

IT and OT Convergence

Andreas Reiter

Siemens – Security Expert

andreasreiter@siemens.com

SIEMENS

Ingenuity for life

#Lets@cluster

Lighthouse Summit in the heart of Europe

March 25th to 27th, 2019



SILICONALPS



DeepTech4Good





Andreas Reiter

andreasreiter@siemens.com

<https://andreasreiter.info>

Siemens AG Austria / Security Expert

- Security Testing for Mindsphere
- Policies and guidelines
- Research projects

#LetsCluster

Lighthouse Summit in the heart of Europe

March 25th to 27th, 2019



SILICONALPS



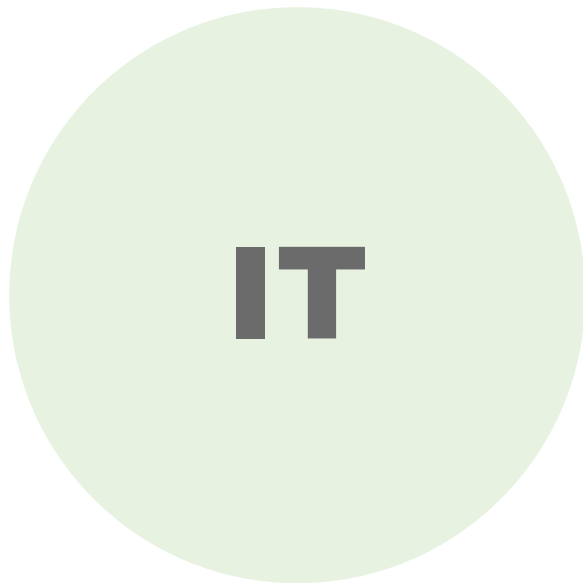
DeepTech4Good



Upcoming Challenges for the Industry

#LetsCluster

IT – OT?



- # Dynamic
- # Full spectrum of technologies
- # Well connected
- # Confidentiality, Integrity, Availability

- # **Data is King**

IT – OT?

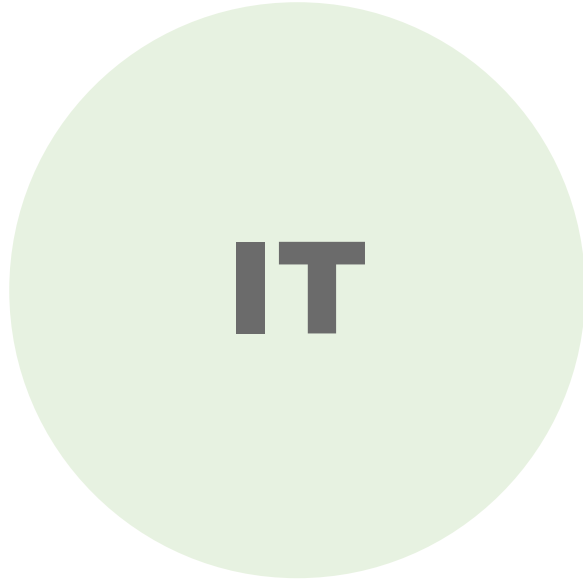
- # Control production floor processes
- # Process oriented
- # Safety/Availability, Integrity, Confidentiality

- # **Process is King**

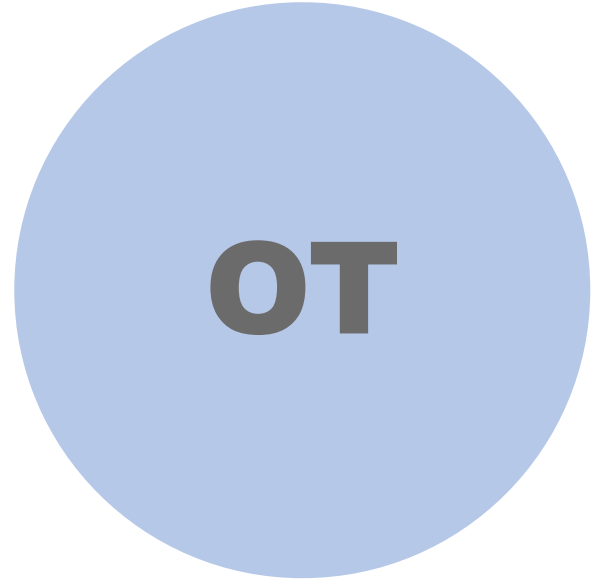


OT

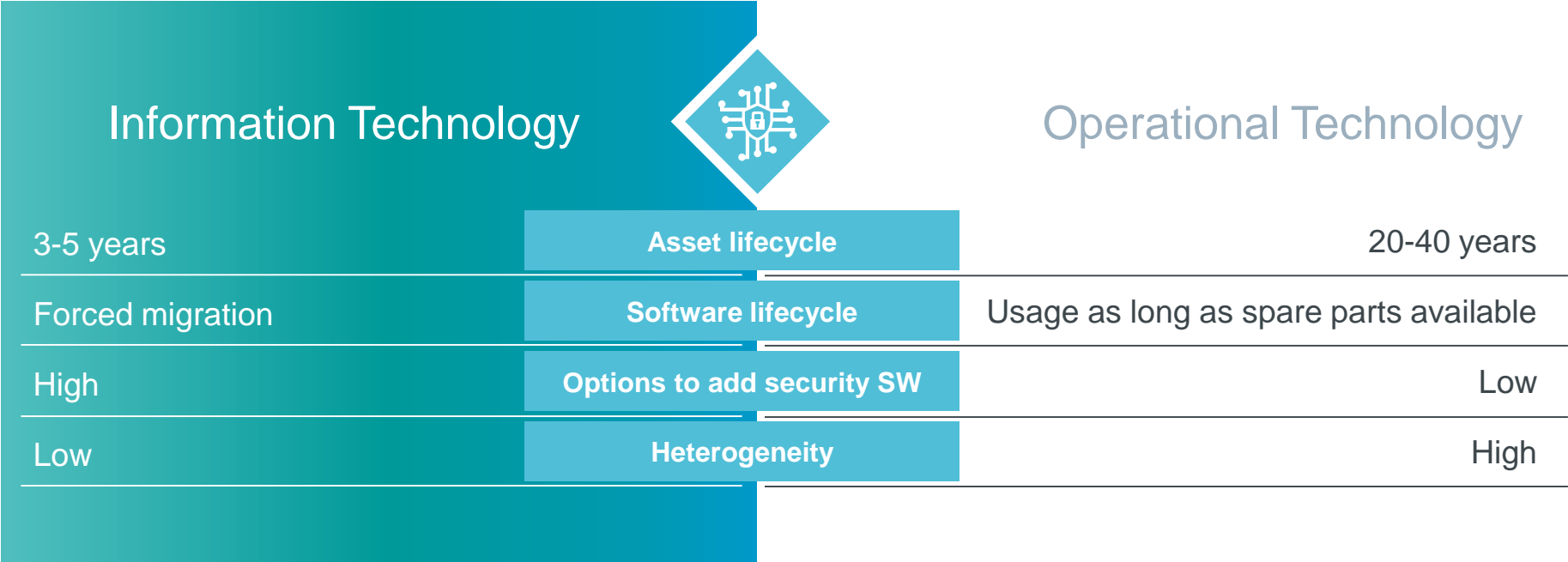
IT – OT?



SILOS



IT - OT Challenges



IT – OT Convergence?

Massive data generation

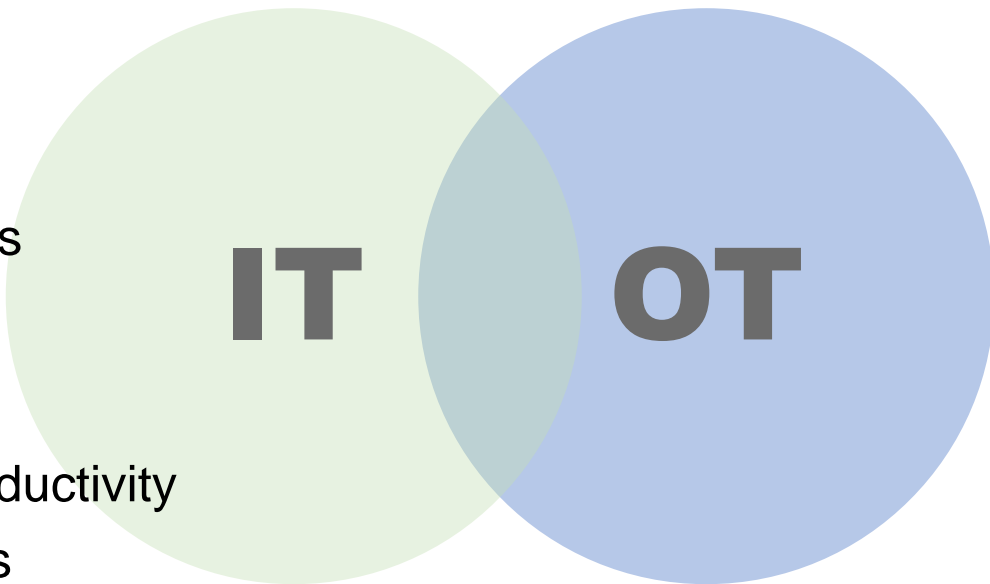
Big data analytics capabilities

Real-time decisions

Predictive maintenance

Increased efficiency and productivity

Create new revenue streams



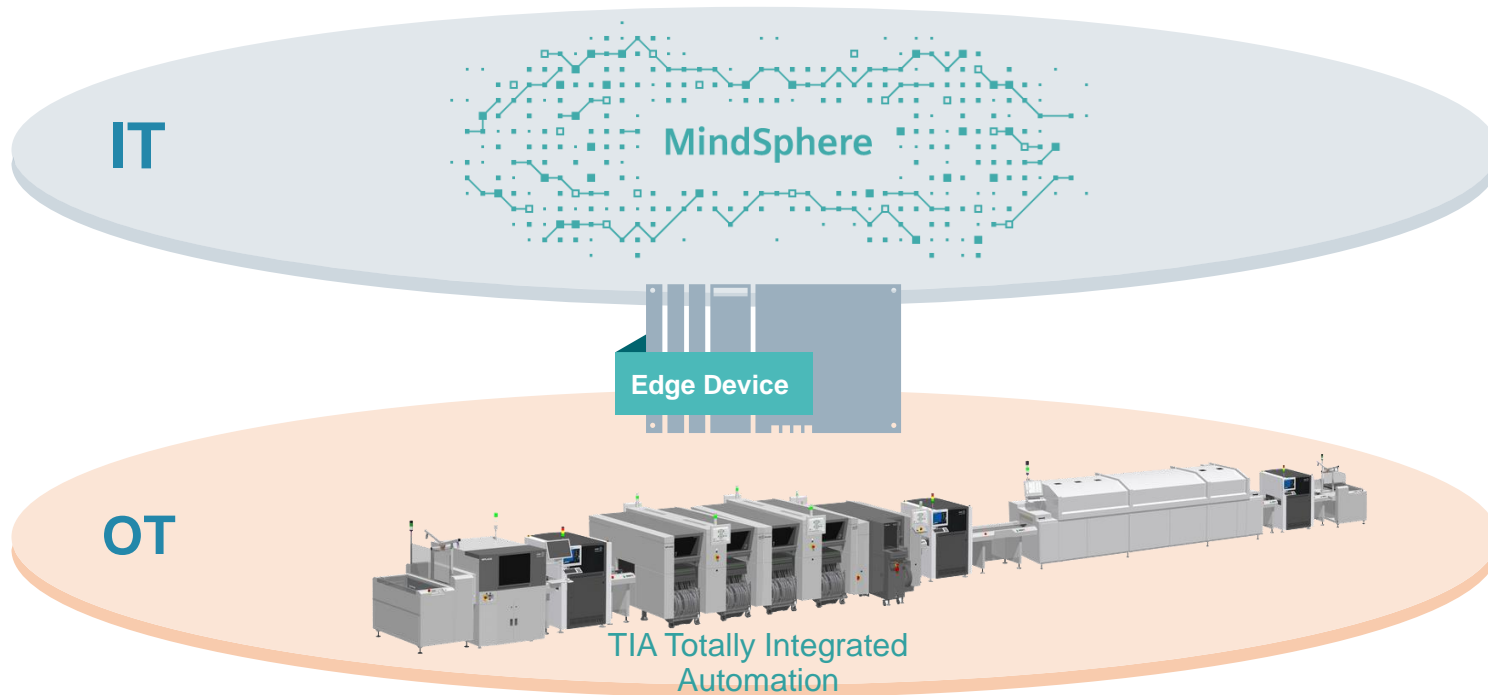
*„Currently, 85 percent of potential assets
remain unconnected...”*

World Economic Forum (2017)



**LIGHTHOUSE SUMMIT
IN THE HEART OF EUROPE**

Real-time decisions



Real-time decisions

Access to mission-critical real-time data on the edge at plant-level

Enables a rapid decision making

Prevent costly downtime

Non-mission-critical data is sent to the cloud

Historical data analysis and storage



Predictive Maintenance

Preventive maintenance

Regular schedules

Manufacturer recommendations

Paradigm shift

Preventive to predictive maintenance

Collect real-time data

Perform anomaly detection

Increases uptime



“...56% of organizations using SCADA/ICS reported a breach in the past year...”

Fortinet (2017)



**LIGHTHOUSE SUMMIT
IN THE HEART OF EUROPE**

*“...the mean time to identify [a data breach]
was **197** days...”*

Cost of a Data Breach (2018)



**LIGHTHOUSE SUMMIT
IN THE HEART OF EUROPE**

Challenges

Security concerns are major road blocks

“Airgap believers”

Shared hardware devices (e.g. USB sticks) – e.g. for data exchange, patching,...

VPN tunnels for maintenance

Intruders are undetectable

Security by design

Security at runtime

Defense in depth

Awareness



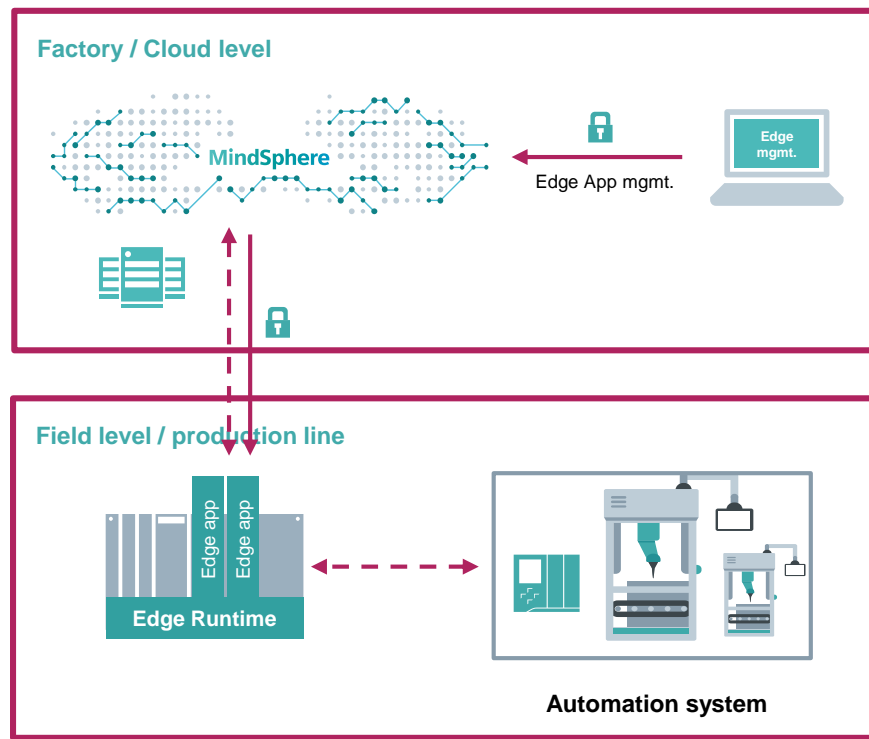
Security by Design

Minimize attack surface

Need to know

Separation of duties

Least privileges



Security at Runtime

Security Management Process/monitoring

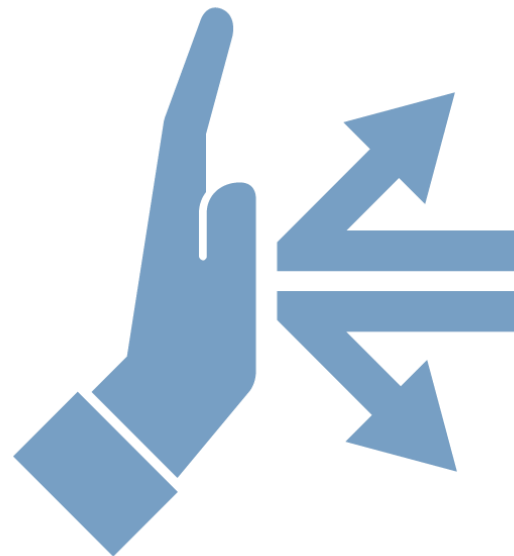
Security Event Management (SEM)

Near real-time security alarms and events

Security Information Management (SIM)

Long-term storage of log data

Patch management

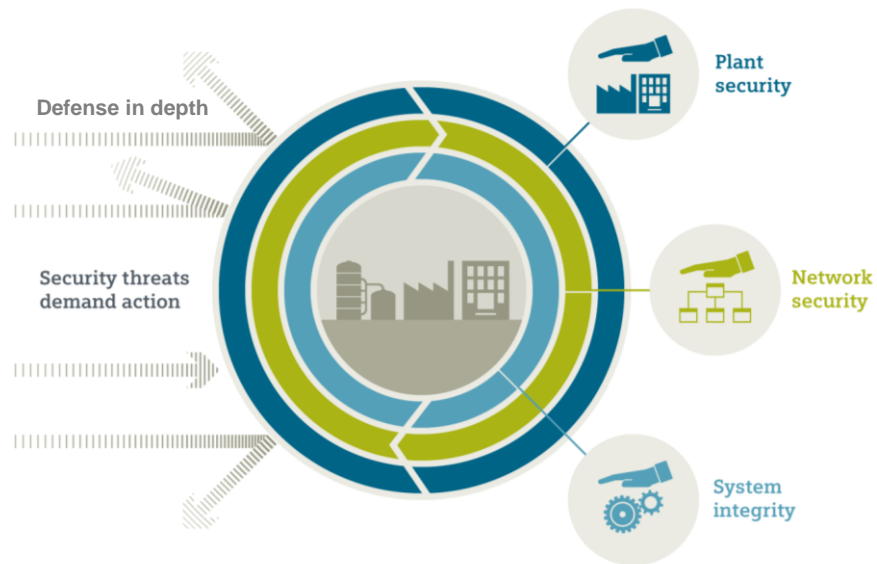


Defense in Depth

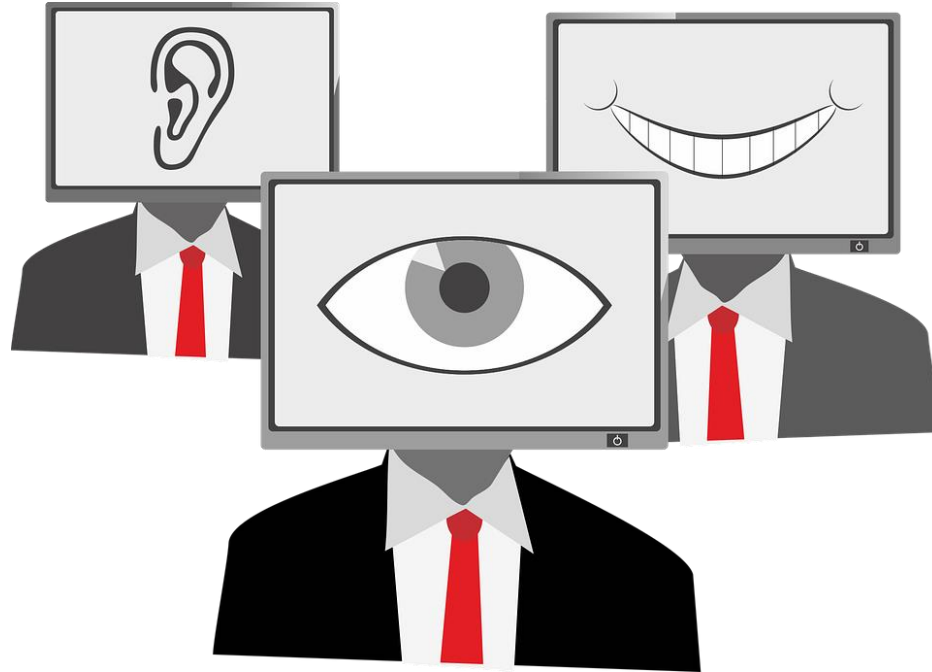
“Castle approach”
Multiple lines of defense

Defense mechanisms don't stop at the perimeter

- # Network segmentation
- # Device security
- # Common cryptographic principles
- # ...



Awareness



Your Takeaways

- # IT – OT convergence offers chances
 - # Maintenance, Productivity, new business models
- # Apply security measures also to siloed solutions
- # IEC62443 standards are a good starting point



#LetsCluster

Lighthouse Summit in the heart of Europe
March 25th to 27th, 2019



SILICONALPS



DeepTech4Good



flex.



LAND KÄRNTEN

