

Confidential & Proprietary

Company Presentation

APERIO 

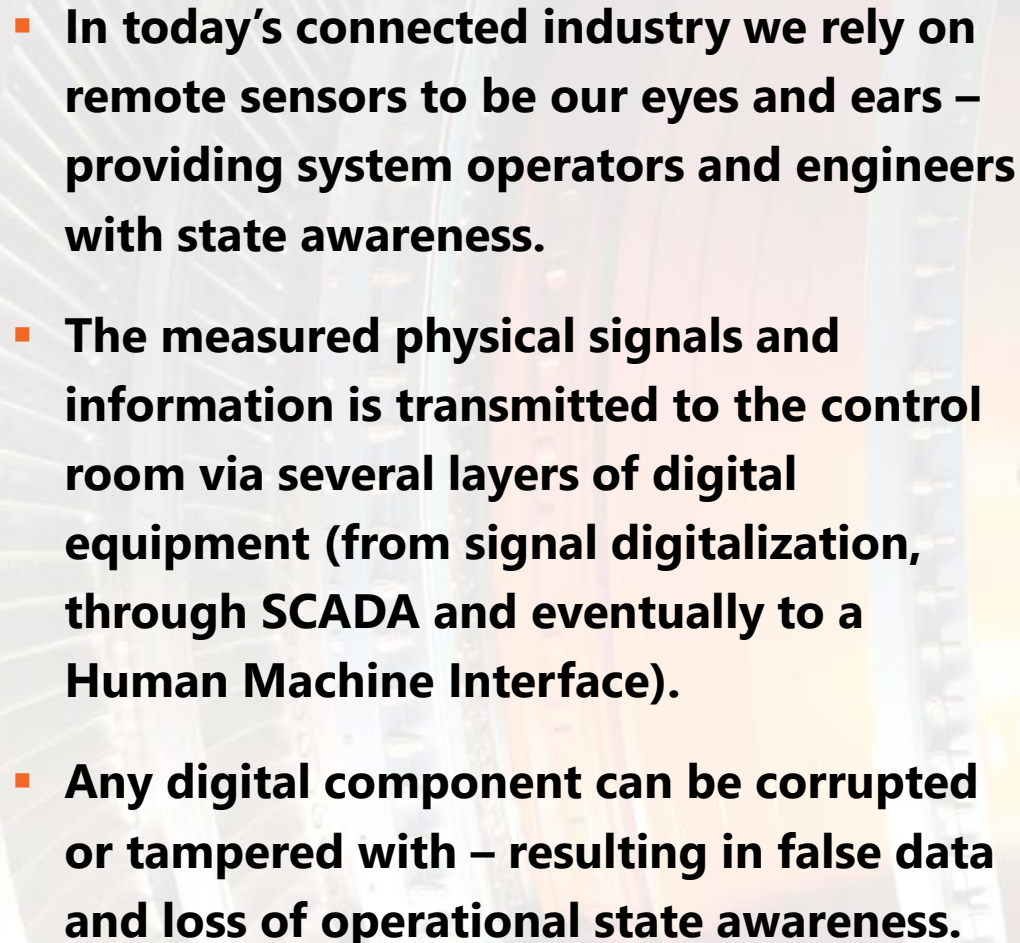
APERIO

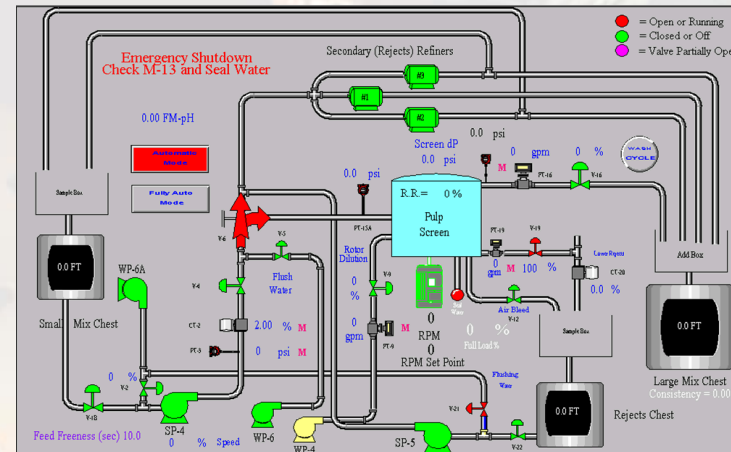
Key concepts:

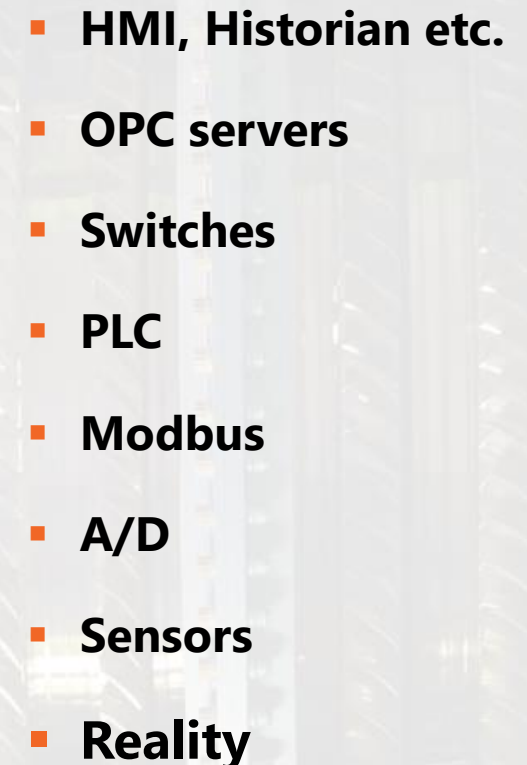
- **Resilience** for industrial systems.
- **Fingerprinting** physical signals.
- **Forgery** detection.

The Problem

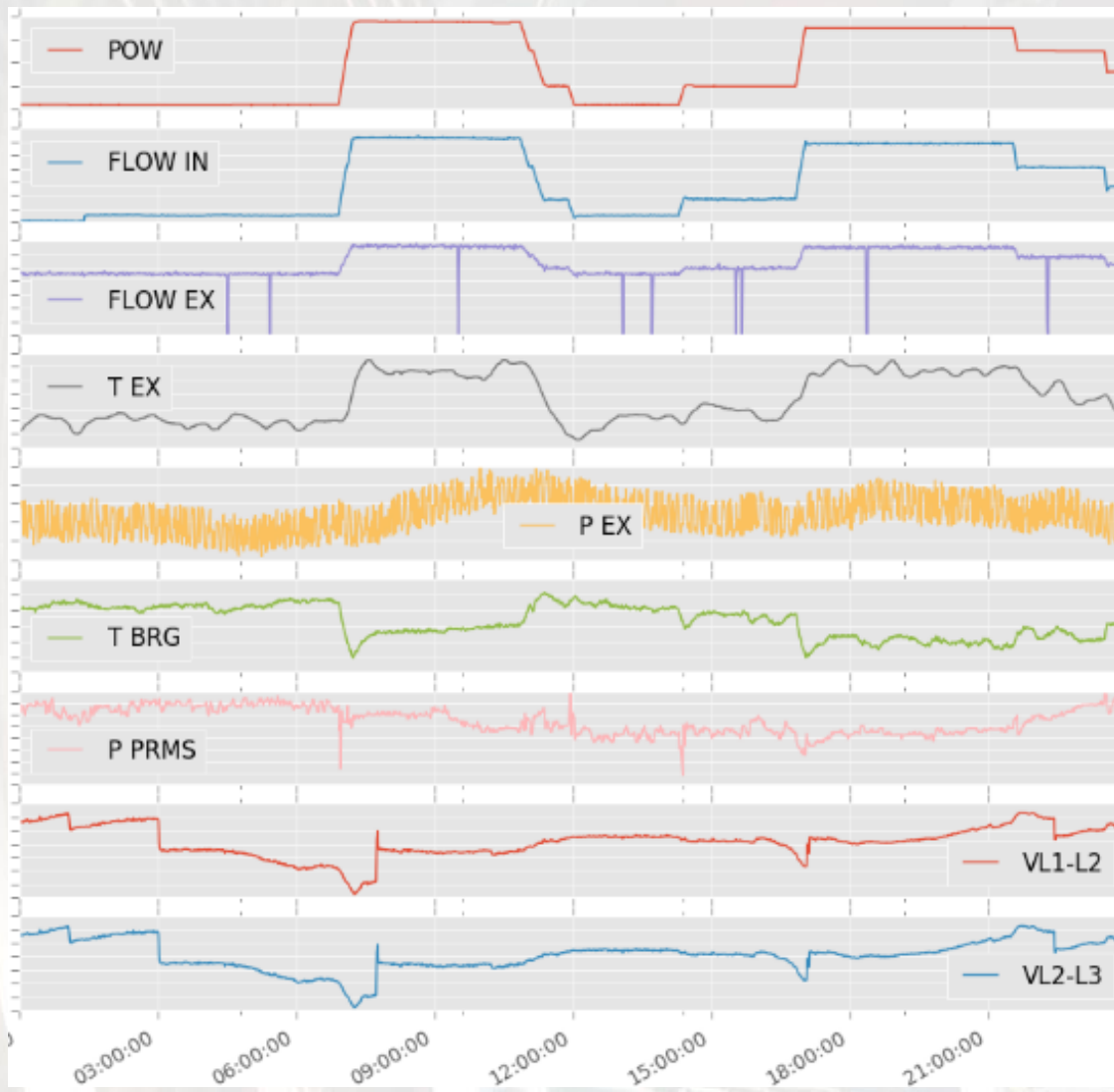
Operational Data Flow

- 
- In today's connected industry we rely on remote sensors to be our eyes and ears – providing system operators and engineers with state awareness.
 - The measured physical signals and information is transmitted to the control room via several layers of digital equipment (from signal digitalization, through SCADA and eventually to a Human Machine Interface).
 - Any digital component can be corrupted or tampered with – resulting in false data and loss of operational state awareness.



- 
- **HMI, Historian etc.**
 - **OPC servers**
 - **Switches**
 - **PLC**
 - **Modbus**
 - **A/D**
 - **Sensors**
 - **Reality**

Sensor Readings From a Customer Power Plant



Types of physical data in the plant:

- Temperature of the metal bearing in turbine (Deg C)
- Exhaust Flow (kg/s)
- Inflow of Gas (kg/s)
- Pressure in the gas pressure reduction system (Bar)
- Generator Voltage (V)
-

Defenses Will Be Breached

**Ukraine Electric Grid Attack
(Dec 2015)**



**US Water Purification Plant Breach
(2016 Verizon report)**



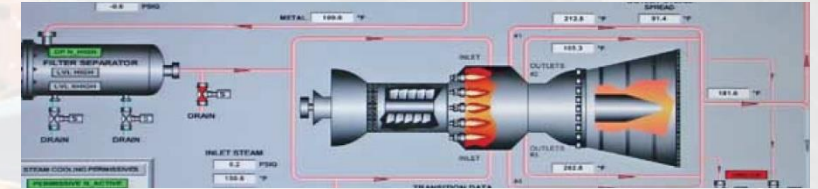
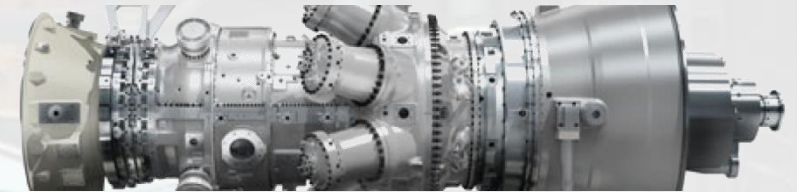
STUXNET



- ICS Attacks are becoming increasingly prevalent.
- Often the main danger is insider threats or contractors with access.
- STUXNET was able to operate for almost 18 months at a high security facility, while destroying crucial equipment, by *forging operational data* – creating an illusion that everything is fine.

State Awareness is the Key For Resilience

- Control systems are built for resilience – as long as they see the truth
- Attackers must forge reported data to overcome controls and create severe damage**



Aperio Data Forgery Protection

APERIO Provides System Resilience



Every physical system has a unique fingerprint



APERIO's cutting-edge algorithms learn these fingerprints



APERIO plugs non-intrusively into existing plant's monitoring systems



APERIO uses the fingerprints to detect forgery and alerts plant operators in real-time



APERIO recovers the true values of the forged data and uncovers the ground truth

APERIO Integrates Into Existing Systems



APERIO Solution

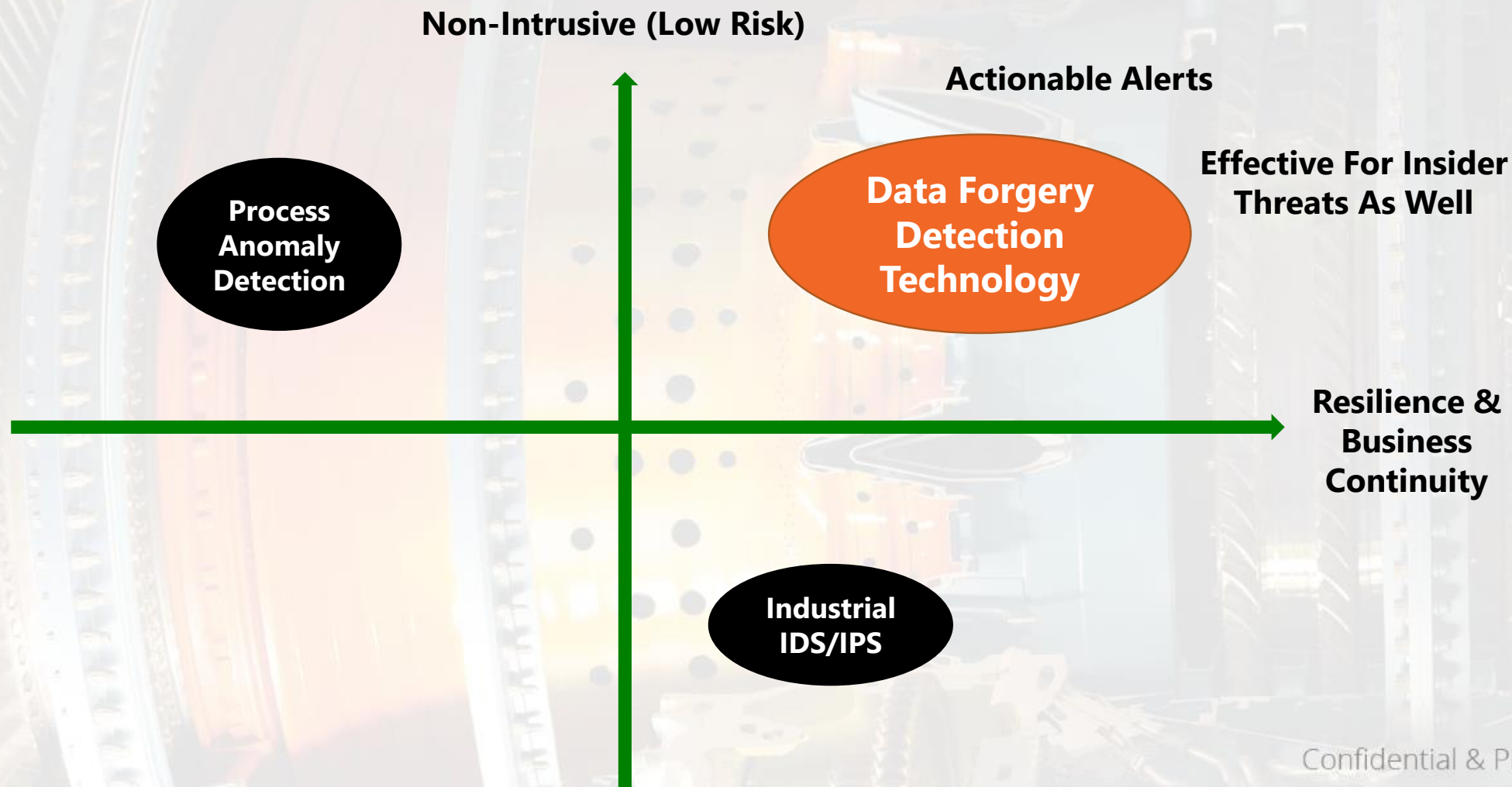
Resilient Control System:

"Maintains **state awareness** and an accepted level of **operational normalcy** in response to disturbances, including threats of an unexpected and malicious nature."

(U.S. Idaho National Laboratories)

APERIO assures **state awareness** at all time, leveraging **existing resilience mechanisms** to prevent malicious actors from causing **severe damage** to equipment, product or human lives.

How Are We Different?



Summary

Awards

**Innovative Security Solution
Competition (Held by ENEL)**



Gartner
**Cool
Vendor
2017**

**1st place, Cybertech Startup
Competition**



**Best Smart Energy Startup (Held
by ESB)**



**Excellence in Corporate Technical
Innovation (Held by ISA)**



**Best Industrial Cybersecurity
Solution (Held by GSN)**



In the Media

- “Tech firm pushes to be the last line of defense against power-plant hackers” - **The Wall Street Journal**
- “Aperio answers the challenge by non-intrusively plugging into an existing control system and unleashing its advanced machine learning algorithms to study and identify the system’s unique ‘fingerprints.’” – **Forbes**
- “Aperio AI detects false fingerprints behind erroneous data” - **Bloomberg**

NOV 15, 2016 @ 09:06 AM 1,039 VIEWS

The Little Bl

Artificial Intelligence Lie Detector To Protect Critical Infrastructure

APERIO System's Value Proposition



- **Non-intrusive**, easy and safe to deploy



- **Extremely low false alerts rate**



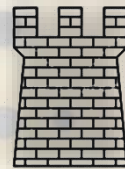
- **Accurate and actionable** alerts



- **Recovers** the ground-truth and **restores resilience**



- **Proactive 0-day attack detection** – catches most advanced attacks before severe damage is caused



- **Last line of defense** – catches both insider and external attackers



- **Enables service continuity** in face of attack

Confidential & Proprietary

Thank You

APERIO 