midokura
cloud enabling technologies

OpenIoTSummit

Journey to an intelligent Industrial IoT Network

Pino de Candia
OpenIoT Summit, Portland, 2017

About me: Pino de Candia

- Midokura CTO
- Expertise in SDN for Data Center virtual workloads
- Previous work on NoSQL databases and caching systems
- Software developer, architect and team manager

About Midokura

- Founded in 2010
- Created and maintains MidoNet
- Open Source SDN for OpenStack, Kubernetes, vSphere, Eucalyptus
- OEMs with Dell and Fujitsu
- Working on virtual networking for Fog and IIoT (SmartFactory)

About this talk

- Industrial network challenges (factory/plant focus)
- Compare/contrast to Data Center
- What is an intelligent network
- Why virtualization is essential

What I mean by “Industrial IoT”

- Extract more information from OT
- Add sensors and devices for data acquisition
- Process the data in the cloud
- Systematic optimization of the whole production pipeline
- Acceleration of innovation cycle

General Challenges

- Explosion of smart IP-enabled devices (not traditionally connected)
- Vertical end-to-end solutions that don't integrate
- Technology fragmentation
- Dynamically changing set of people, services, solutions, sensors, and cells/locations.
- Changing team dynamics

Security Challenges

Heavily targeted

OT natively has few defenses

IT ≠ OT security

Need OT-specific Firewalls

Remote access

Auto-updates

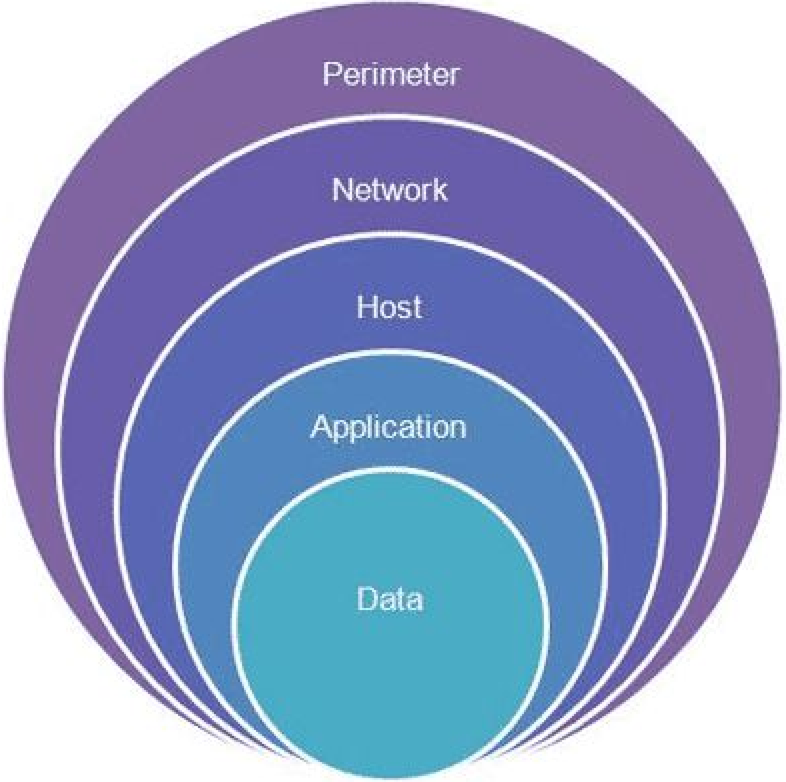
Fragmented community

Domain-specific certifications

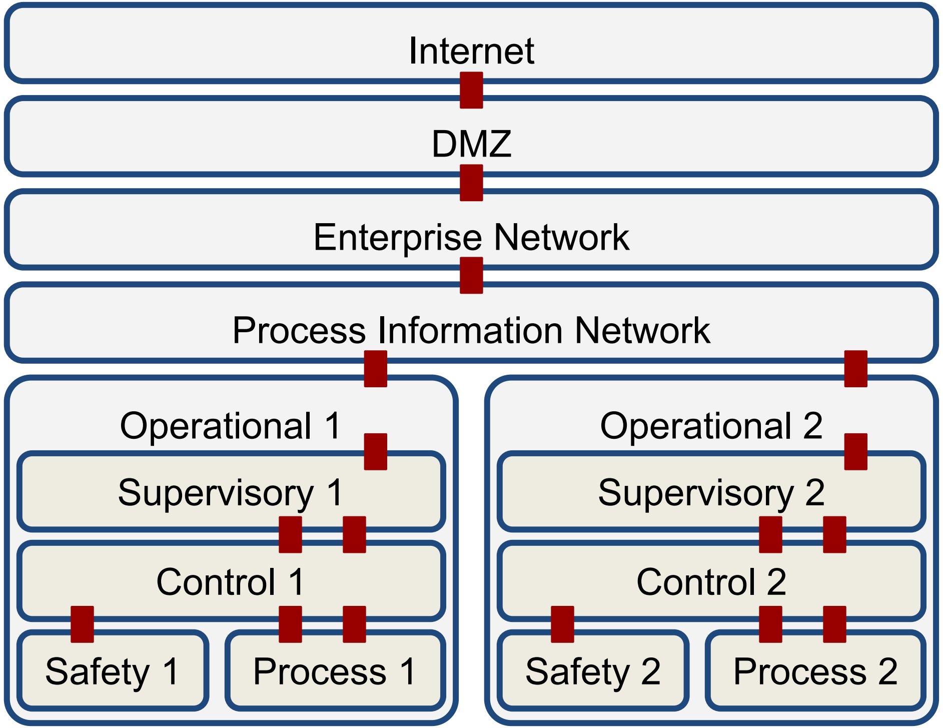
The air gap has long been a fantasy

Defense in Depth

- Layers of defense, like in a fortress.
- Includes company policies and procedures, physical, and digital protections.
- Further layering within each area.
- Segment network into zones and conduits (ISA99).

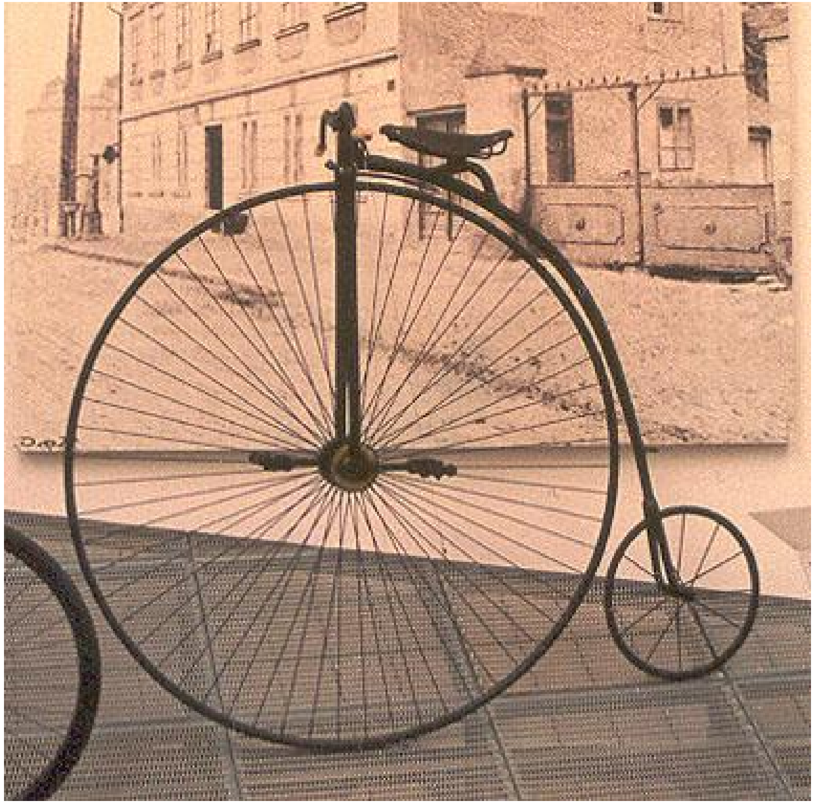


Zones and Conduits



VLANs alone don't solve the problem

- Are you using spreadsheets?
- Zone/conduit design is spread across network switches
- No distinction between intent and current state
- Hard to audit
- Hard to change
- Hard to place Firewalls



What happened in data center networks

Virtualization and cloud stressed the network infra and team.

The network was in the way.

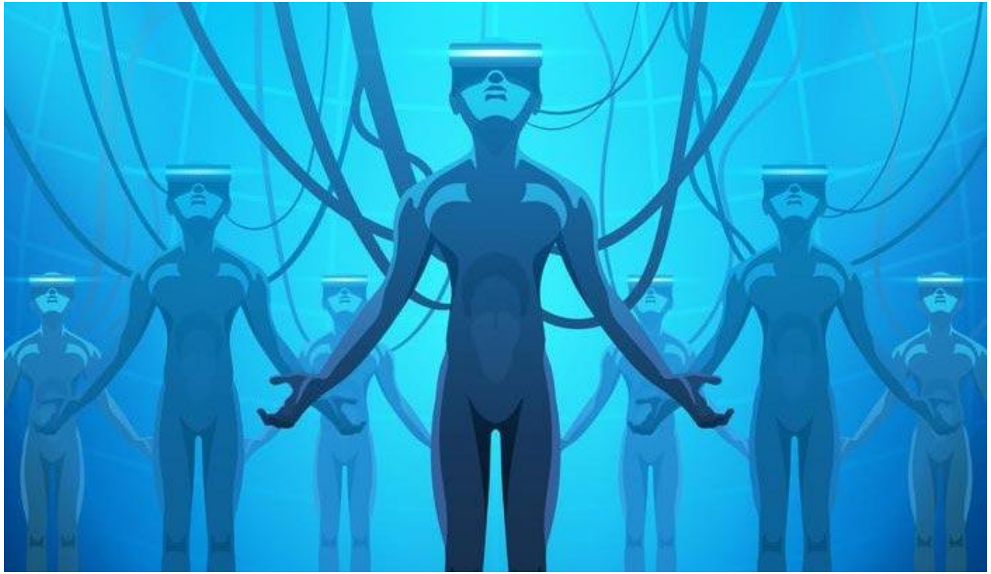
East-West security was an after-thought.

So network evolved to be application-centric.

We virtualized the data center network

Decouple the physical from the logical network topology

Not just L2 and L3



Self-service

Self-troubleshooting

Place any network service anywhere

Micro-segmentation

Intent-based policy

Differences between DC and Factory/Plant networks

- Hardware refresh cycle
- Devops
- Priorities
- Speed of deployment
- Number of applications vs. IoT solutions
- Static vs. dynamic

What is an intelligent industrial network?

Allows layering policy from different teams.

Allows scoped visibility, audit and troubleshooting based on role.

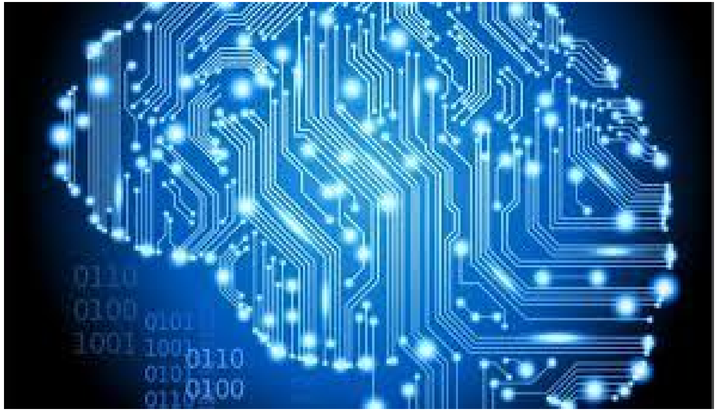
Encrypted links.

Protects devices from each other, even within a zone.

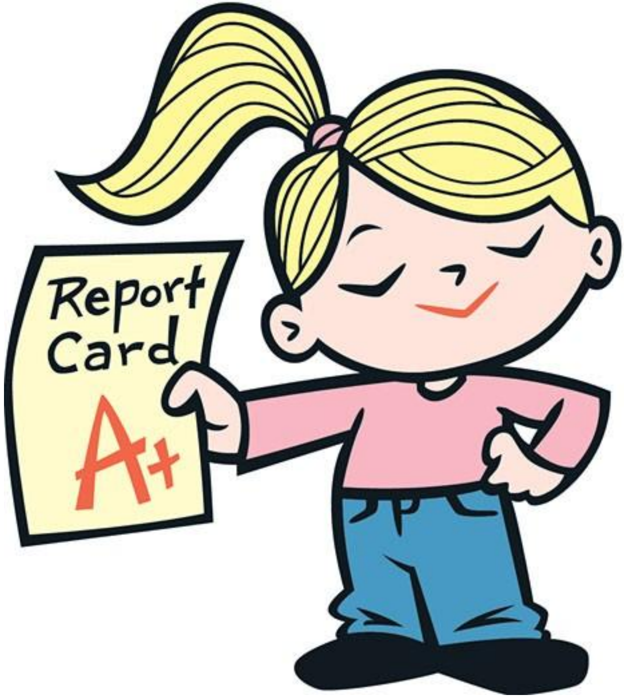
Audit trail - traffic and state

SD-WAN over multiple channels

SPOF (single pane of glass)



What is an intelligent industrial network?



Can be very prescriptive about what to allow - only white-listed traffic allowed.

Learns traffic patterns and detects deviation.

Allows dry-run of new policies

Easy roll-back to previous policy or config

Context-based traffic prioritization

Identity and context-based provisioning

What is an intelligent industrial network?

Policy based on meta-data, not addresses

Per-flow redirection to FW or DPI, IPS/IDS, whatever topology (NFV)

Integration with domain-specific (OT) Firewalls

Layered remote access management

Virtualization, the key ingredient for intelligence

Virtualization, and SDN more broadly, is a key ingredient to achieve this kind of intelligent network.

Overlay networks or not?

Implement at edge or in the fabric?

Some thoughts on Fog and Industrial Ethernet

What role for Open Source?

OpenFog

Kura

omapd - open IF-MAP server (by TCG)

OpenICS

- Can gateways provide network virtualization?
- Should the gateways or the network provide the databus?
- Can we separate GW functionality (data pipelines) from network and security concerns?
- Can we standardize device and patch management?

Thanks and Questions

pino@midokura.com @pino_midokura