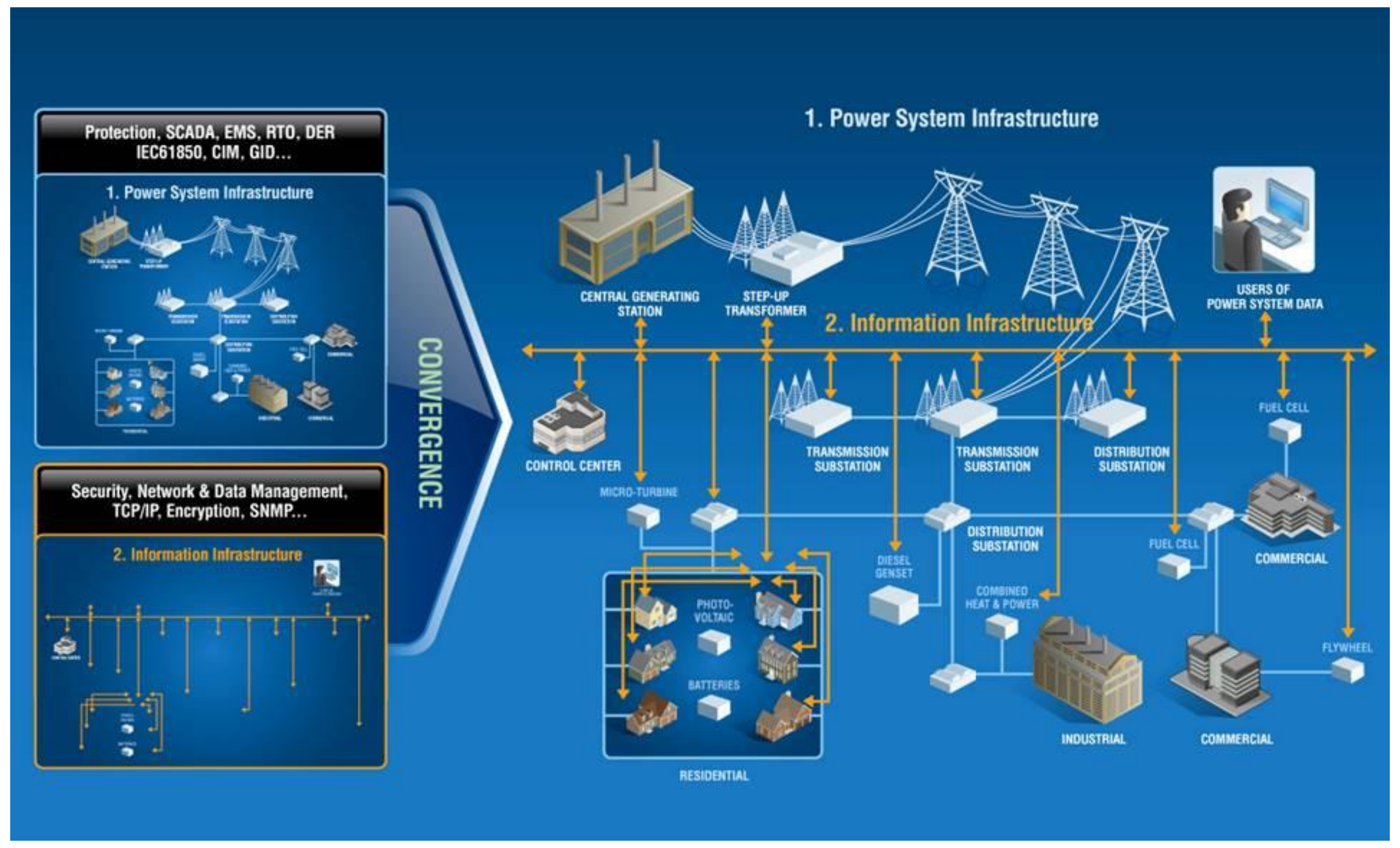
# Industrial Control System Security

Marc Stoecklin, Andreas Wespi

## Industrial Control Systems – Are They Secure?

The convergence of IT (information technology) and OT (operational technology) and the rise of the "Internet of Things" make cybersecurity imperative, in particular for industrial control system (ICS) and supervisory control and data acquisition (SCADA) environments.


Protection, SCADA, EMS, RTO, DER IEC61850, CIM, GID...
1. Power System Infrastructure
Security, Network & Data Management, TCP/IP, Encryption, SNMP...
2. Information Infrastructure
CONVERGENCE
1. Power System Infrastructure
CENTRAL GENERATING STATION
STEP-UP TRANSFORMER
USERS OF POWER SYSTEM DATA
2. Information Infrastructure
CONTROL CENTER
MICRO-TURBINE
TRANSMISSION SUBSTATION
DISTRIBUTION SUBSTATION
FUEL CELL
DIESEL GENSET
COMBINED HEAT & POWER
PHOTO-VOLTAIC
BATTERIES
RESIDENTIAL
INDUSTRIAL
COMMERCIAL
FLYWHEEL

## ICS Security Challenges and Opportunities

**Key challenge: Getting access to data**

- "Do not change a running system" – this principle makes it difficult to develop novel solutions
- In the best case only passive, non-intrusive data collection and analysis is possible
- Collaboration with partner is key to get access to real-world data and to build ICS security solutions

**Opportunities**

- IBM as a leader in IT security intelligence (QRadar) can enhance its portfolio with novel OT security intelligence solutions
- OT security intelligence also provides operational insight – double benefit for customers

### References and links:

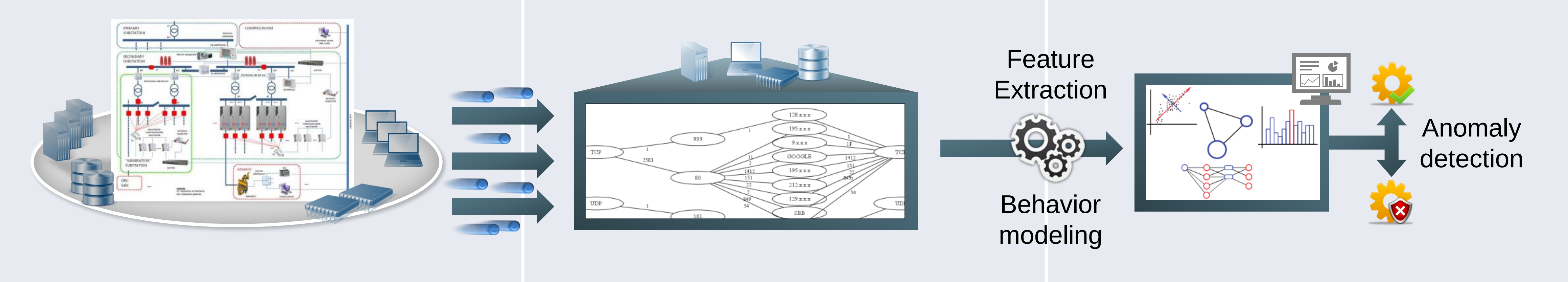
- IBM Security Intelligence: www-03.ibm.com/software/products/en/category/security-intelligence
- IBM Security Research - Zurich: www.zurich.ibm.com/csc/security/

**www.zurich.ibm.com/science-posters/**

## Our Approach to Secure Industrial Control Systems

IBM Research, in close cooperation with IBM GTS and IBM Security Services, is engaging with a large international power-generation and distribution company. We are following a three-pronged approach to assess and improve the security of industrial control systems.

| Activity 1<br>**Instrumentation and Collection** | Activity 2<br>**Passive Network Exploration** | Activity 3<br>**Anomaly Detection** |
|---|---|---|
| – Identify strategic points in the network<br>– Collection of network data (e.g., NetFlow, packet header information, DHCP/ARP data) | – Identification of devices<br>– Collection of much as possible information about the devices<br>– Understanding the traffic flows, communication patterns, and dependencies | – Characterize the normal behavior of the network traffic<br>– Mine the traffic for abnormal deviations |



## Our Solution – ICS Security Console

**Use case and data-driven**

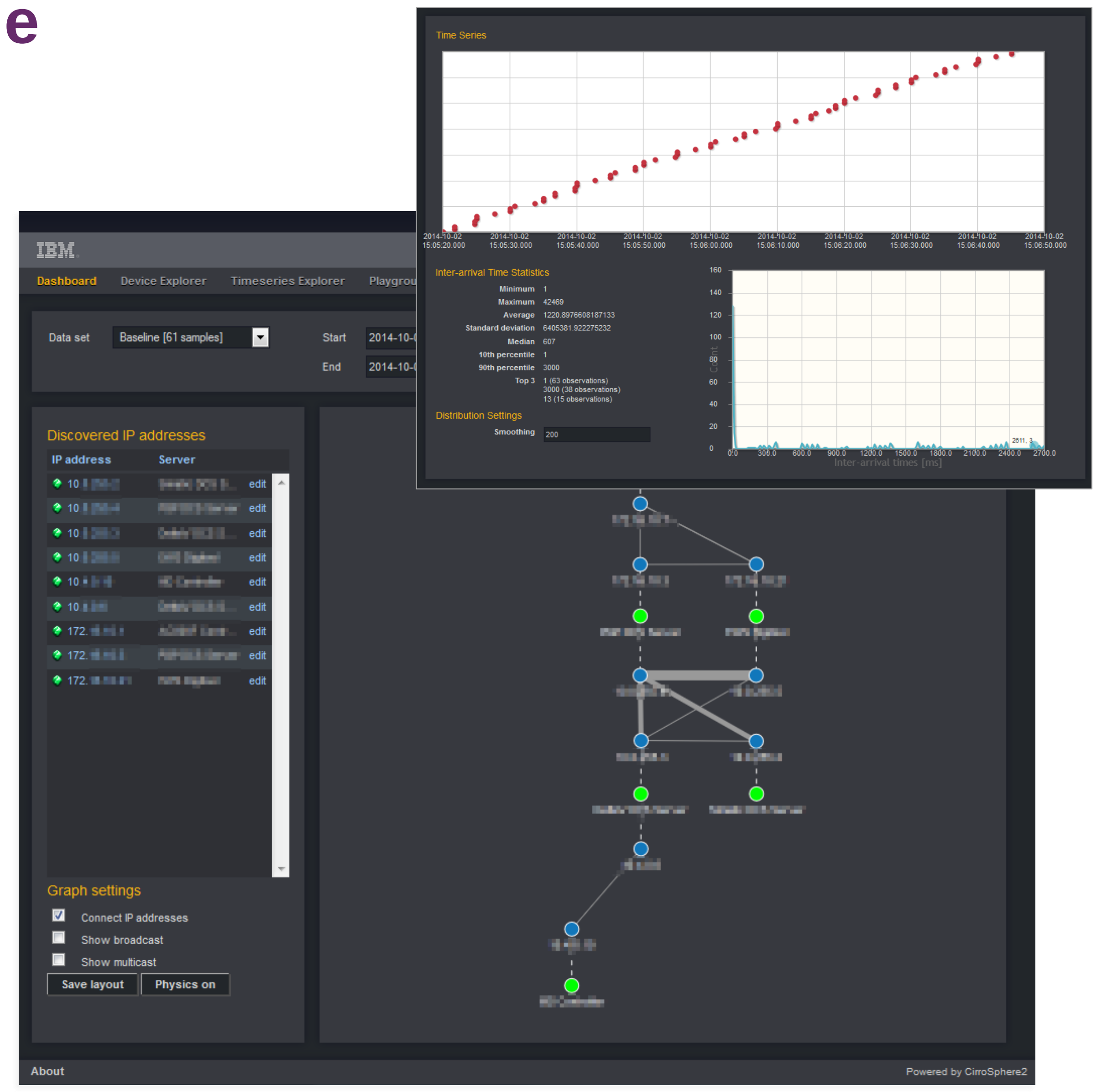
- Known attacks (e.g., Stuxnet, Havex, Duqu)
- Access to real-world data and environments
- Feedback from ICS domain experts

**Multi-layer anomaly detection**

- Device layer: inventory behavior
- Traffic layer: behavior/interaction patterns
- Control layer: access and command actions
- Operation layer: OPC tag operations and values

**Techniques**

- Machine learning on categorical and time-series data
- Statistical analyses


Time Series
IBM
Dashboard
Device Explorer
Data set
Baseline
Start
End
Discovered IP addresses
IP address
Server
Graph settings
Connect IP addresses
Show broadcast
Show multicast
Save layout
Physics on
About