.conf18
splunk>

IIoT-Security & Production Data Analytics at Volkswagen

A Winning Team for more efficient and secure Production

Ahmet Cubukcuoglu – Volkswagen AG
Dr. Sebastian Schmerl - Computacenter

02/10/2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Key Takeaways

What you will learn in this session

- Security and efficiency goes hand in hand
- Acquiring production and security relevant data
- Data analytics and use cases

Agenda

1. Some words about us
2. Challenges in industrial and shop floor security
3. Why security and production data analytics goes hand in hand
4. Data layers for production & security data in production environments
5. Use cases for security and production efficiency
6. Q&A

Some words about us

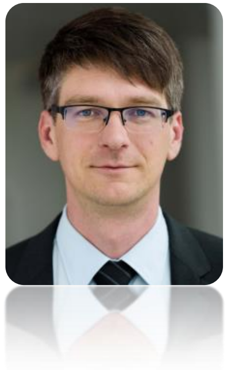
Ahmet Cubukcuoglu

Project Coordinator for IT-Shop floor Security

Volkswagen AG

- Subject matter expert for:
  - Industrial & shop floor security
  - Security concepts & functional developments
  - Security assessments for production sites

Dr. Sebastian Schmerl



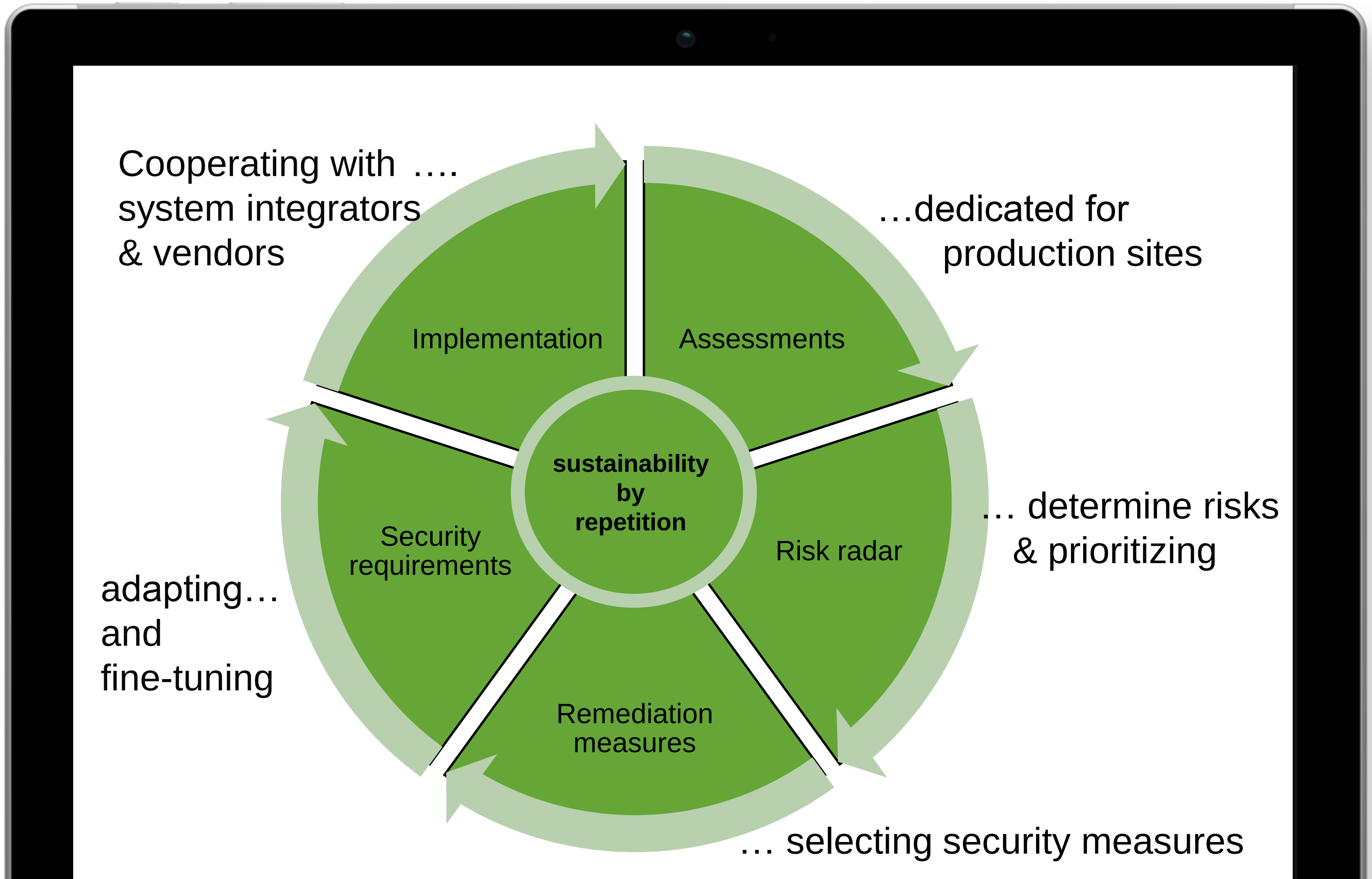
Head of Production Data Analytics, Industrial Security & Cyber Defense

Computacenter

- Subject matter expert for:
  - ICS & SCADA security
  - Industry 4.0 & data science
  - SOCs

Assessments and sustainability model

for production environments

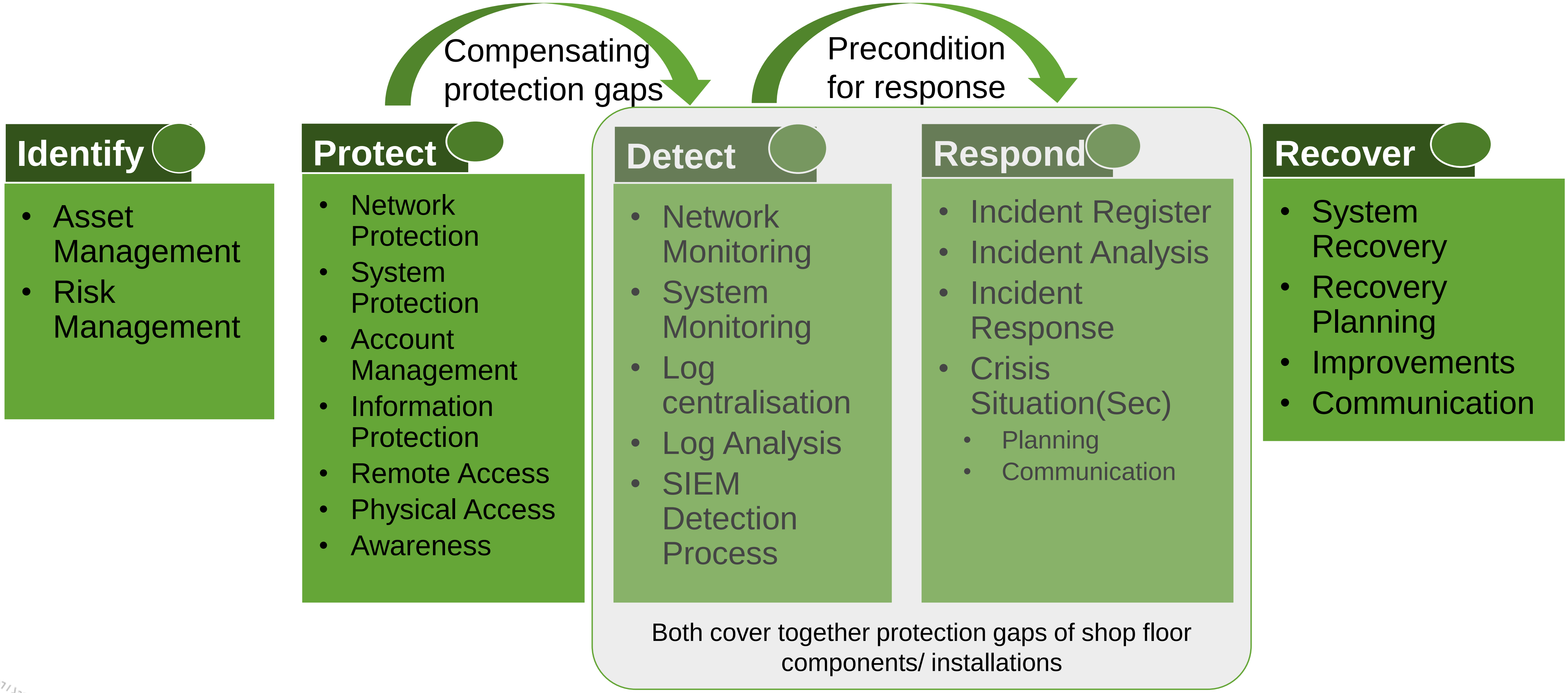


Challenges

- Large and complex systems with plenty of components, e.g.:
  - Conveyor systems, robots, gripping systems, welding systems, cluing systems, screwing systems, safety-system and …
- Unique systems, tailored to the production process
- Build by system integrators
- Long lifespan >10 years

NIST Cyber Security Framework

The need of security monitoring & detection



Compensating protection gaps

Precondition for response

Identify

- Asset Management
- Risk Management

Protect

- Network Protection
- System Protection
- Account Management
- Information Protection
- Remote Access
- Physical Access
- Awareness

Detect

- Network Monitoring
- System Monitoring
- Log centralisation
- Log Analysis
- SIEM Detection Process

Respond

- Incident Register
- Incident Analysis
- Incident Response
- Crisis Situation(Sec)
  - Planning
  - Communication

Recover

- System Recovery
- Recovery Planning
- Improvements
- Communication

Both cover together protection gaps of shop floor components/ installations

Production efficiency and security in combination

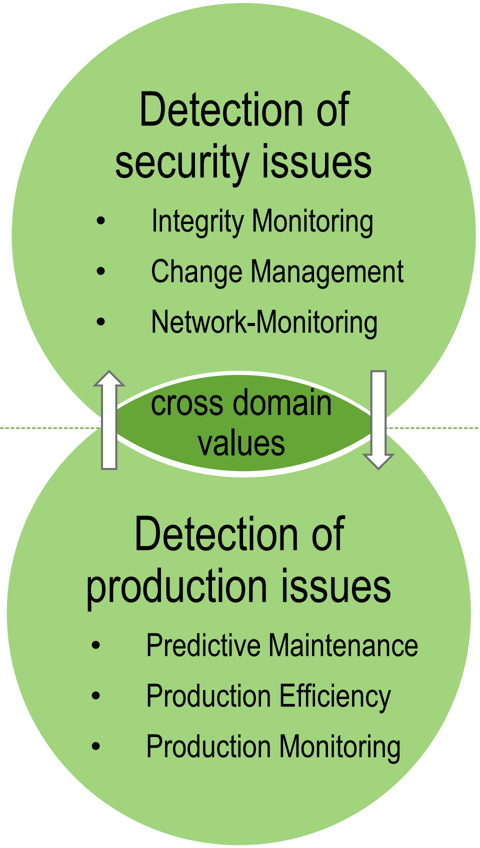
Challenges & advantages - mutual support & synergies

Industrial Security

- No calculable RoI
- No changes please
- Stakeholder conflicts

Production Analytics

- Clear RoI
- Passive Data Acquisition
- Explicit Request



Detection of security issues

- Integrity Monitoring
- Change Management
- Network-Monitoring

cross domain values

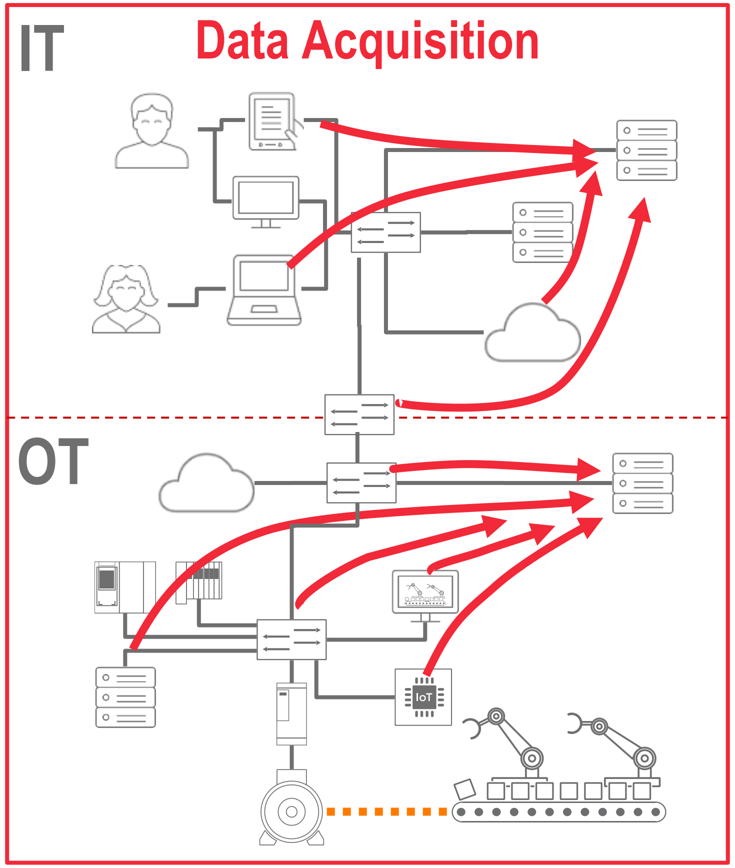
Detection of production issues

- Predictive Maintenance
- Production Efficiency
- Production Monitoring

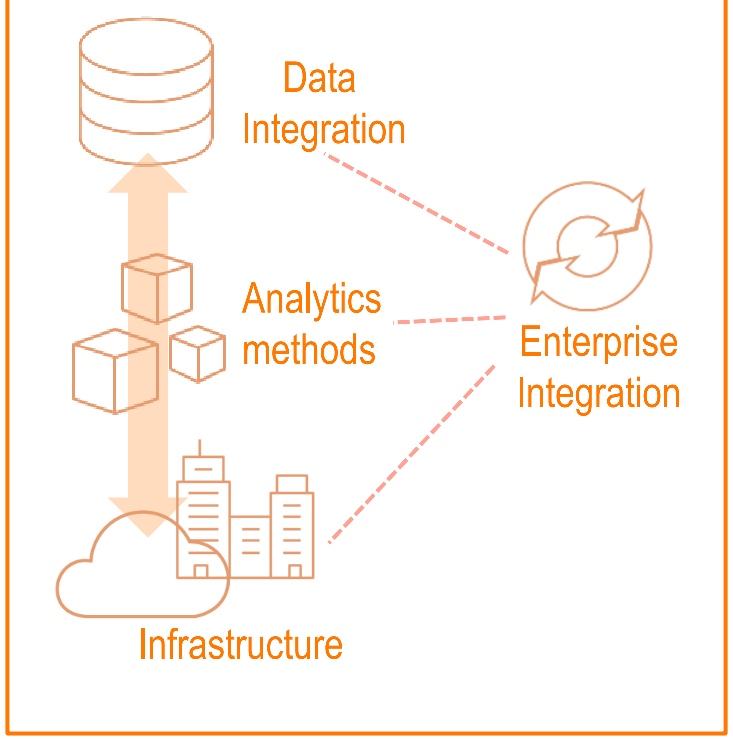
Industrial security & production data analytics

One technology stack for three domains

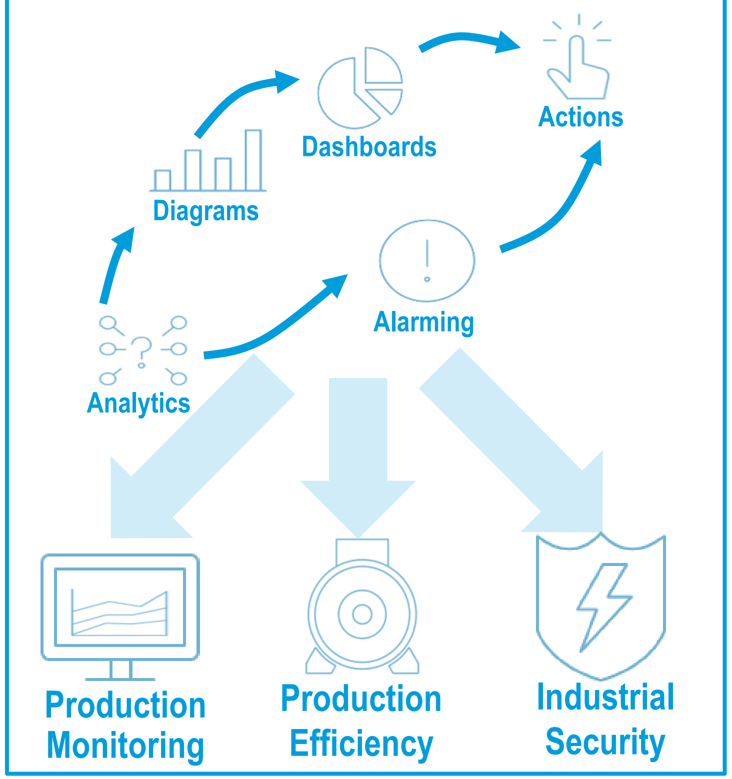
Data Acquisition



Analytics Infrastructure



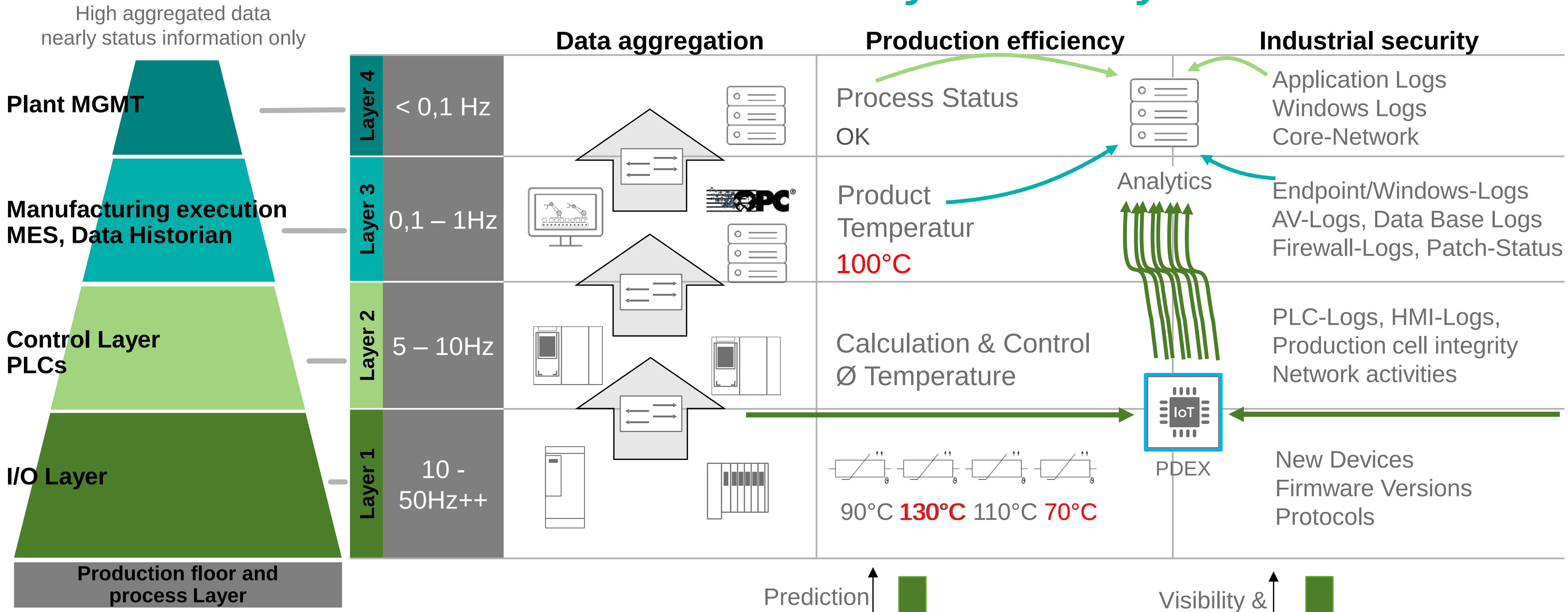
End-to-End Analytics



Data layers for production & security data

Data acquisition & collection

Production and security data layers

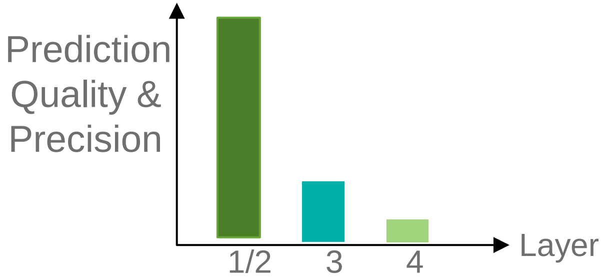


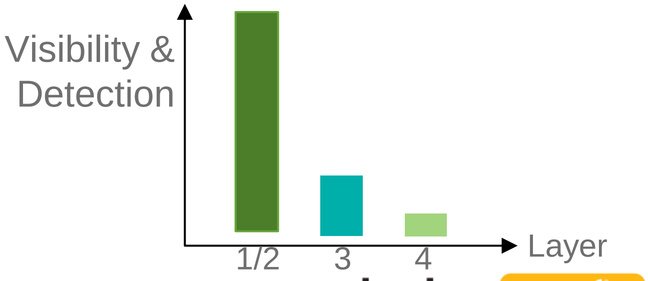
High aggregated data nearly status information only

			Data aggregation	Production efficiency	Industrial security
Plant MGMT	Layer 4	< 0,1 Hz		Process Status OK	Application Logs Windows Logs Core-Network
Manufacturing execution MES, Data Historian	Layer 3	0,1 – 1Hz		Product Temperatur 100°C	Endpoint/Windows-Logs AV-Logs, Data Base Logs Firewall-Logs, Patch-Status
Control Layer PLCs	Layer 2	5 – 10Hz		Calculation & Control Ø Temperature	PLC-Logs, HMI-Logs, Production cell integrity Network activities
I/O Layer	Layer 1	10 - 50Hz++		90°C 130°C 110°C 70°C	New Devices Firmware Versions Protocols

Production floor and process Layer

Fine grained temporal & sensor values of production data





Active and passive data acquisition

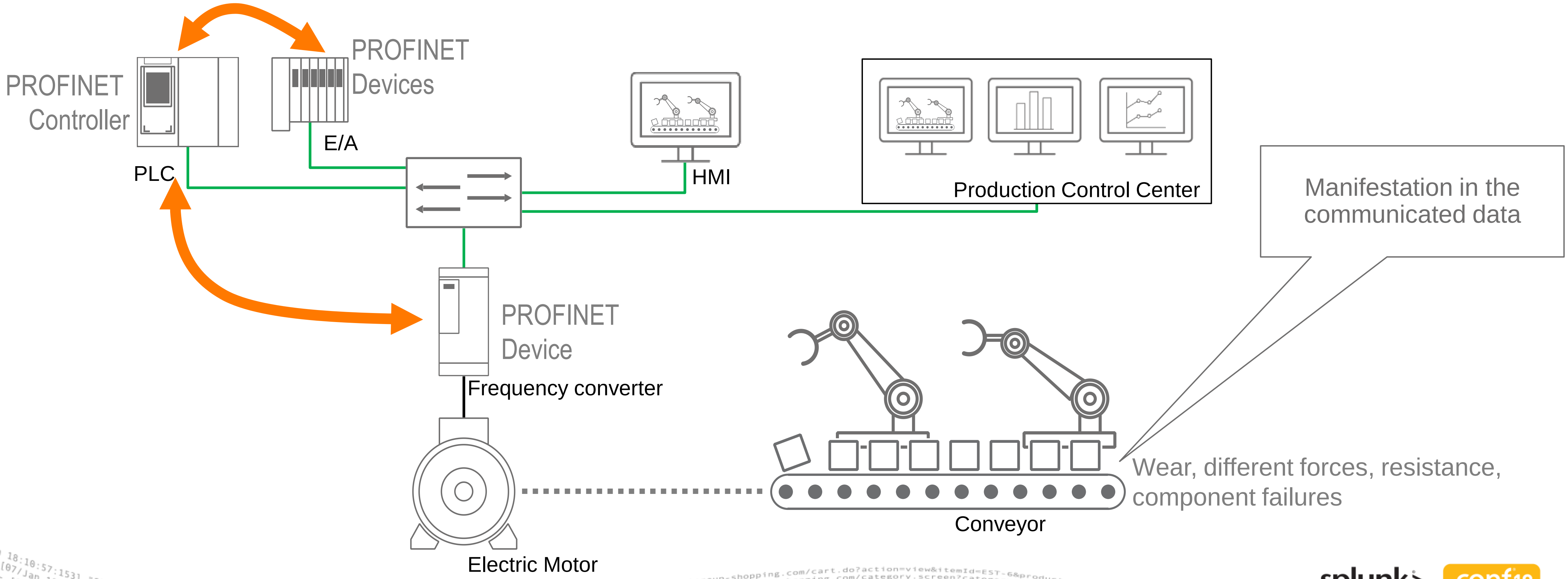
For the different layers

	ACTIVE	PASSIVE
PRO	• no data transformation • no data dissection	• non invasive • no changes on automation cells • no discussions, no re-certifications • easy rollout
CON	• configuration changes • polling of information • PLC CPU time & memory	• Complex data extraction
Options	• Agent based • e.g. Splunk UF, Syslog,… • OPC based	• CC Production Data Extractor

Production analytics & industrial security

Fine grained production data

Cyclic data exchange



PROFINET Controller

PLC

PROFINET Devices

E/A

HMI

Production Control Center

Manifestation in the communicated data

PROFINET Device

Frequency converter

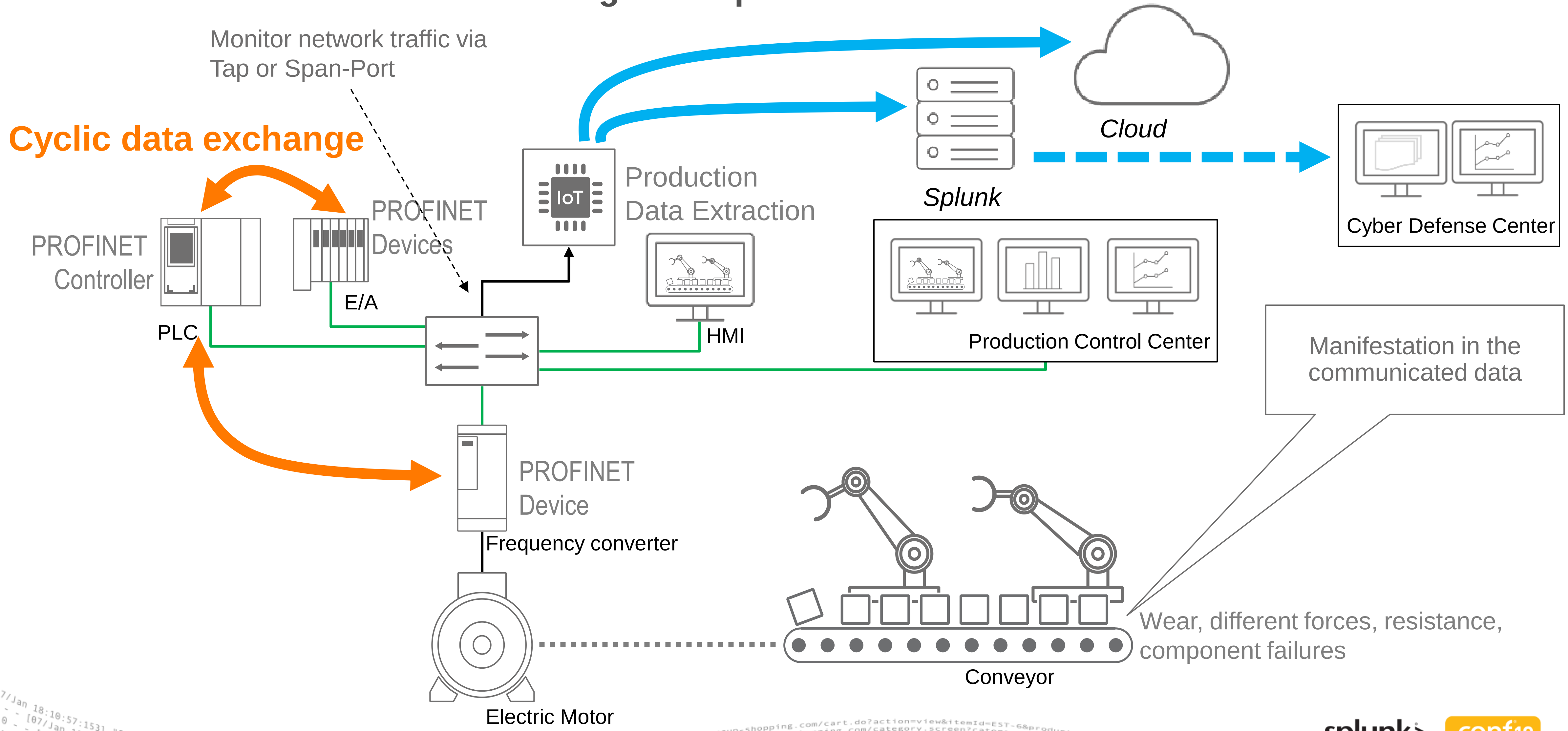
Electric Motor

Conveyor

Wear, different forces, resistance, component failures

Production analytics & industrial security

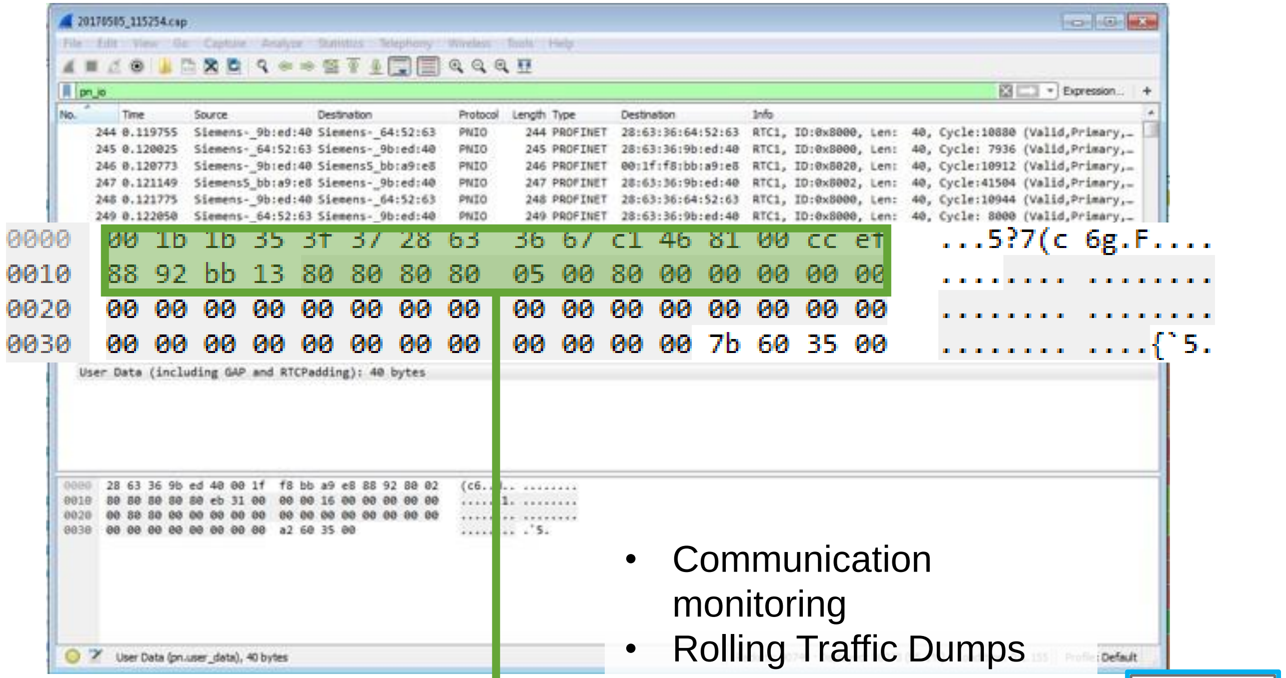
Fine grained production data



PDEX – Production Data Extractor

How it works

Captured network traffic with production data

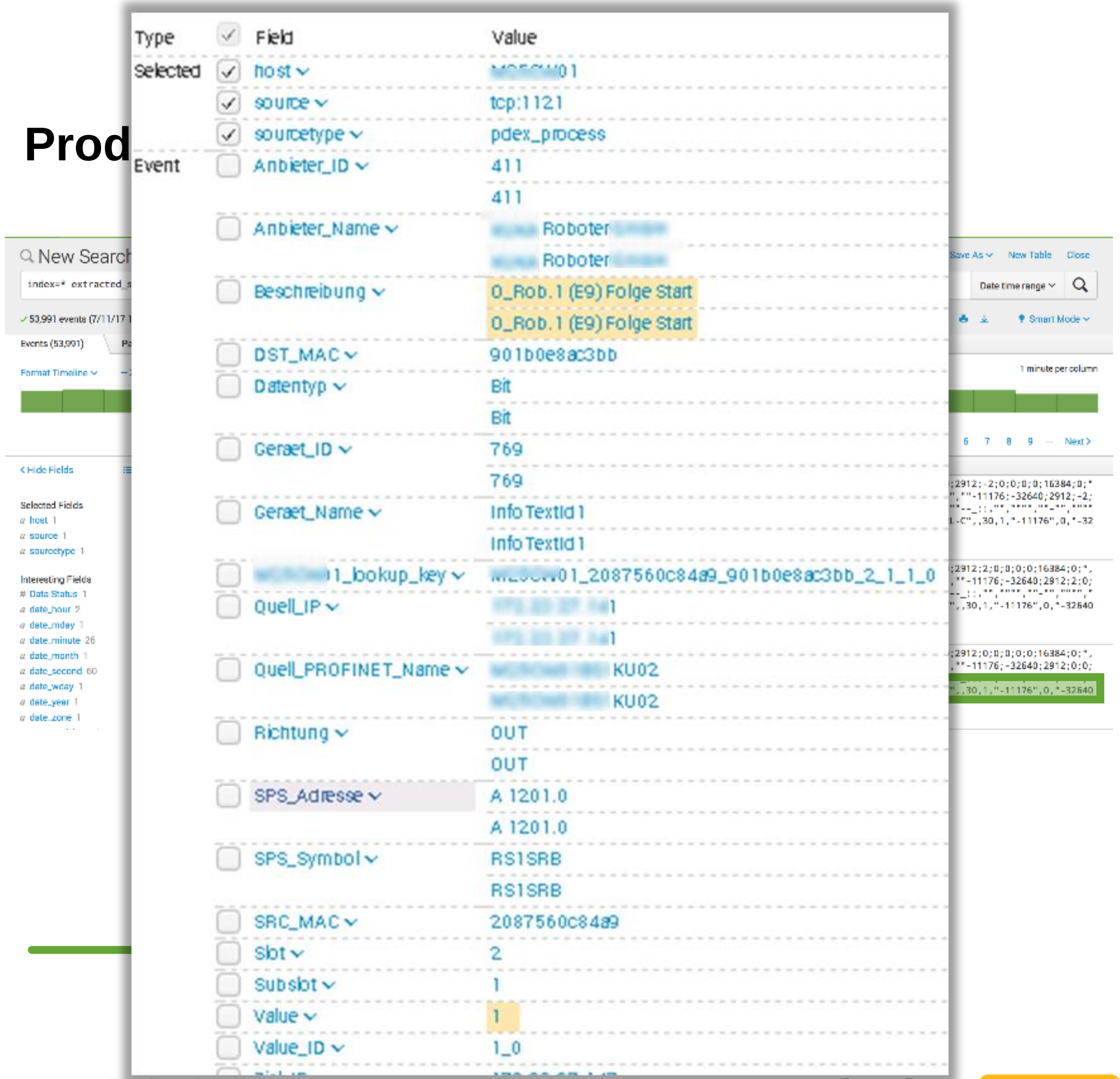

20170505_115254.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pn_io
Expression...
Profile: Default

```
No.  Time     Source            Destination       Protocol Length Type      Destination        Info
 244 0.119755 Siemens-_9b:ed:40 Siemens-_64:52:63 PNIO     244 PROFINET  28:63:36:64:52:63  RTC1, ID:0x8000, Len:  40, Cycle:10880 (Valid,Primary,…
 245 0.120025 Siemens-_64:52:63 Siemens-_9b:ed:40 PNIO     245 PROFINET  28:63:36:9b:ed:40  RTC1, ID:0x8000, Len:  40, Cycle: 7936 (Valid,Primary,…
 246 0.120773 Siemens-_9b:ed:40 SiemensS_bb:a9:e8 PNIO     246 PROFINET  00:1f:f8:bb:a9:e8  RTC1, ID:0x8020, Len:  40, Cycle:10912 (Valid,Primary,…
 247 0.121149 SiemensS_bb:a9:e8 Siemens-_9b:ed:40 PNIO     247 PROFINET  28:63:36:9b:ed:40  RTC1, ID:0x8002, Len:  40, Cycle:41504 (Valid,Primary,…
 248 0.121775 Siemens-_9b:ed:40 Siemens-_64:52:63 PNIO     248 PROFINET  28:63:36:64:52:63  RTC1, ID:0x8000, Len:  40, Cycle:10944 (Valid,Primary,…
 249 0.122050 Siemens-_64:52:63 Siemens-_9b:ed:40 PNIO     249 PROFINET  28:63:36:9b:ed:40  RTC1, ID:0x8000, Len:  40, Cycle: 8000 (Valid,Primary,…

0000  00 1b 1b 35 3f 37 28 63  36 67 c1 46 81 00 cc ef   ...5?7(c 6g.F....
0010  88 92 bb 13 80 80 80 80  05 00 80 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00 7b 60 35 00   ........ ....{`5.

  User Data (including GAP and RTCPadding): 40 bytes

0000  28 63 36 9b ed 40 00 1f  f8 bb a9 e8 88 92 80 02   (c6..@.. ........
0010  80 80 80 80 80 eb 31 00  00 00 16 00 00 00 00 00   ......1. ........
0020  00 80 80 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  a2 60 35 00               ........ ..`5.

User Data (pn.user_data), 40 bytes
```

- Communication monitoring
- Rolling Traffic Dumps
- Packet dissection
- Data Extraction
- Data Conversion
- Data Reduction
- Data Forwarding

PDEX

Prod

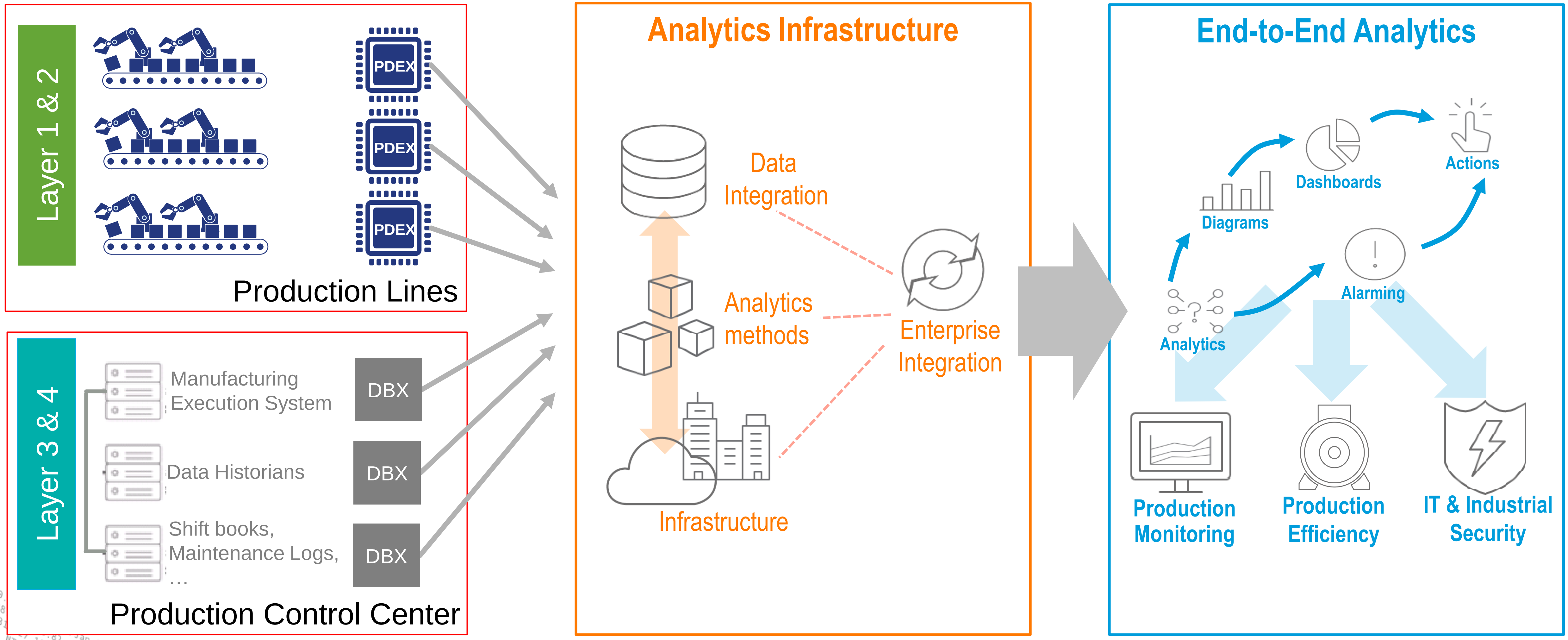


Type	☑	Field	Value
Selected	☑	host	[redacted]01
	☑	source	tcp:1121
	☑	sourcetype	pdex_process
Event	☐	Anbieter_ID	411 411
	☐	Anbieter_Name	[redacted] Roboter [redacted] [redacted] Roboter [redacted]
	☐	Beschreibung	0_Rob.1 (E9) Folge Start 0_Rob.1 (E9) Folge Start
	☐	DST_MAC	901b0e8ac3bb
	☐	Datentyp	Bit Bit
	☐	Geraet_ID	769 769
	☐	Geraet_Name	Info TextId 1 Info TextId 1
	☐	[redacted]1_lookup_key	[redacted]01_2087560c84a9_901b0e8ac3bb_2_1_1_0
	☐	Quell_IP	[redacted]1 [redacted]1
	☐	Quell_PROFINET_Name	[redacted] KU02 [redacted] KU02
	☐	Richtung	OUT OUT
	☐	SPS_Adresse	A 1201.0 A 1201.0
	☐	SPS_Symbol	RS1SRB RS1SRB
	☐	SRC_MAC	2087560c84a9
	☐	Slot	2
	☐	Subslot	1
	☐	Value	1
	☐	Value_ID	1_0

splunk> .conf18

PDEX/Splunk analytics infrastructure

for data on Layer 1, 2, 3 und 4



Layer 1 & 2

PDEX

PDEX

PDEX

Production Lines

Layer 3 & 4

Manufacturing Execution System

DBX

Data Historians

DBX

Shift books, Maintenance Logs, …

DBX

Production Control Center

Analytics Infrastructure

Data Integration

Analytics methods

Infrastructure

Enterprise Integration

End-to-End Analytics

Diagrams

Dashboards

Actions

Analytics

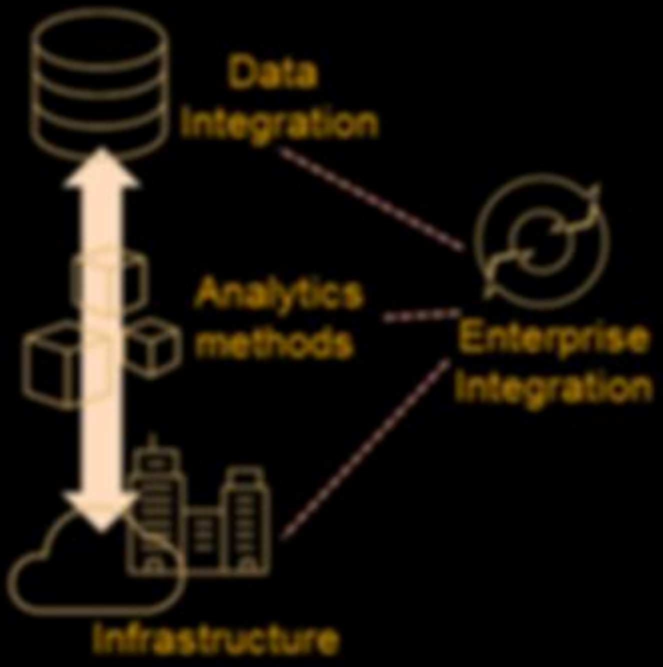
Alarming

Production Monitoring

Production Efficiency

IT & Industrial Security

splunk> .conf18

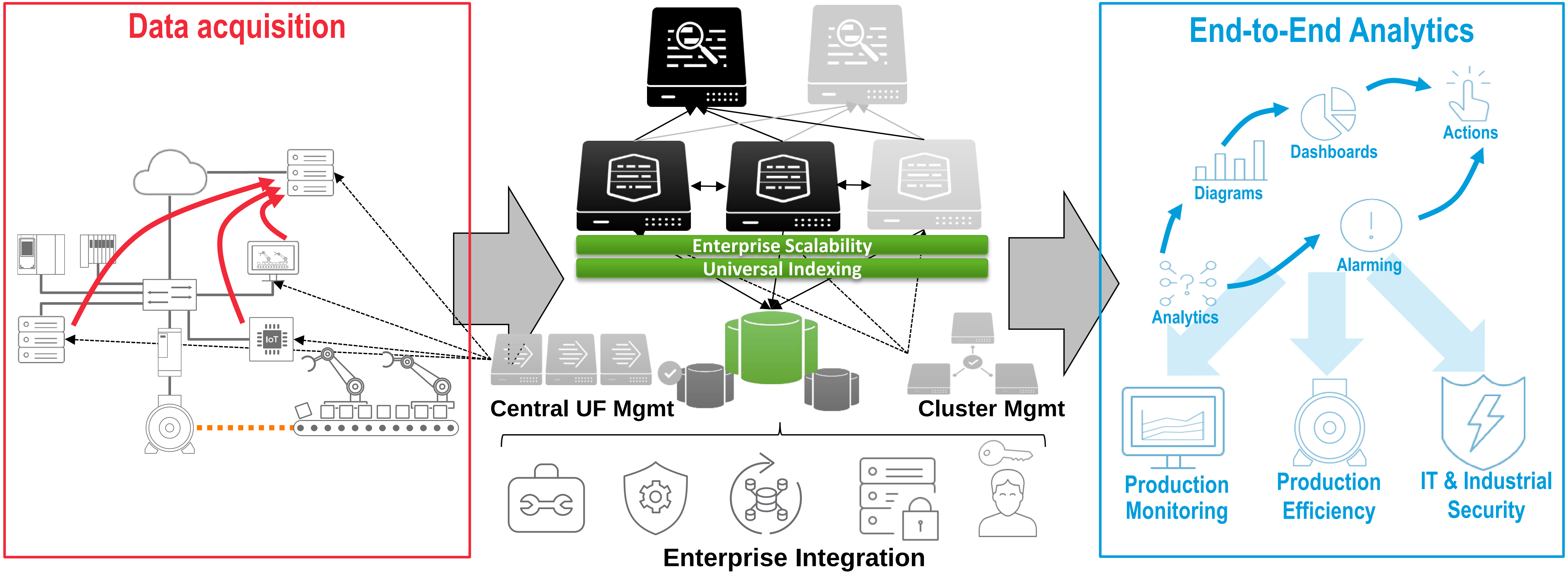


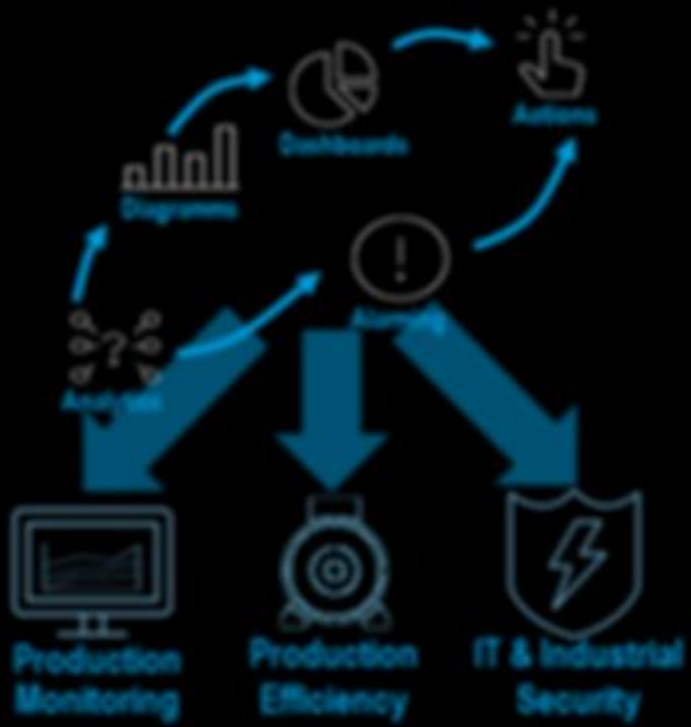
Analytics Infrastructure

Storage, Integration & Analytics

Analytics infrastructure from small to large

Scalable & enterprise ready analytics infrastructures



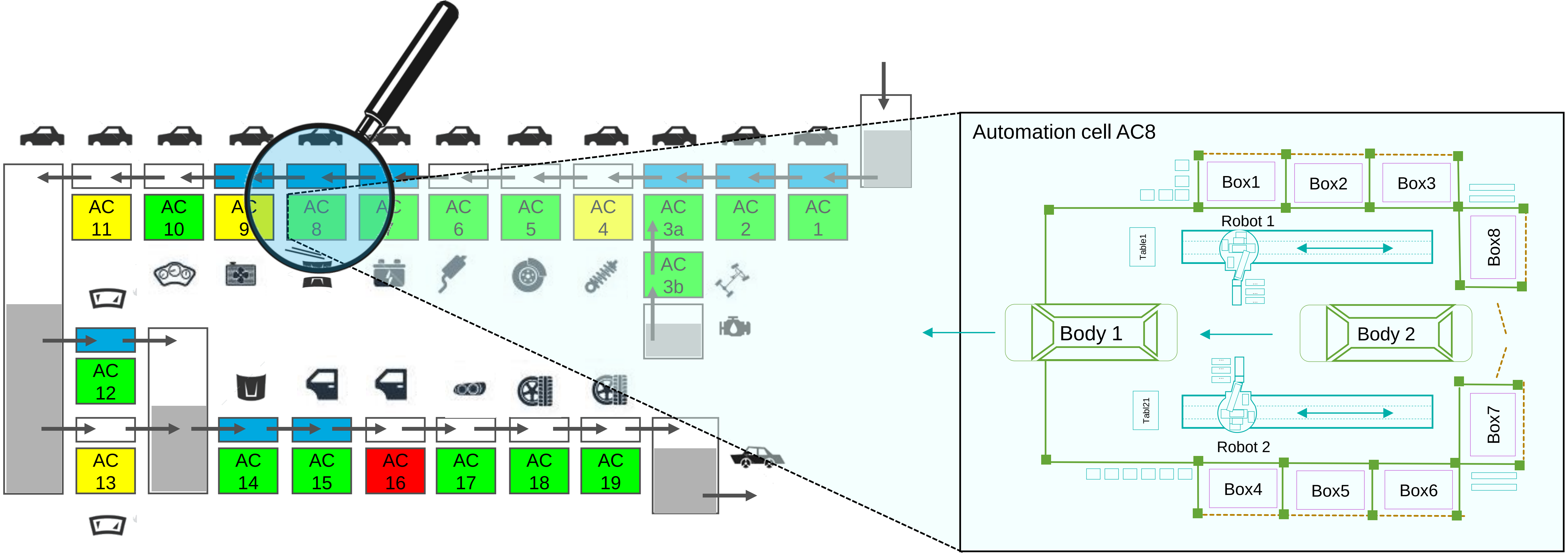


Use Cases

Splunking manufacturing lines including robots and industrial networks

Predictive health monitoring for assembly lines

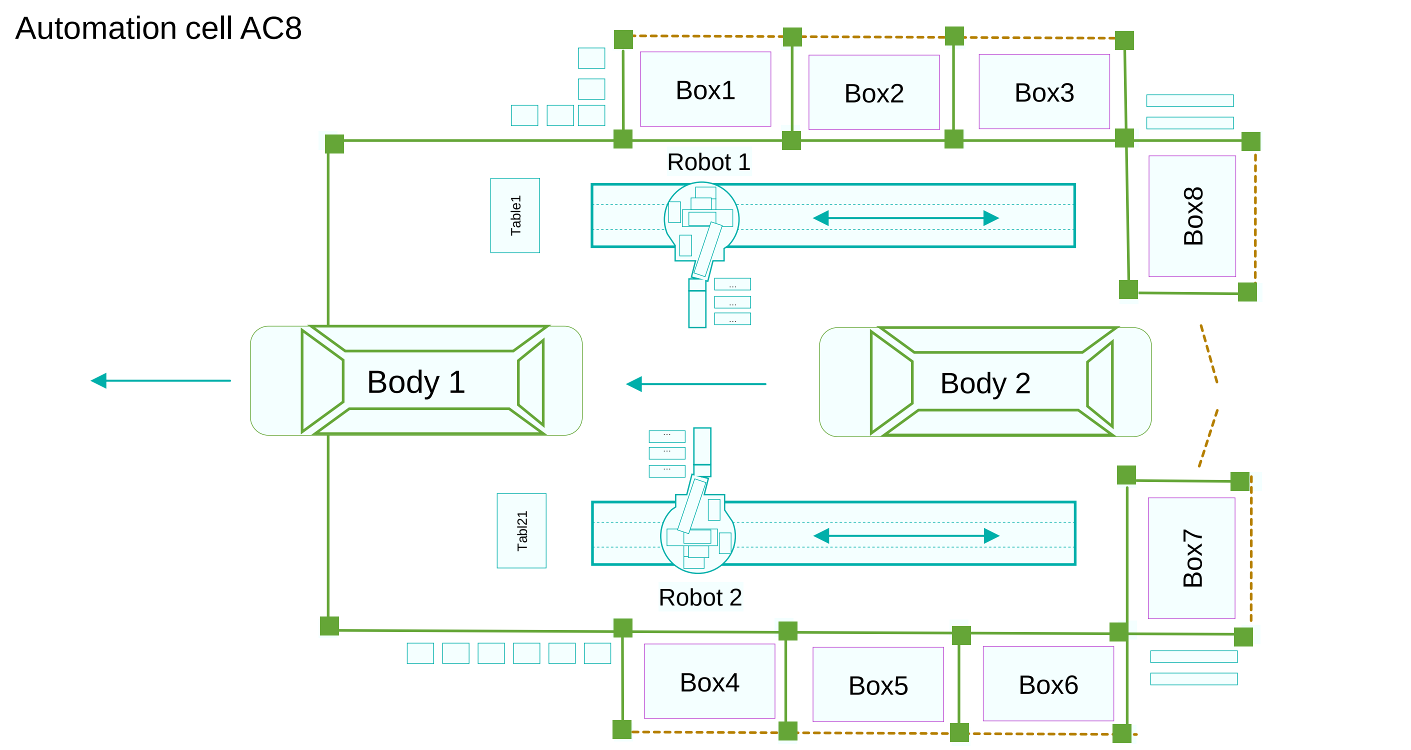
19 production cells on 600 meters



Light barriers
Robots and tools
Component boxes

Production data analytics & security monitoring

Health monitoring, predictive maintenance & integrity



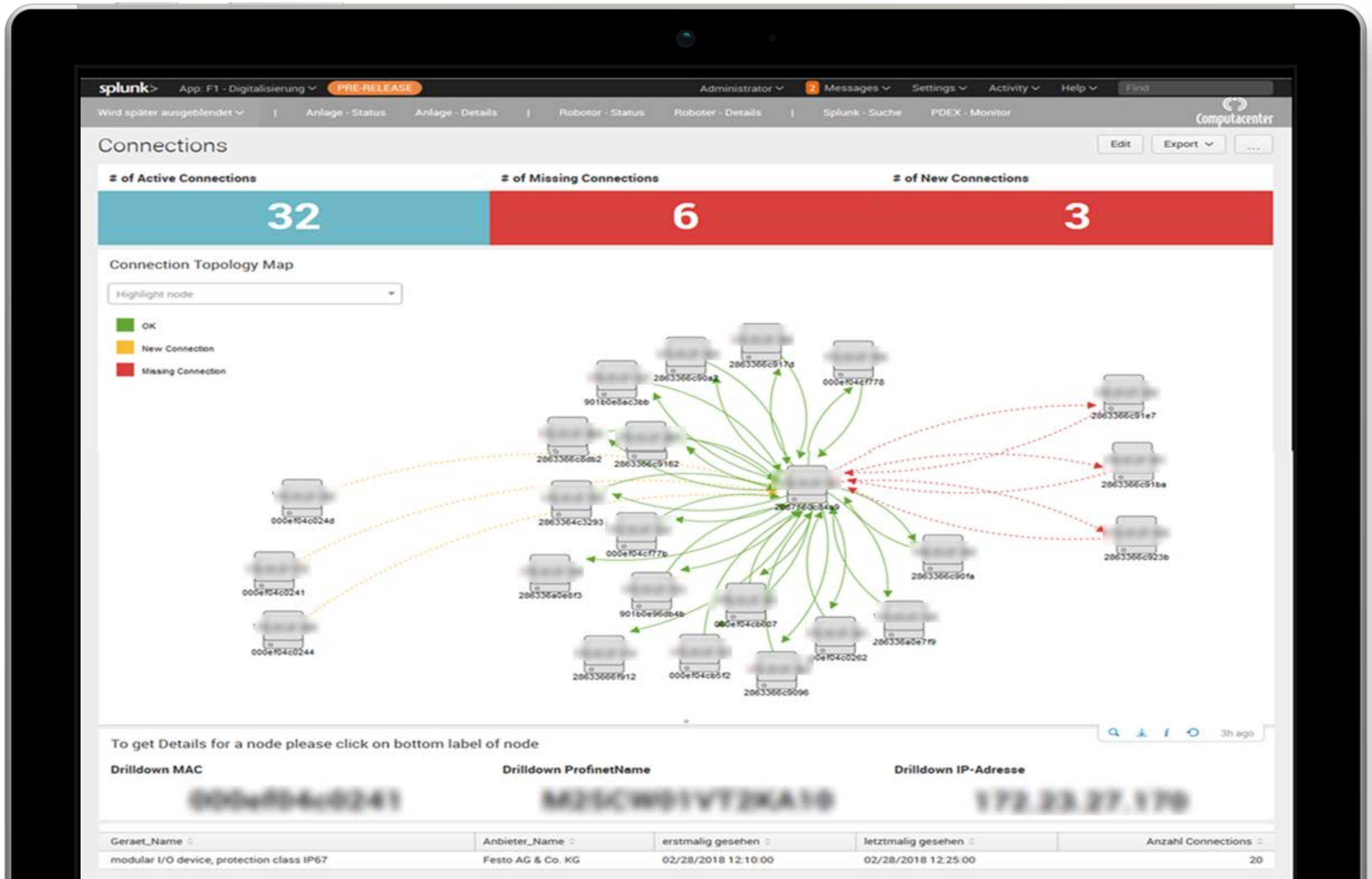
One automation cell - more than 600 components, actors & sensors

Project goals:

- Reduction of unplanned maintenance activities
- Faster maintenance activities in case of errors
- Learning of the normal behavior of the automation cells
- Anomaly detection with root cause analysis
- Predictive health monitoring for all components in the automation cells
- Integrity monitoring
- Data analytics for fine grained production data from PLC and IO-Layer

Integrity monitoring

Rapid overview on new, changed and missing elements



Connections

# of Active Connections	# of Missing Connections	# of New Connections
32	6	3

Connection Topology Map

🟩 OK
🟨 New Connection
🟥 Missing Connection

To get Details for a node please click on bottom label of node

Drilldown MAC [redacted]

Drilldown ProfinetName [redacted]

Drilldown IP-Adresse [redacted]

Geraet_Name	Anbieter_Name	erstmalig gesehen	letztmalig gesehen	Anzahl Connections
modular I/O device, protection class IP67	Festo AG & Co. KG	02/28/2018 12:10:00	02/28/2018 12:25:00	20

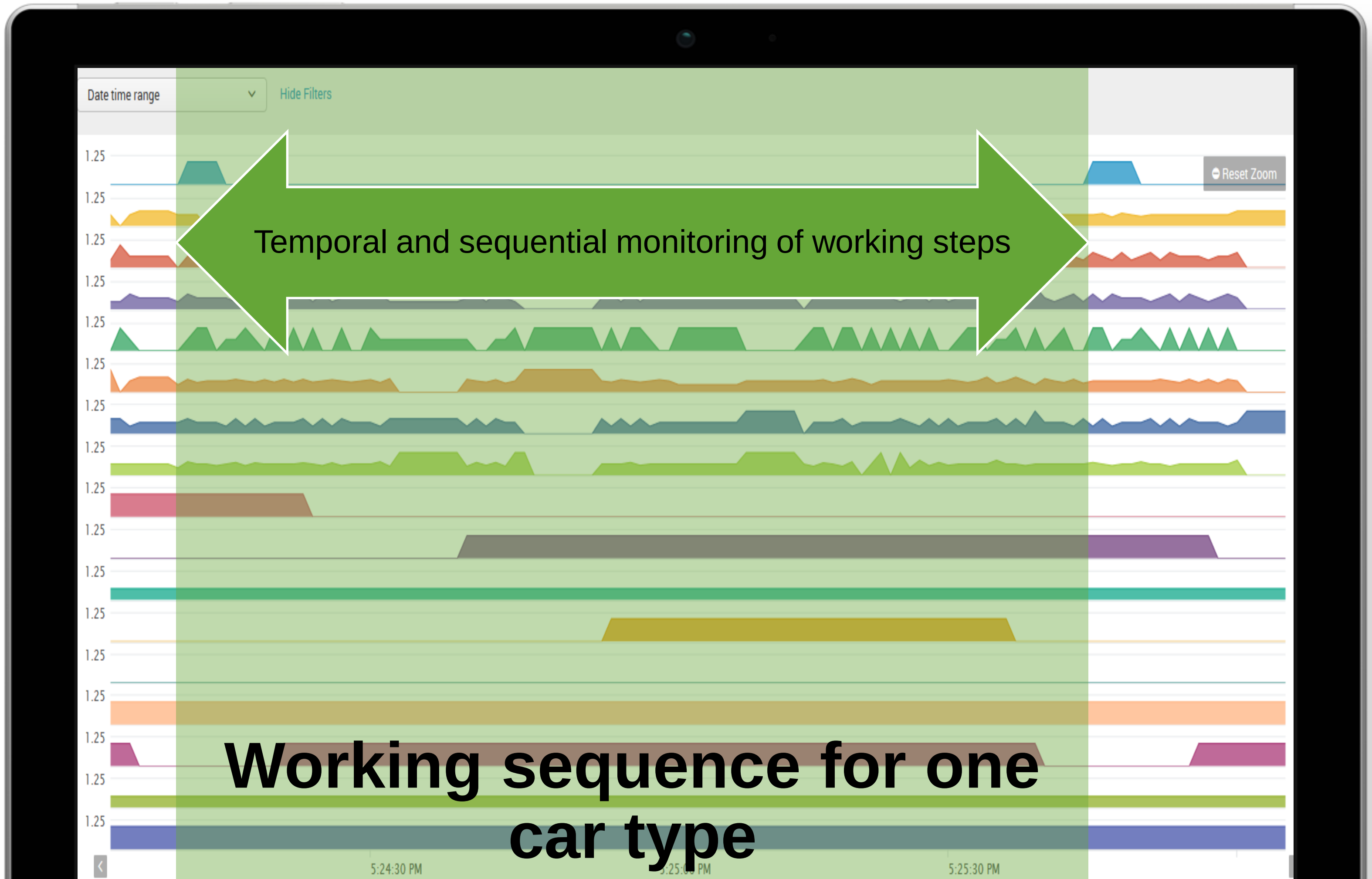
Overview on:

- Logical communication
- Used protocols & data volumes
- Physical cabling based on MAC tables
- Identification of
  - missing components (technical issues)
  - New devices
  - New communication
- Alarming on cell configuration changes
  - PLC programs/ configurations
  - IO configurations

splunk> .conf18

Production data analytics

from anomalies, root causes and health monitoring



Temporal and sequential monitoring of working steps

Working sequence for one car type

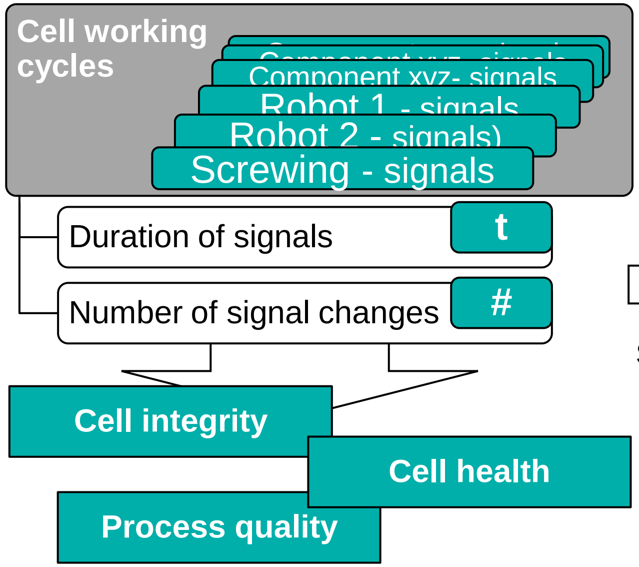
Challenges:

- Different car types
- Different components (doors..)
- Different component weights
- Different automation cell working modes (normal, guided, manual)

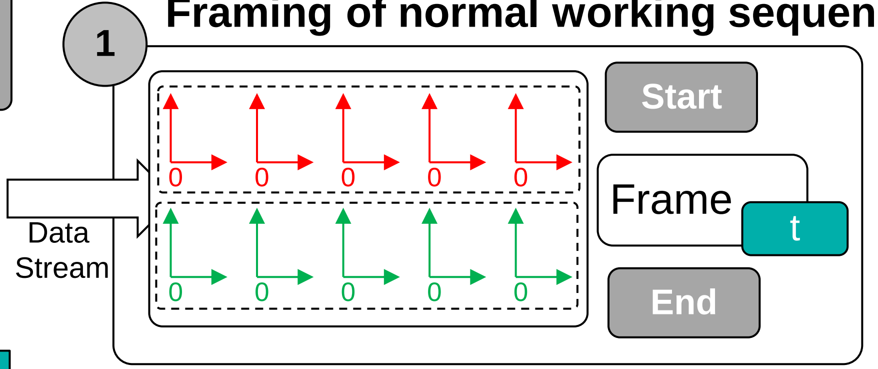
- Automatic type detection
- Automated normal profile learning
- Automated thresholding
- Human readable/understandable health calculations

General analytics approach

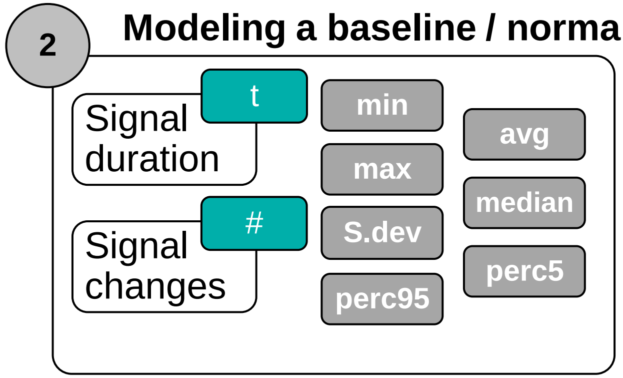
Five simples steps



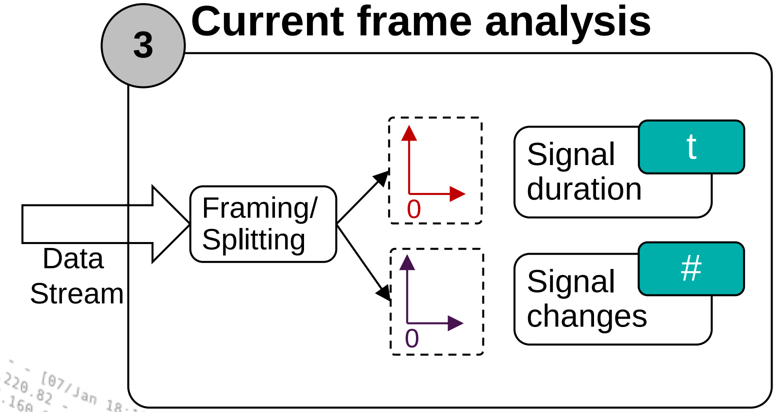
Framing of normal working sequences



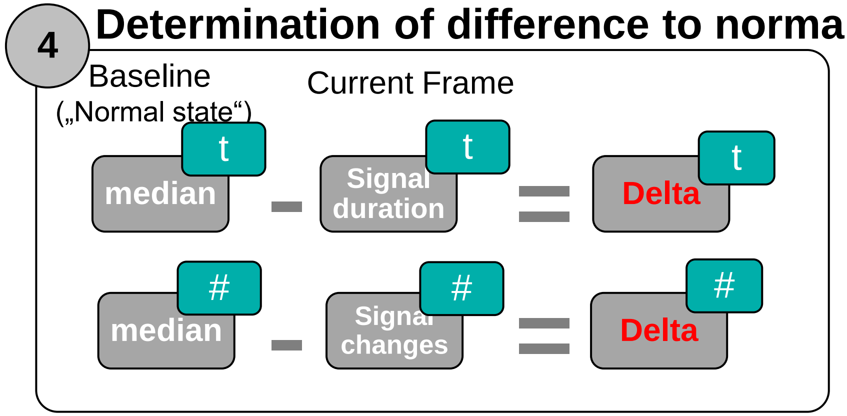
Clustering



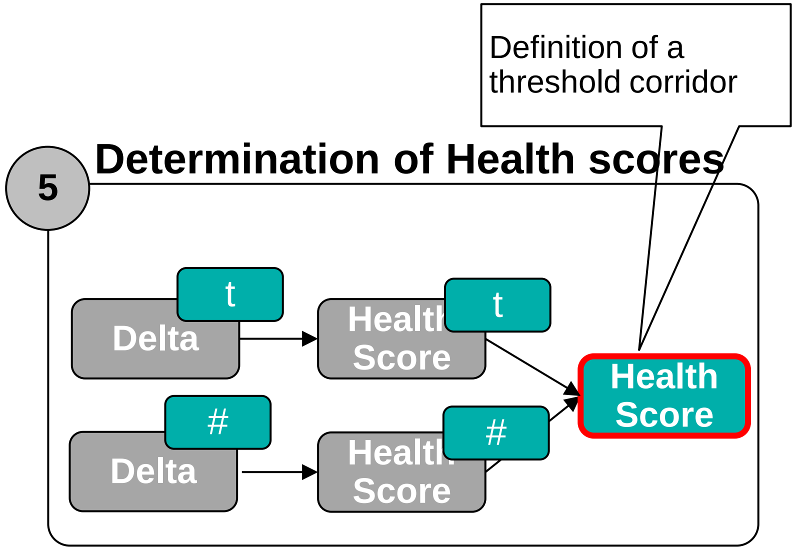
Current frame analysis



Determination of difference to normal



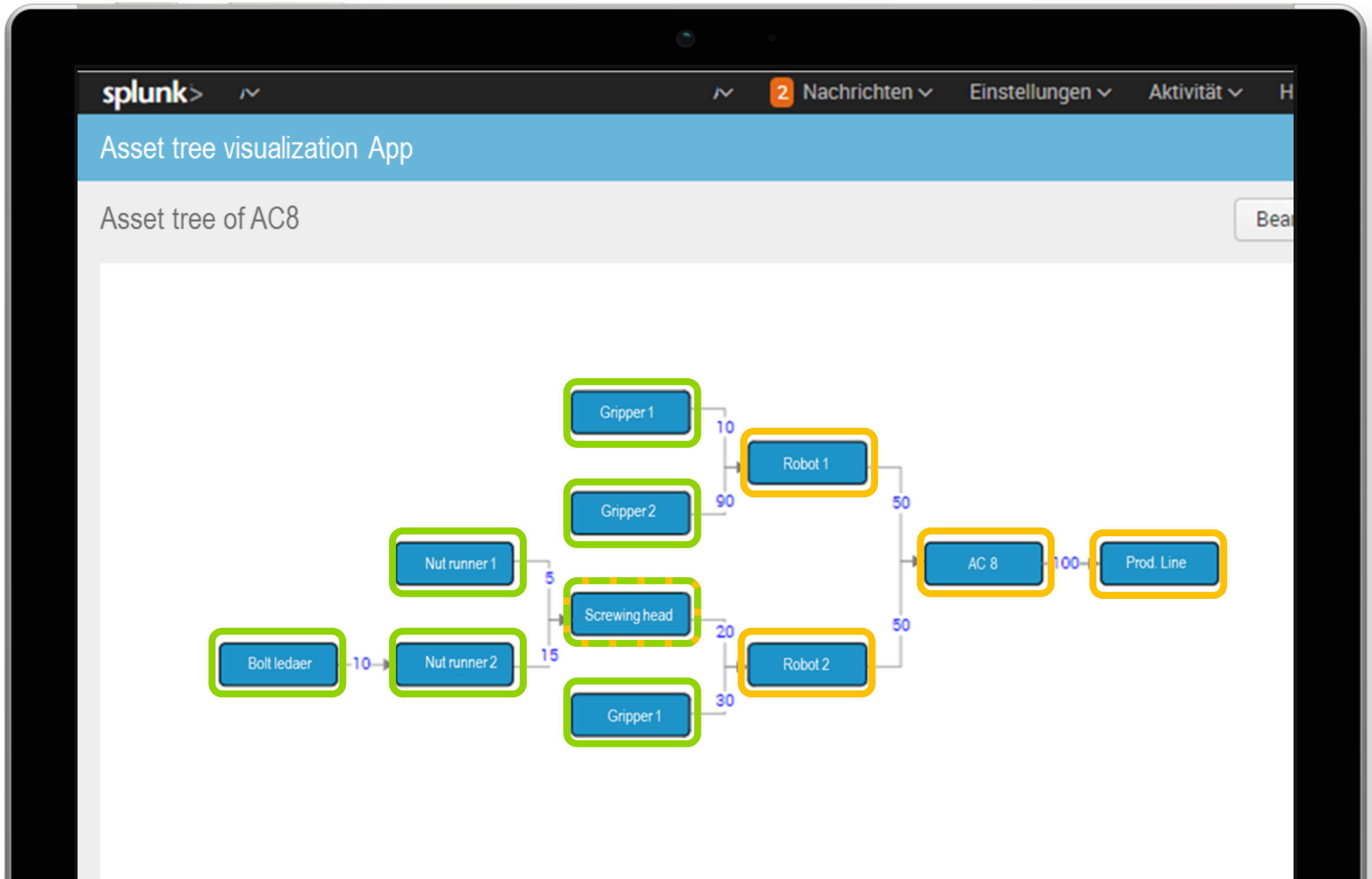
Determination of Health scores



splunk> .conf18

Production data analytics

Health score aggregation vial asset trees



From complex to simple:

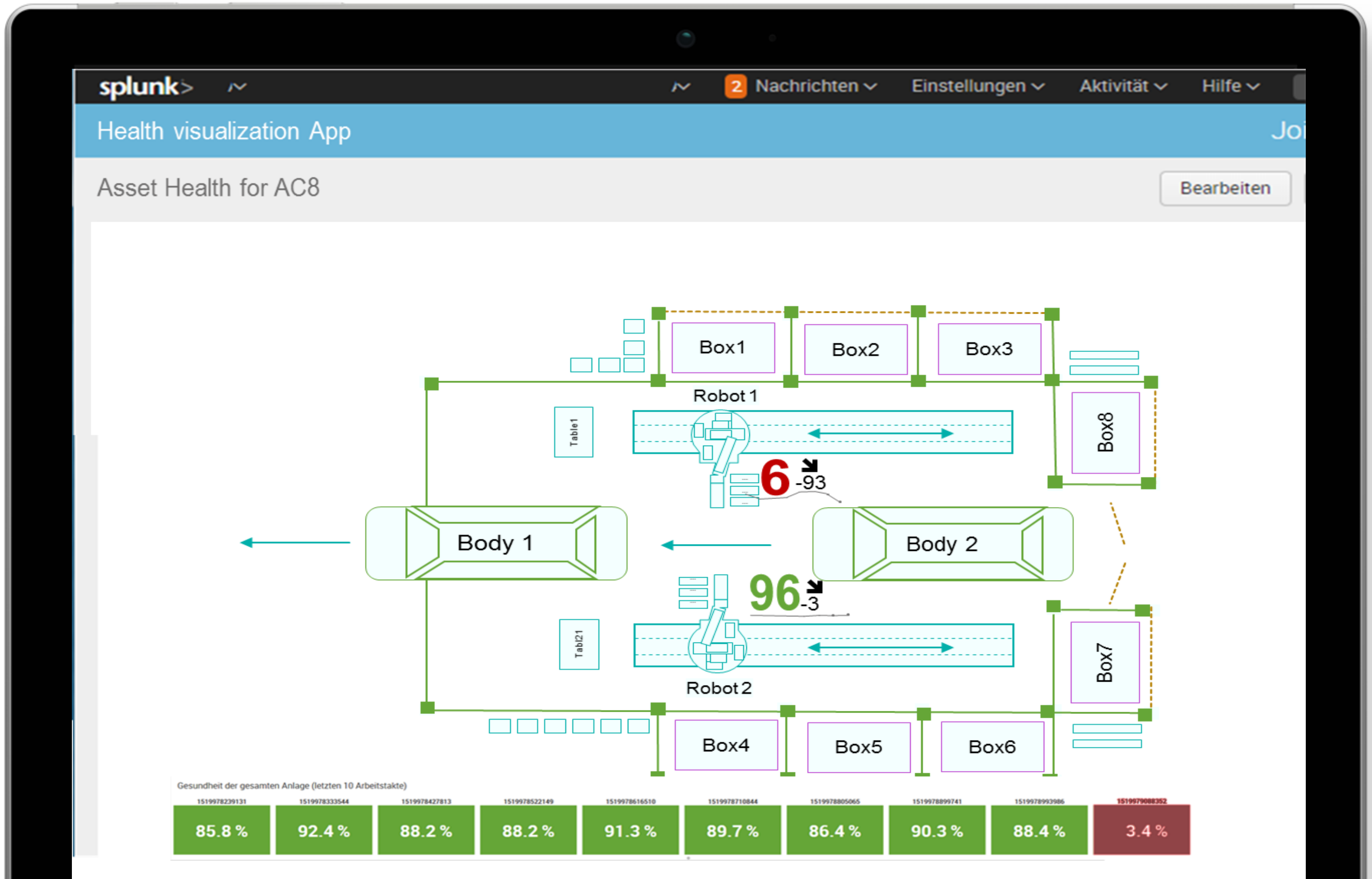
🟧 Aggregated Health Score

🟩 Component Health Score

- Assets as nodes
- Group of assets
- Edge weights determine the influence

Visualization of results

Health monitoring, predictive maintenance and root causes



Gesundheit der gesamten Anlage (letzten 10 Arbeitstakte)

1519978239131	1519978333544	1519978427813	1519978522149	1519978616510	1519978710844	1519978805065	1519978899741	1519978993986	1519979088352
85.8 %	92.4 %	88.2 %	88.2 %	91.3 %	89.7 %	86.4 %	90.3 %	88.4 %	3.4 %

Visualization:

- Using the drawings from construction plans
- Indication of the KPIs next to assets in the drawing
- Drilldown capabilities from high level into the details
- Overview on the last 10 production cycles
- Showing health monitoring KPIs, trends & anomalies based on
  - Components
  - Asset groups
- Integrity monitoring: configuration changes are also visualized based on components and asset groups

Analyzing production lines

Win-Win for security and efficiency

- Increased cyber protection
- Reduction of unplanned maintenance activities
- Increased availability
- Reduction of operational costs

Summary

Key takeaways

- You can do security monitoring und production data analytics on different layers
  - Layer 3&4 production data is often available already and can provide the context
  - Layer 1&2 data is required to cover security und production efficiency
    - Security monitoring: layer 1&2 are holding > 80 % of production assets
    - Production analytics: only layer 1&2 data allows for predictive maintenance
  - Use passive data collection to avoid configuration, service, guarantee discussions

- Shop floor data analytics
  - Use the same technology stack for production data analytics and security monitoring
  - Main stakeholder are the maintenance
  - Combine production analytics with security analytics and vice versa

- Security und production data analytics is a winning team

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>