RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: ECO-F03

A Case Study for Building Cybersecurity Policies for Industrial Robots

Francis Cianfrocca
Founder & CEO
Bayshore Networks
@BayshoreNet @cianfrocca

Gartner COOL VENDOR
2015: Managing OT in a Digital Business

Bryce Barnes
IoT Solutions Architect, Manufacturing & Energy
Cisco
@Cisco

What IT Professionals Need to Know About OT Security

- A new reality for industrial enterprises
- Data capture from OT (Operational Technology) environments
- Operational and SCADA visibility
- Predictive analytics
- Continual process optimization

Why It Matters

- A competitive advantage:
  - Intelligent capture,
  - Aggregation,
  - Inspection, and
  - Analysis
- It’s necessary for survival

Why It's Hard

- Security
- Security
- Security

What's Hard About OT Security

- It's less about CIA
- It's more about Availability, Uptime and Safety
- You can't just shut down or update machines to remediate security problems

OT Security Is Fundamentally Different

- A holistic approach is needed
- Point solutions are not the answer
- Visibility (thru authentication and authorization) *plus* content inspection
- Holistic policy frameworks
- Manageability at scale
- Pervasive enforcement

A Broader View for Enterprise IT

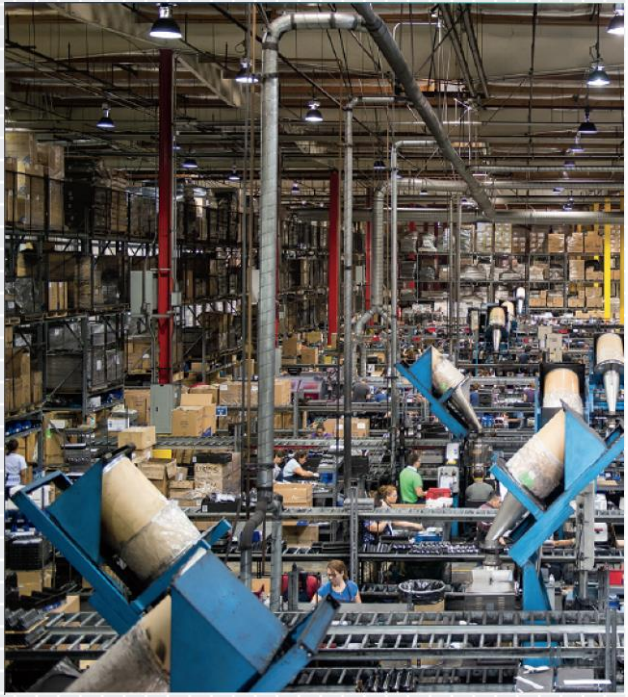
- Computers, apps and networks are managed by IT
- Arrgh! Who will help me figure this out?
  - As assets within Information Security, computers, apps and networks are managed by IT
  - As assets within an Operations Center, their productivity efficiencies and use, computers, apps and networks are managed by IT
  - How are they to be reconciled/converged?

Toward a Solution

- IT *and* OT people need to be deeply conscious of security

Experience and Learnings

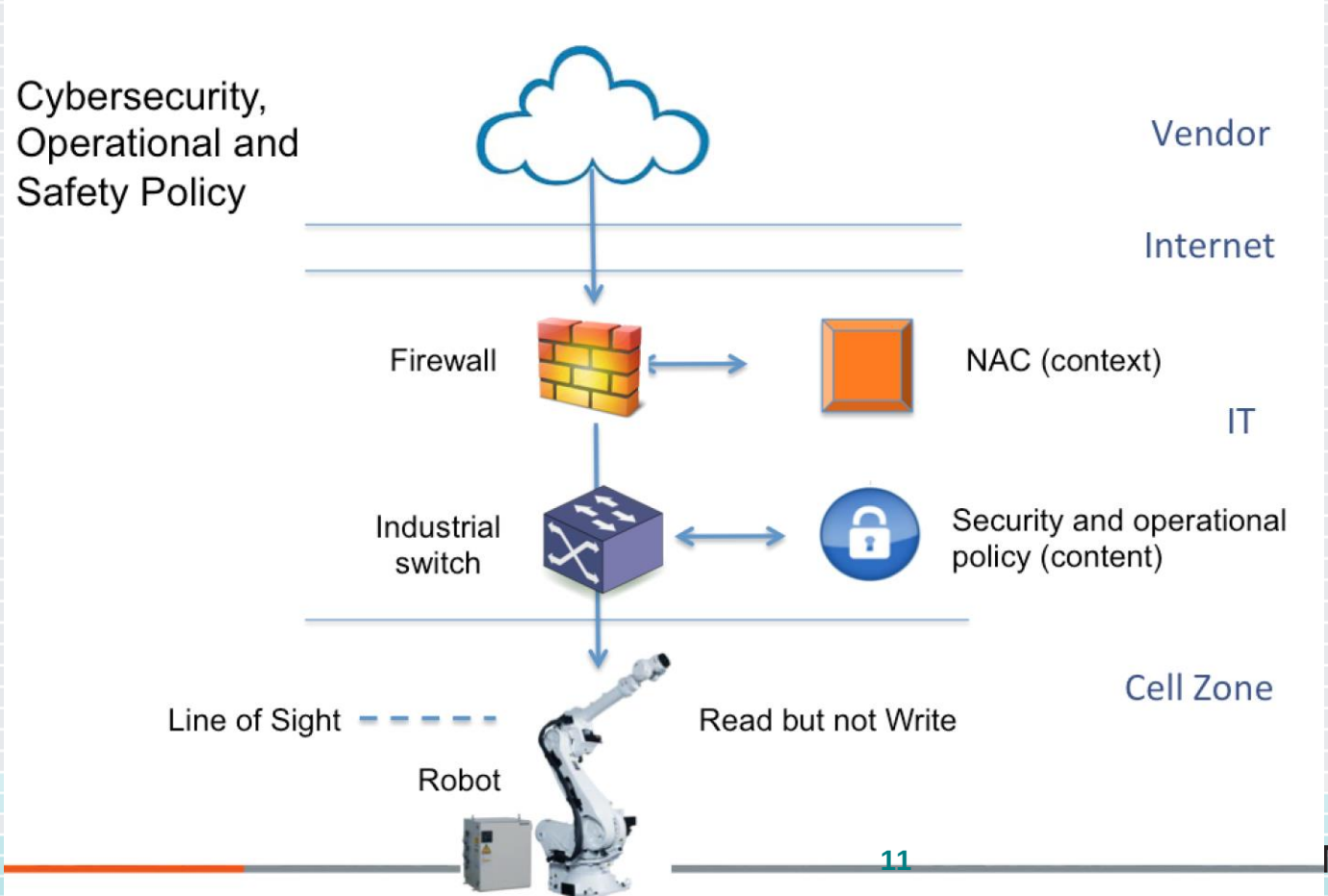
- We'll present an extended example
- Discrete manufacturing
- The general problems are broadly applicable



The Business Driver

- Predictive analytics
- A classic Industrial Internet application:
  - Cuts production downtime
  - Provides secure remote access
  - Cuts maintenance costs

Here's the Architecture



The Technical Objective

- Transmit fine-grained SCADA telemetry to a cloud-based application
- Permit intermittent access by remote access service personnel

The Security Problems

- Requires a new integration between IT and OT networks

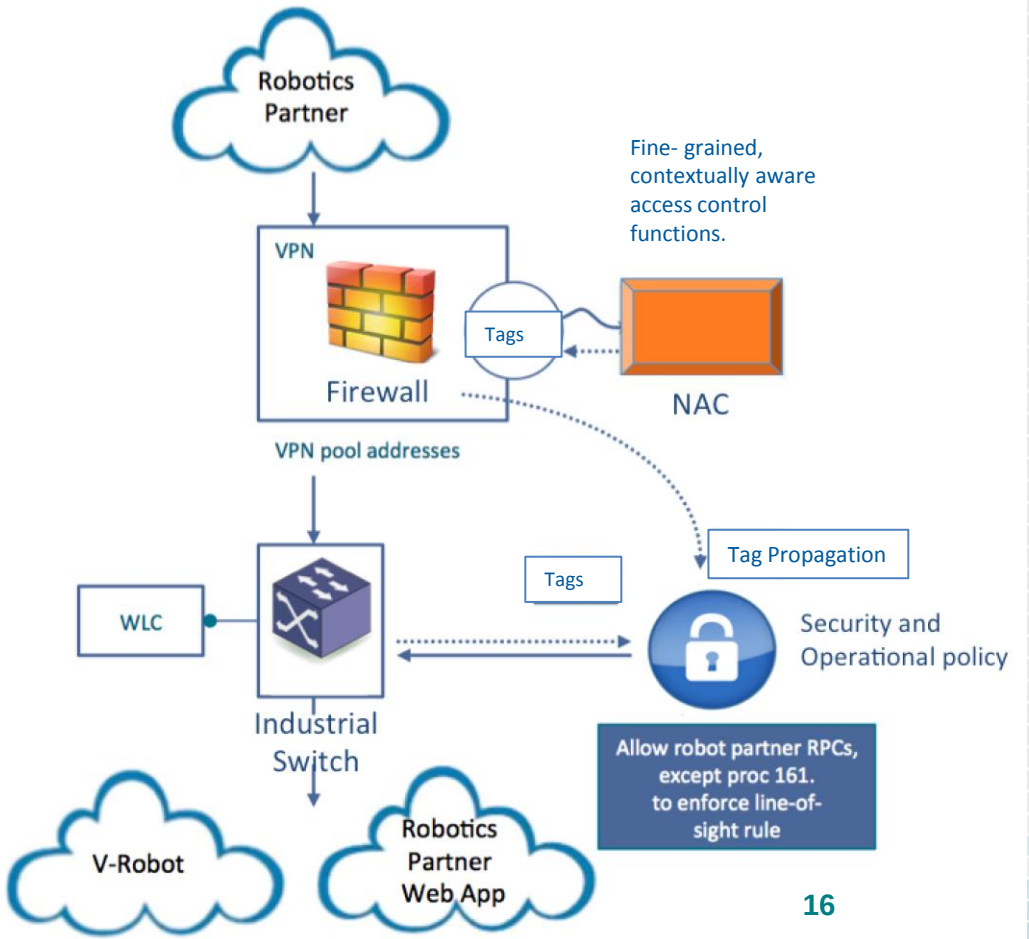
Industrial Networking Is Different

- Transmit identity and contextual-based access controls
- Enforcing who, what, where and their role
- Enforce content-based policy constraints

The Security Risks

- Bad things can happen, particularly if PLCs (Programmable Logic Controllers) or control loops or machines are written to.

Here's the Solution Architecture



Why It Works

- Unsafe transactions are blocked and machine access is restricted to specific user roles

Holistic Policy

- Many policy frameworks are possible, but you just need one.

How It Helps IT People

- Holistic management
- Solves the *scale* problem
- New, OT-aware security products fill the knowledge gap

How It Helps OT People

- Addresses the business driver.
- Presents minimal risk to availability and uptime.

- **The ideal solution bridges IT and OT.**

How You Can Use This

- The basic technique in OT security is to maintain the aspects of closed system while permitting communications.
  - This means that *identity-based security and encryption* are inadequate, because identity-based controls are inadequate.
  - *Network-based controls* are challenging in the OT space.
  - *Content-based controls* are required to prevent unsafe operations.

  - ***All three are needed for a holistic solution.***

Apply What You Have Learned Today

- Next week you should:
  - Schedule an IT/OT planning meeting to get ahead of your organization's industrial IoT security questions.
- In the first three months following this presentation you should:
  - Identify the roles of IT and OT with regards to your organization's cybersecurity strategy.
- Within six months you should:
  - Select a cybersecurity solution which allows proactive operational, security and safety policy to be set according to your organization's needs
  - Drive an implementation project to protect your industrial infrastructure.