Tableau

Future-Proof Zoning for OT Networks

ETH zürich

Piet De Vaere

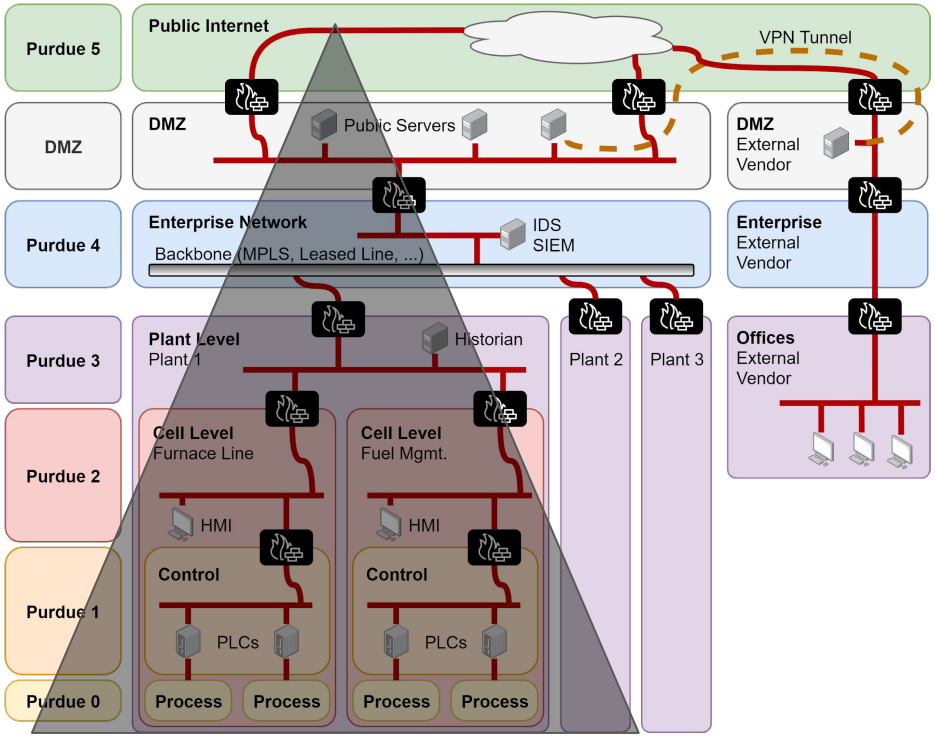
Claude Hähni

Adrian Perrig

Monti Stampa Furrer

Franco Monti

Today's network structure is hierarchical, because ...



… processes are hierarchical

Purdue Model

Control systems collocated with processes

… it is good for security

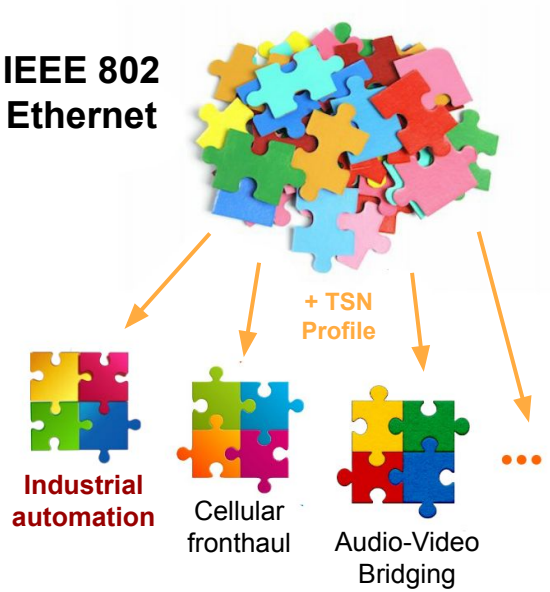
Layered security protects the processes

Changes to the network are challenging Purdue

SDN has taken over the datacenter

IT/OT convergence is bringing SDN to the factory

IEEE Time-Sensitive Networking (TSN) enables standard Ethernet to replace today's fieldbusses



Closer integration
→ **Harder to separate Purdue levels**

Centrally managed technologies
→ **Reduced robustness of distributed security enforcement**

Changes to the automation infrastructure are challenging Purdue

Dedicated systems are replaced by general-purpose components

- IT/OT convergence
- Virtualized Automation Functions: Soft-PLC, Soft-SCADA, Soft-HMI

No need to place virtual functions close to the process

- Placed at the edge
- Placed in the cloud

→ **Logical and physical location must be decoupled**

Changes to information flows ...

Flows increasingly cross more then 1 Purdue level

→ **High management overhead and reduced security**

Changes to threat models ...

Attackers increasingly enter at lower Purdue levels

→ **Incremental security undermined**

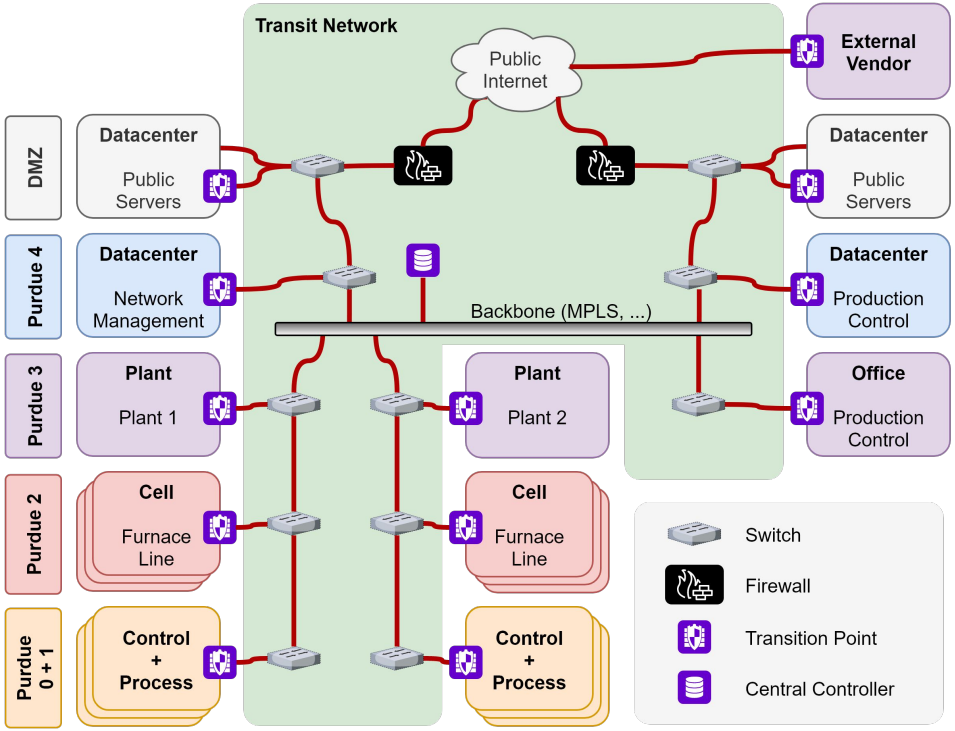
Changes to operation models ...

Remotely operated plants

→ **Control traffic exposed to inter-domain networks**

… are challenging Purdue

A Tableau production plant flattens the hierarchy



Separate end host and transit functions of network

Each zone has a dedicated Transition Point

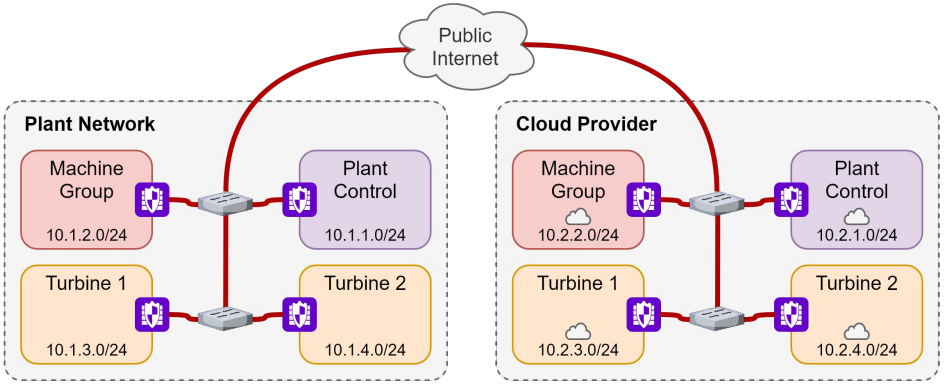
Flattened hierarchy with full connectivity

Single, centrally administered zone transition policy

Open transit network with protected inter-TP traffic

Tableau facilitates hybrid plant-cloud networks

Physical layout



Logical view

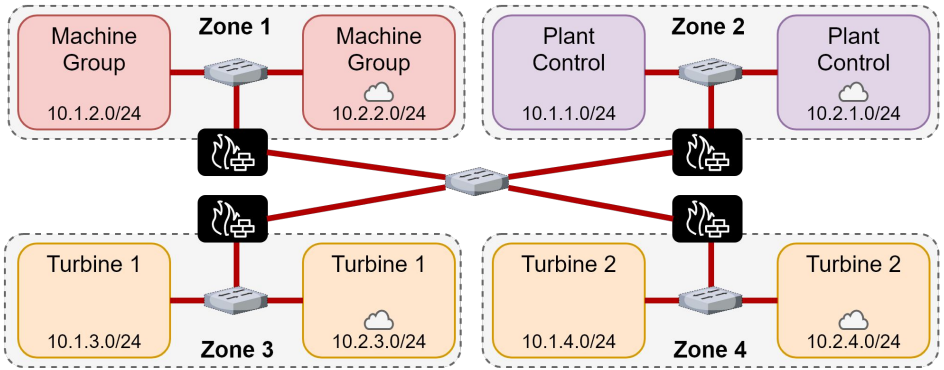


Tableau simplifies multihoming

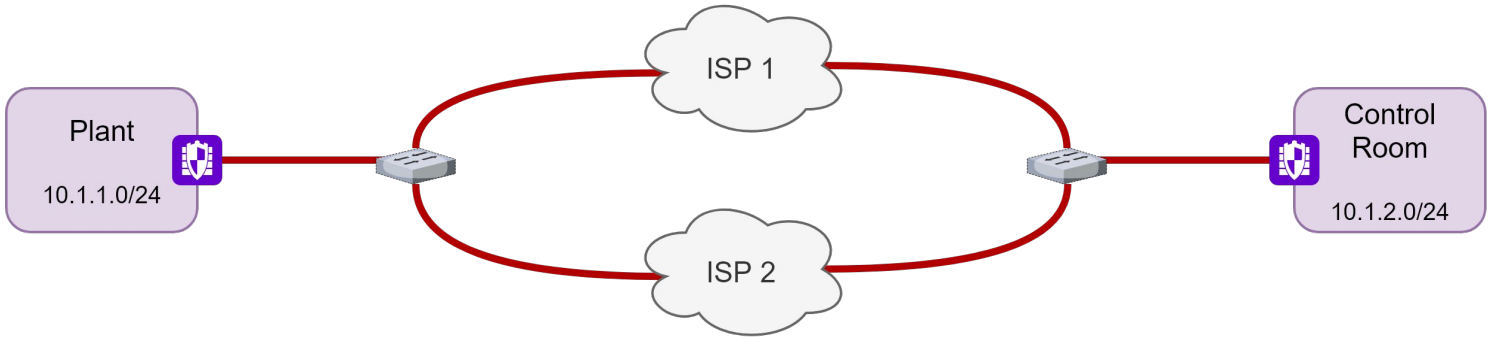
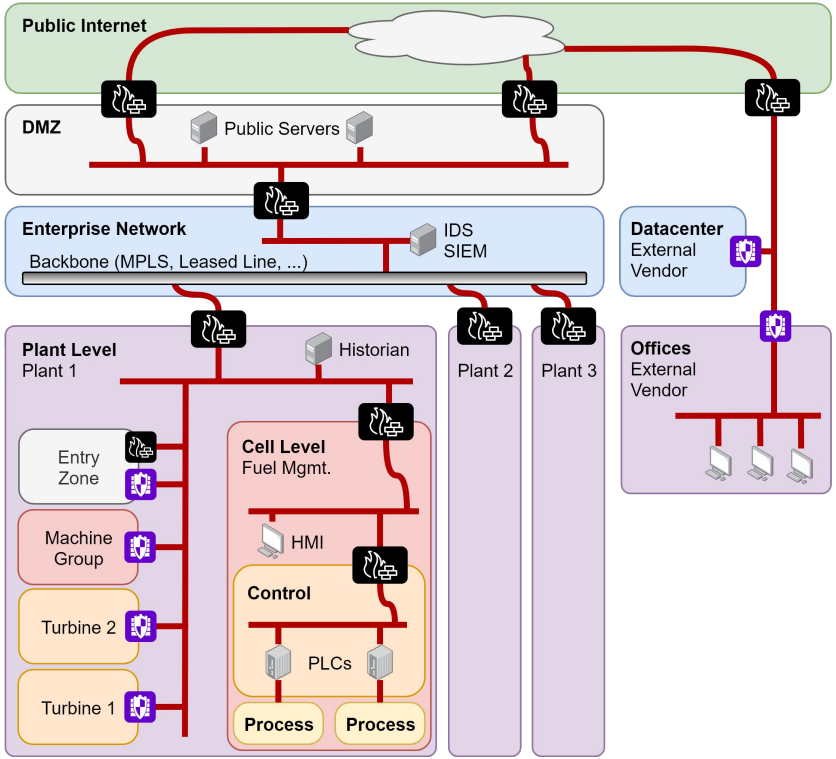


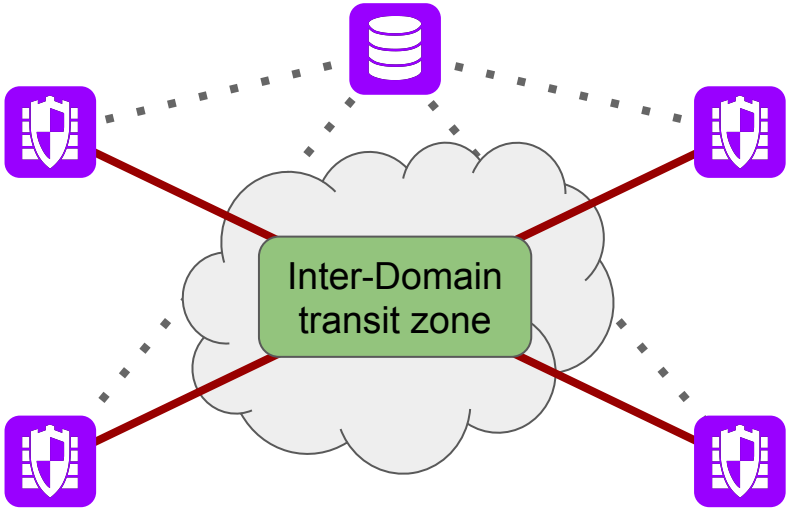
Tableau is brownfield compatible



Partial Deployment

Hierarchical overlay

Mondrian facilitates inter-transition point traffic



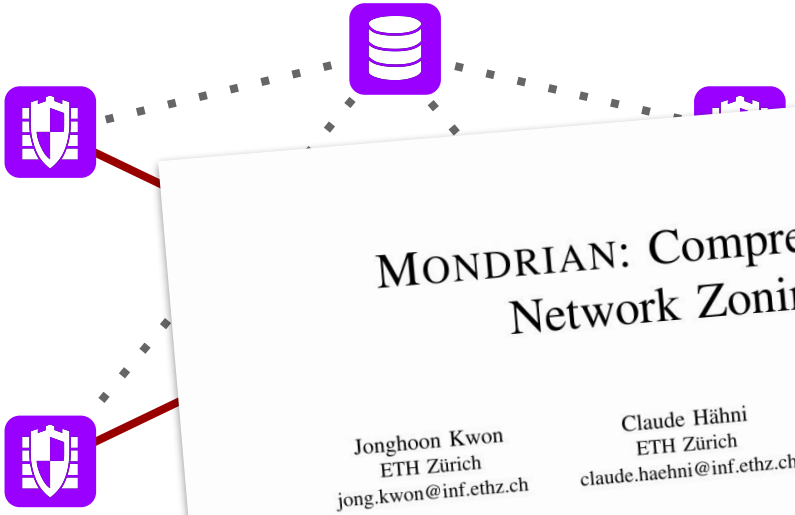
Designed for enterprise networks

All Inter-TP traffic is encrypted + authenticated

Zone transitions checked against central policy file

TP overhead < 5 µs

Mondrian facilitates inter-transition point traffic



Designed for enterprise

crypted

ed

e

MONDRIAN: Comprehensive Inter-domain Network Zoning Architecture

Jonghoon Kwon
ETH Zürich
jong.kwon@inf.ethz.ch

Claude Hähni
ETH Zürich
claude.haehni@inf.ethz.ch

Patrick Bamert
Zürcher Kantonalbank
patrick.bamert@zkb.ch

Adrian Perrig
ETH Zürich
adrian.perrig@inf.ethz.ch

***Abstract*—A central element of designing IT security infrastructures is the logical segmentation of information assets into network zones sharing the same security requirements and policies. As more business ecosystems are migrated to the cloud, additional demands for cybersecurity emerge and make the network-zone operation and management for large corporate networks challenging. In this paper, we introduce the new concept of an inter-domain transit zone that securely bridges physically and logically non-adjacent zones in large-scale information systems, simplifying complex network-zone structures. With inter-zone translation points, we also ensure communication integrity and confidentiality while providing lightweight security-policy enforcement. A logically centralized network coordinator enables**

Bridging geographically distant network zones is very challenging today. In general, network zones are created not only for security purposes but also because of geographical, operational, or organizational factors. Large enterprises with geographically distributed branch networks, and possibly collaborative partners' networks need to be interconnected. Given that distant network zones exchange information over an untrusted network (e.g., the Internet), there is a risk that the communication exposes security-sensitive information during transit. To mitigate such threats, administrators leverage additional security mechanisms (e.g., IPsec [32] and TLS-VPN [55]) which ensure confidentiality and integrity of the transmission over the untrusted network by encrypting and authenticating the data with shared cryptographic keys.

But what about defence in depth?

Layered firewalls
Heterogenity
}  defence in depth

Complexity leads to poor security

Threat (and network) models are changing

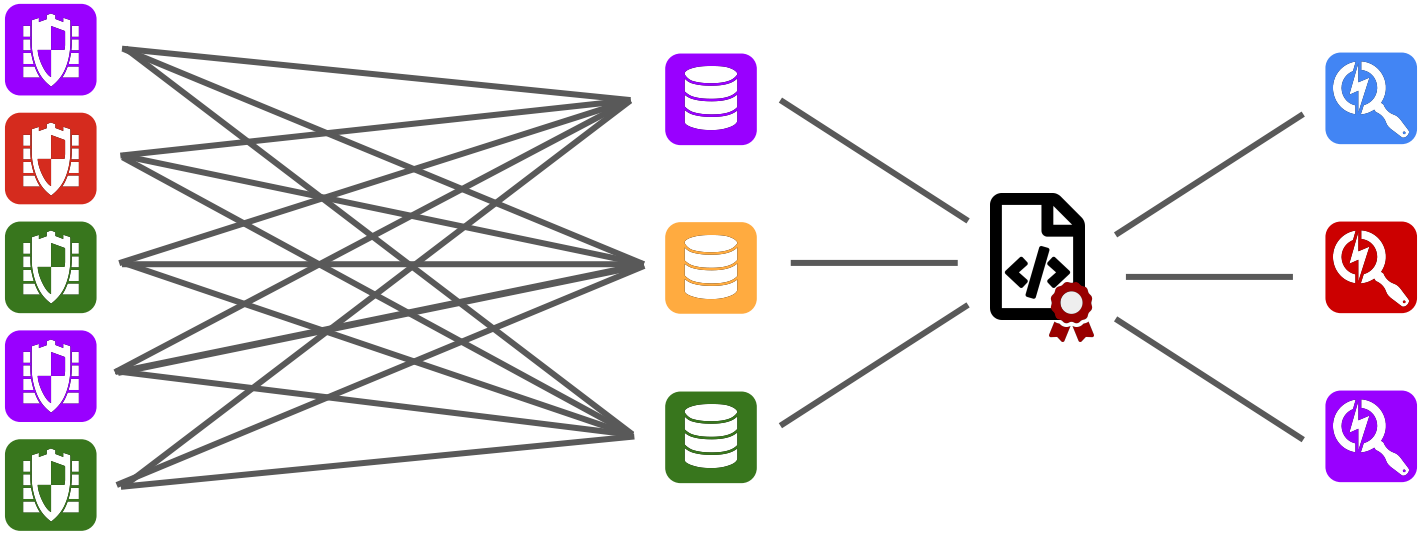
Tableau facilitates

Policy simplification

Fine-grained zoning

Automated network verification

Tableau introduces structured heterogeneity



Heterogeneous transition points require a threshold number of flow approvals

from heterogeneous controller implementations

operating on one policy

verified by heterogeneous verifiers

Conclusion

IIoT and IT/OT convergence are challenging OT defences

Purdue assumptions on network no longer hold
⇒ Security is eroding

Tableau flattens OT networks and
enables flexible inter-domain traffic management
with centralized policy management

Modern security practices and structured heterogeneity
replace layered firewalls where needed