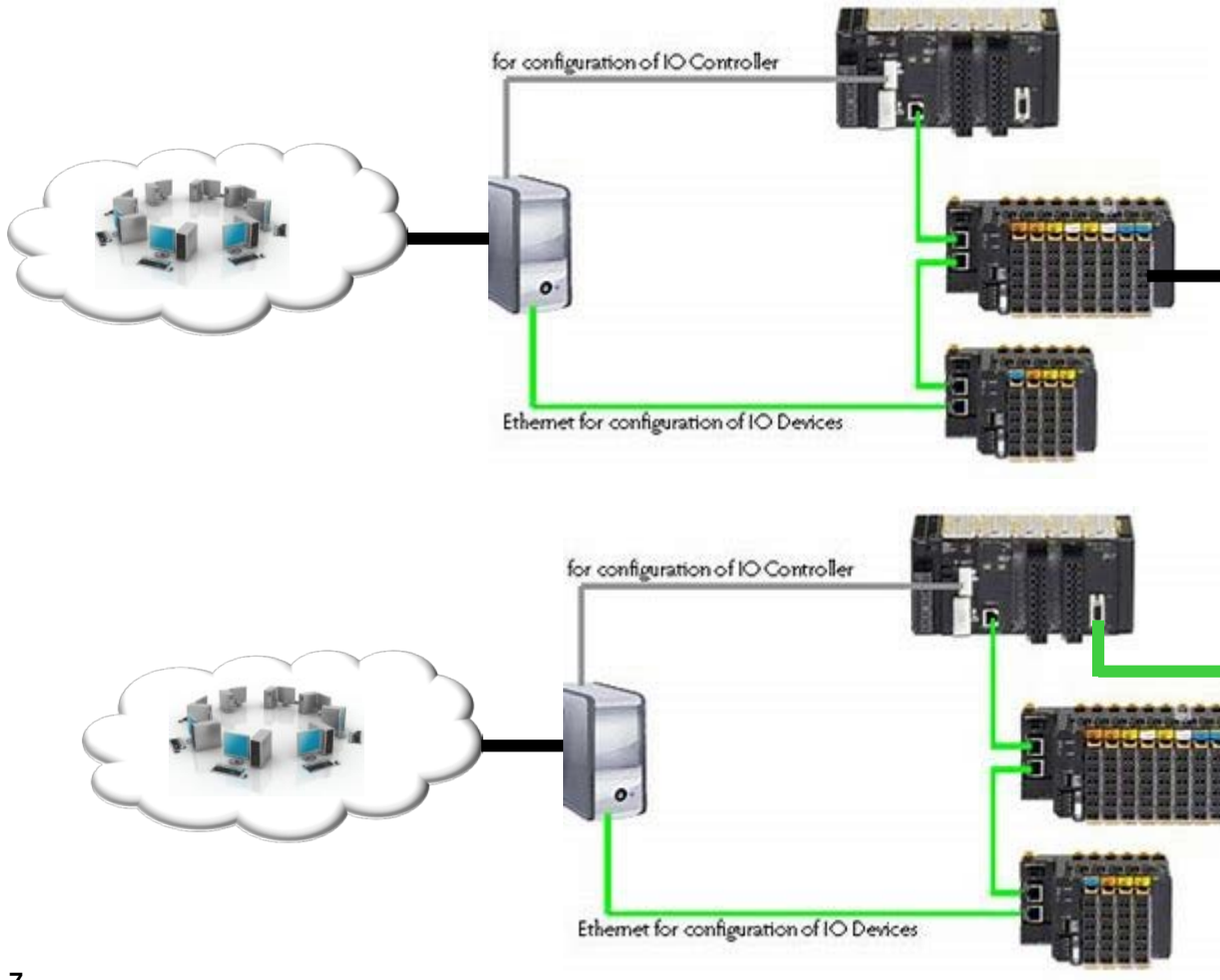



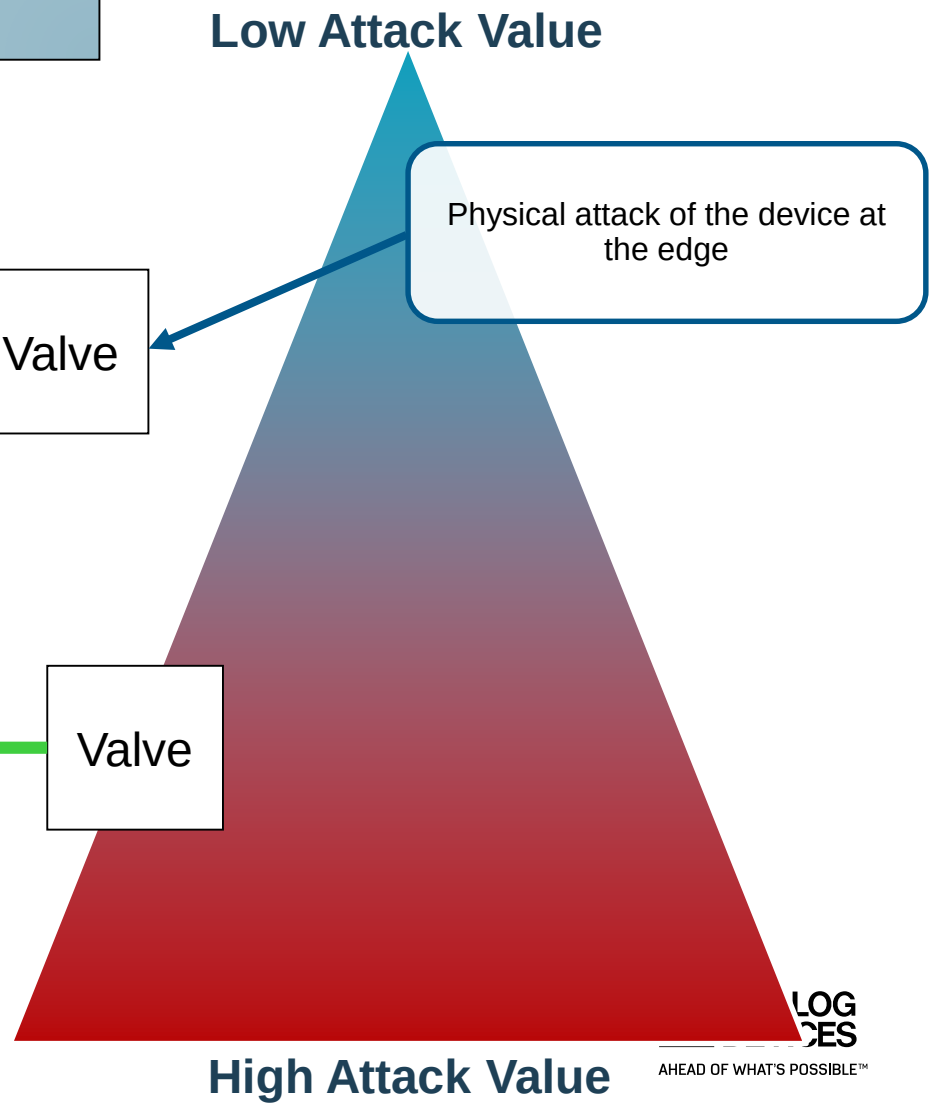



# Likelihood of an Attack versus Impact of an Attack

- Likelihood increases with ease
- Impact is the amount of damage

Low Attack Value means little return for amount of work

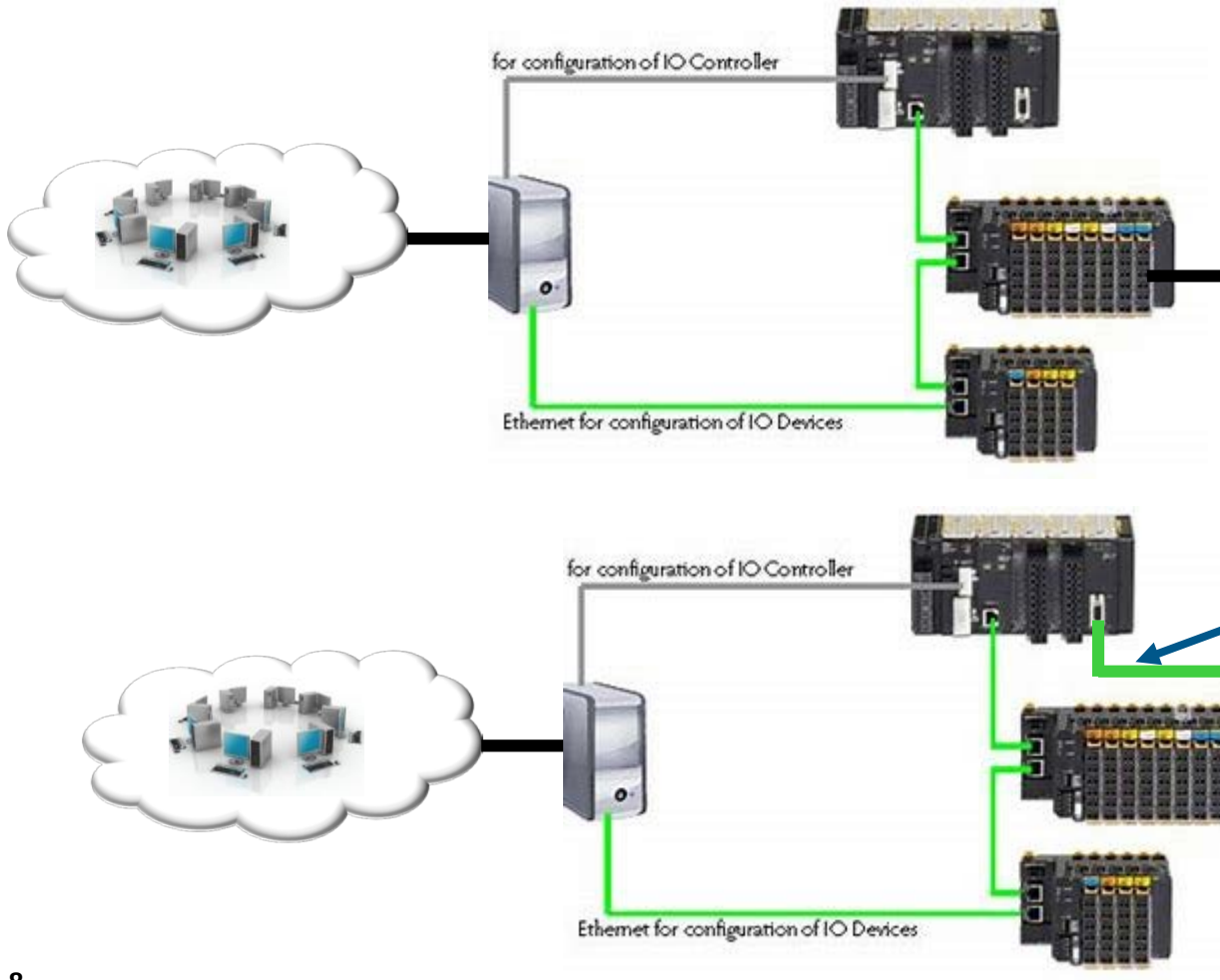


# Likelihood of an Attack versus Impact of an Attack

- Likelihood increases with ease
- Impact is the amount of damage

Low Attack Value means little return for amount of work




Low Attack Value

Physical attack of the device at the edge

Read unencrypted data across the wire

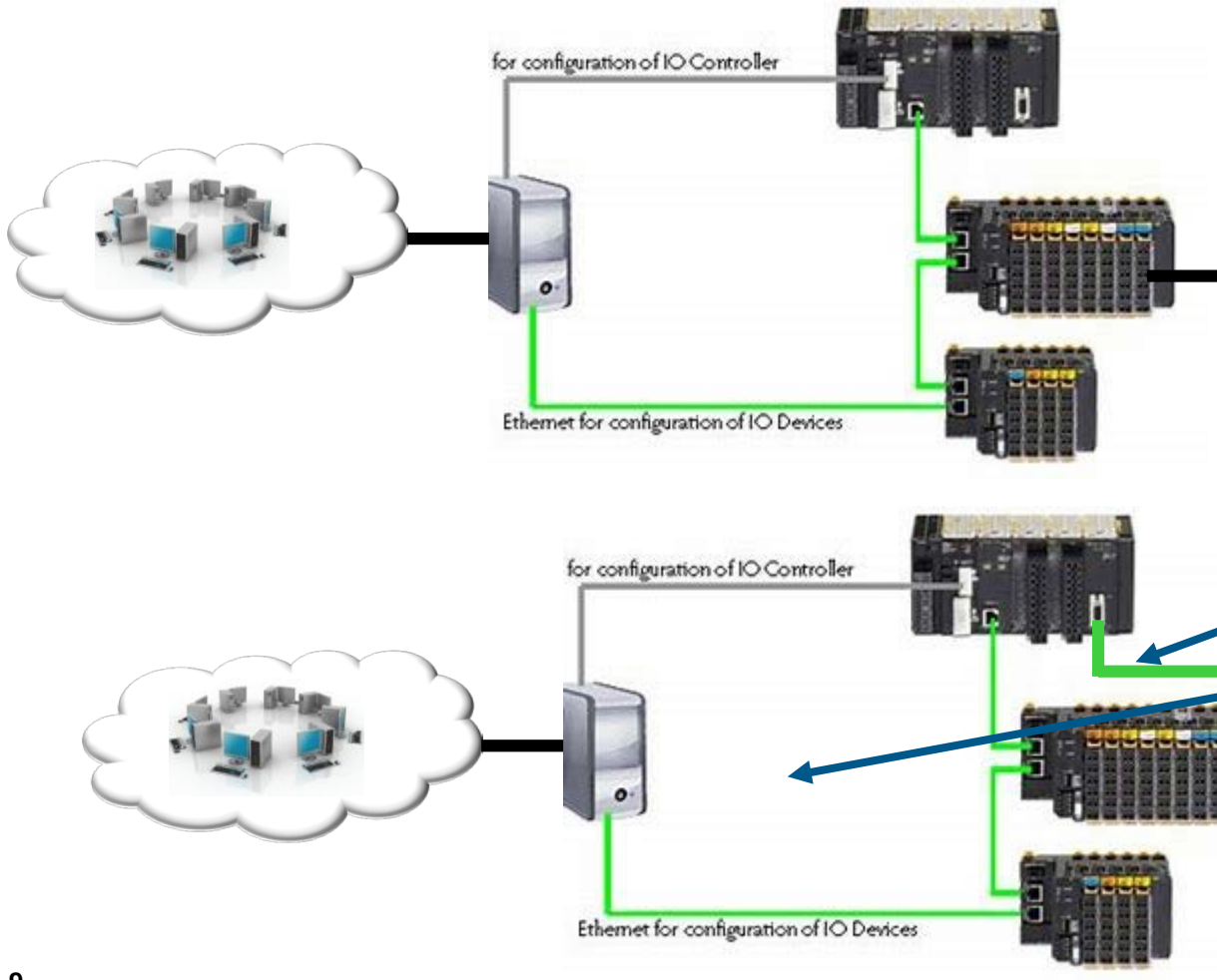
High Attack Value

AHEAD OF WHAT'S POSSIBLE™

# Likelihood of an Attack versus Impact of an Attack

- Likelihood increases with ease
- Impact is the amount of damage

Low Attack Value means little return for amount of work




Low Attack Value

Physical attack of the device at the edge

Read unencrypted data across the wire

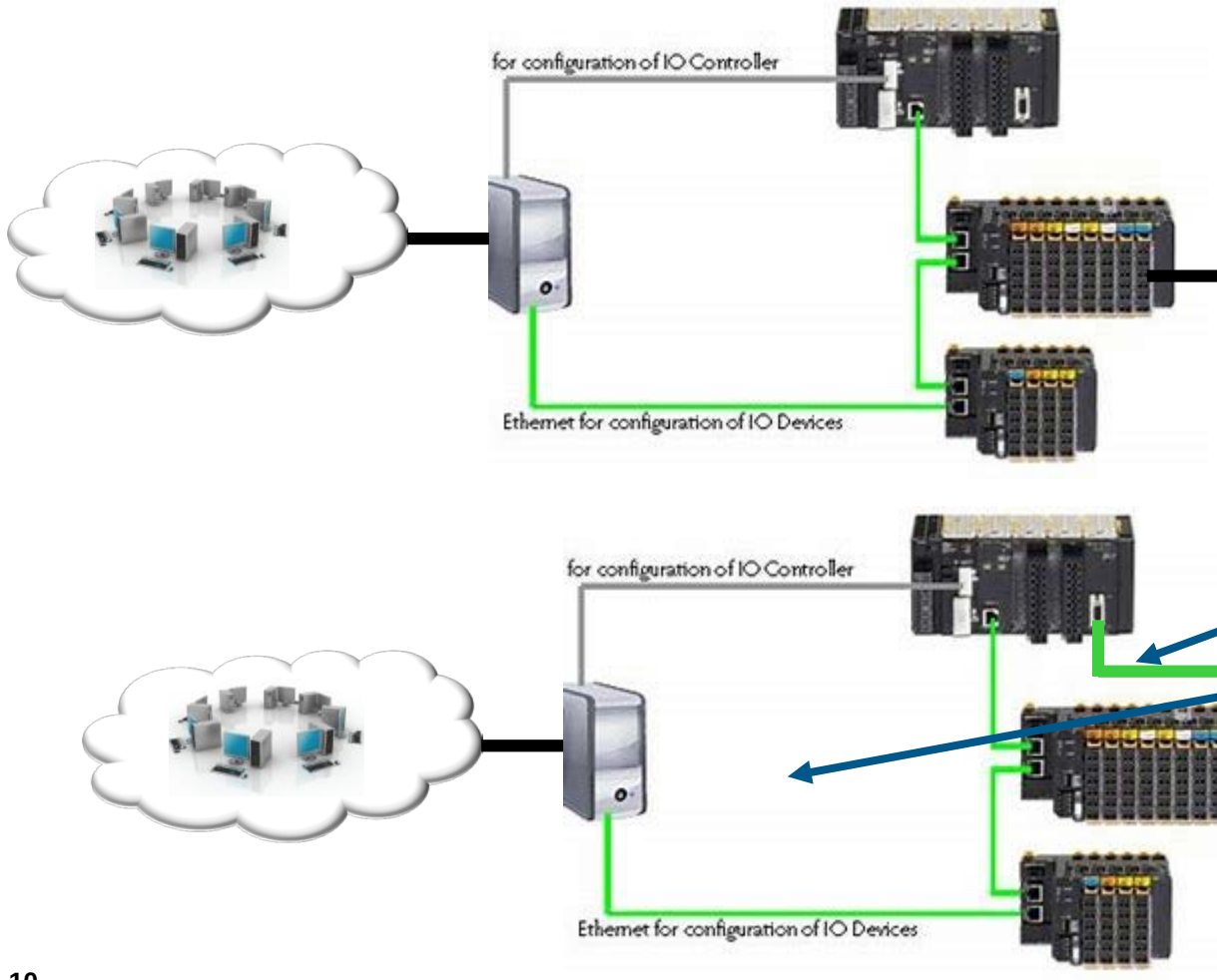
Plug into the factory network and attack unsecured devices

High Attack Value

# Likelihood of an Attack versus Impact of an Attack

- Likelihood increases with ease
- Impact is the amount of damage

Low Attack Value means little return for amount of work




Low Attack Value

Physical attack of the device at the edge

Read unencrypted data across the wire

Plug into the factory network and attack unsecured devices

Attack the network or other devices on the network through physical attack of the device at the edge

High Attack Value

# Next Steps

- This contributor favors an approach for security that highlights threats and mitigations rather than specific mitigation mechanisms.
  - Focus should be on what the Joint Project can do (w.r.t. security in Industrial Networks) that would accelerate the adoption of TSN into Industrial markets.
  - Need to determine what risks can be minimized by implementing mitigations.
  - Mitigations are generally a trade-off decision – security comes with a cost.
- This contributor will provide contributions to the draft if the Joint Project agrees this is an appropriate topic for the profile.

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

# Thank You