Are Mobile Technologies Safe Enough for Industrie 4.0?

Presented by

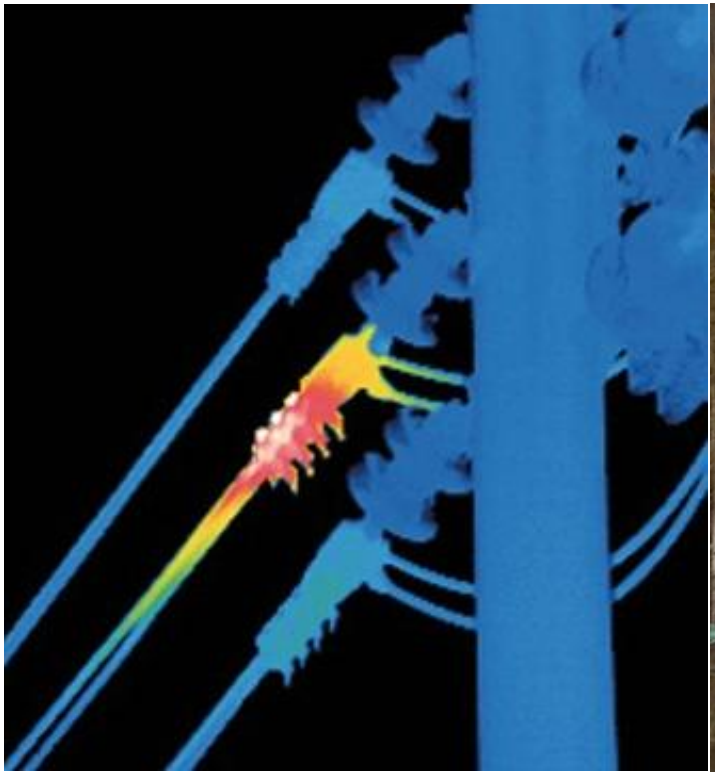
Bryan Owen PE

Mobile Technology is Awesome!

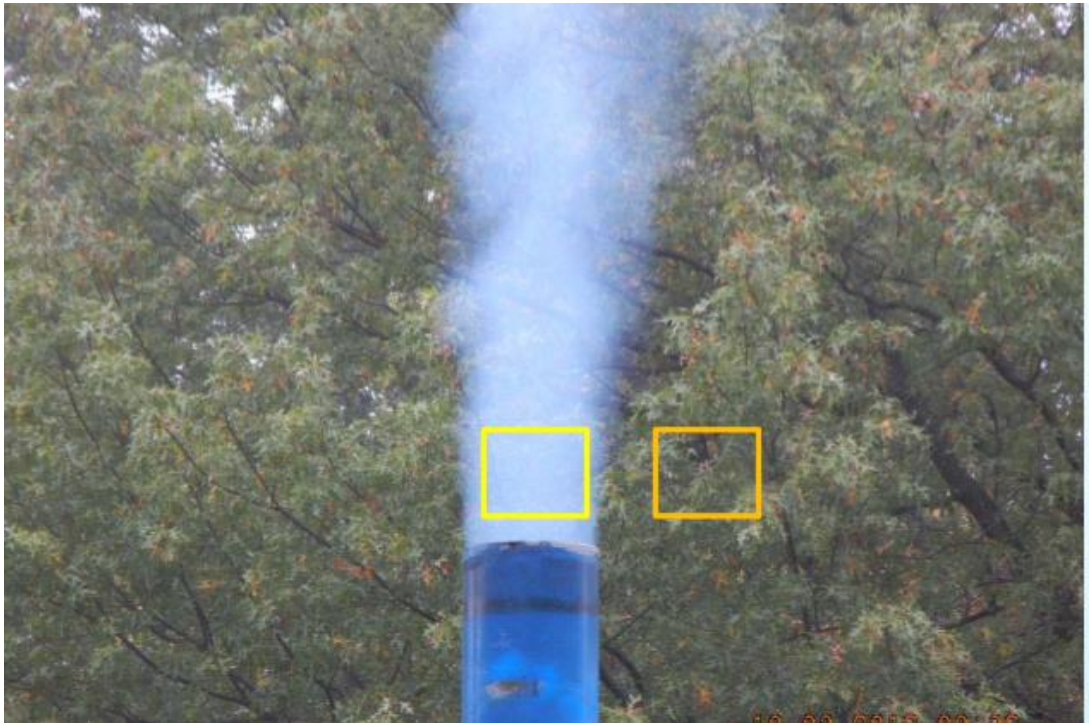
- Cameras
- Drone UAVs
- GPS
- Sensors
- Smart phones
- Wearables

https://www.osisoft.com/Presentations/Geospatial-Sensor---Driven-Analytics-Using-Drones/

Optimize remote asset inspection use cases



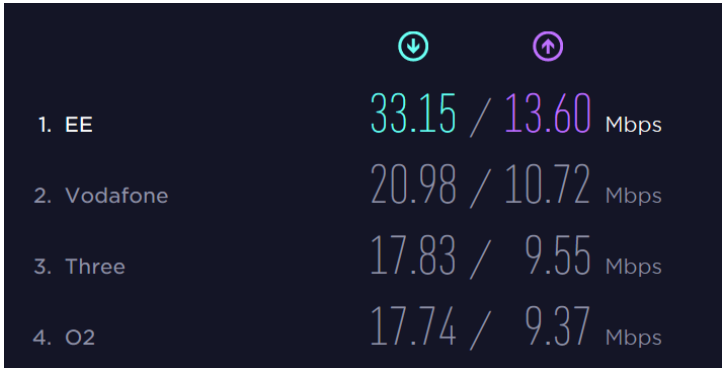
Extend from inspection to Regulatory Monitoring



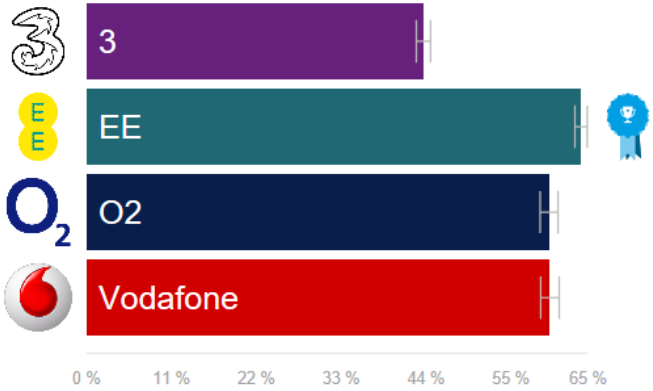
- Calculate the average Red, Green, Blue (RGB) values in the plume and in the background using imaging software like ImageJ.
- Subtract the RGB values.
- Plot the difference.

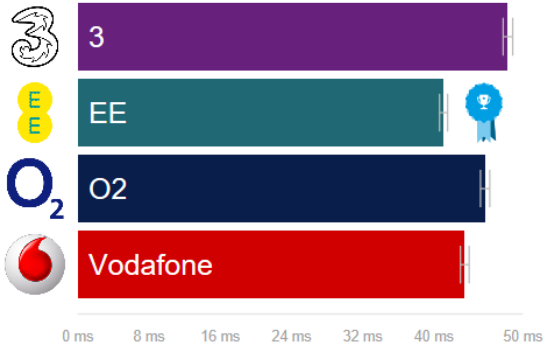
4G is Convenient and Fast Enough

- Availability ~50%
- Down speed ~20Mbps
- Up speed ~10Mbps
- Latency ~45 ms



http://www.speedtest.net/awards/gb/london





https://opensignal.com/reports/2016/10/uk/state-of-the-mobile-network

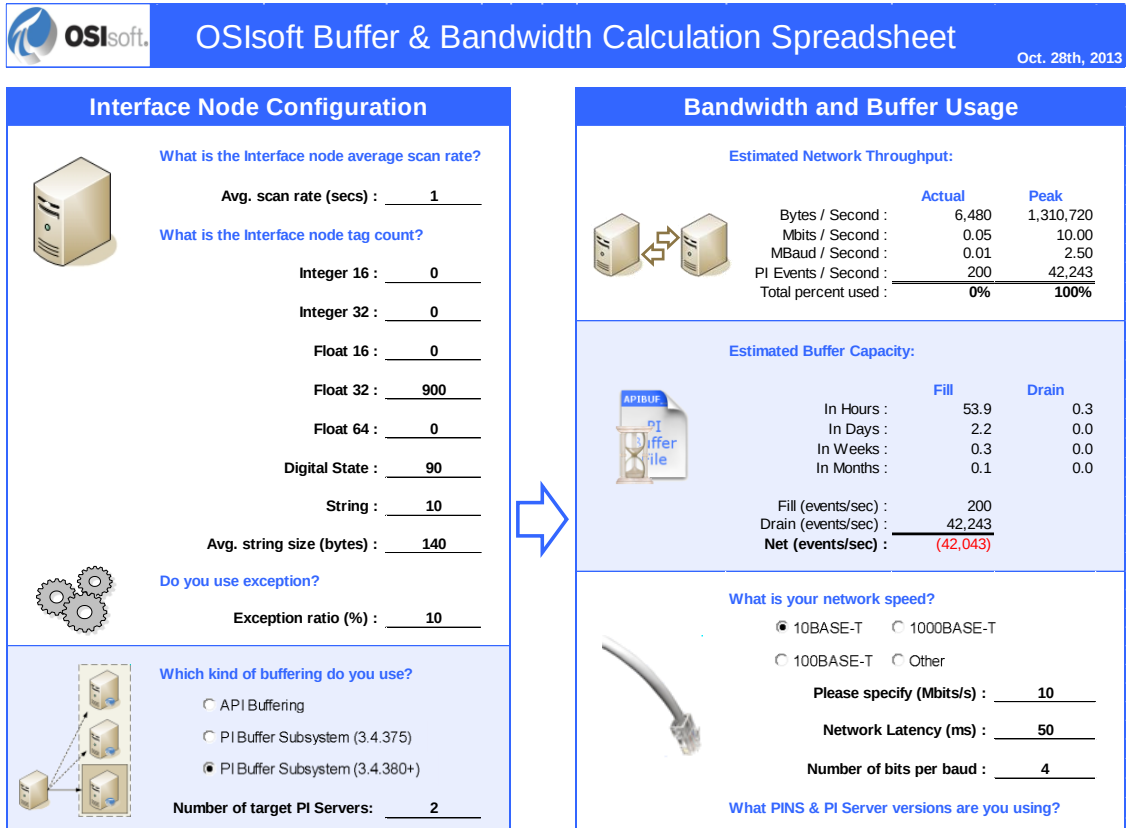
Lightweight Data Collection at the Edge over 4G

Benchmark

- Tags ~1000
- Scan ~1s
- Utilization ~5%

Buffering (2 Servers)

- ~2days/GB
- ~20m/GB @10Mbps



What about Security Issues with Mobile Networks?

Signaling System 7

- All carriers
- Design flaw
- No quick fix

Congress calls on Homeland Security to warn Americans of SS7 hacking threat

Tech Crunch Mar 15, 2017 by Taylor Hatmaker (@tayhatmaker)

Oregon Senator Ron Wyden and California Representative Ted Lieu are pressing the Department of Homeland Security (DHS) on a mobile network vulnerability that they consider to be a systemic digital threat. In a new joint letter, the two members of Congress questioned DHS Secretary John Kelly about flaws inherent in Signaling System 7 (SS7), a global telecommunications protocol that allows phone networks to route calls and texts

What about industrial protocols like Modbus?

Vulnerable by design too (e.g. “Force Listen Only Mode”)

- Active communication is turned off
- Waits forever until “Restart Communications Option”
- Script kiddie exploits in the wild

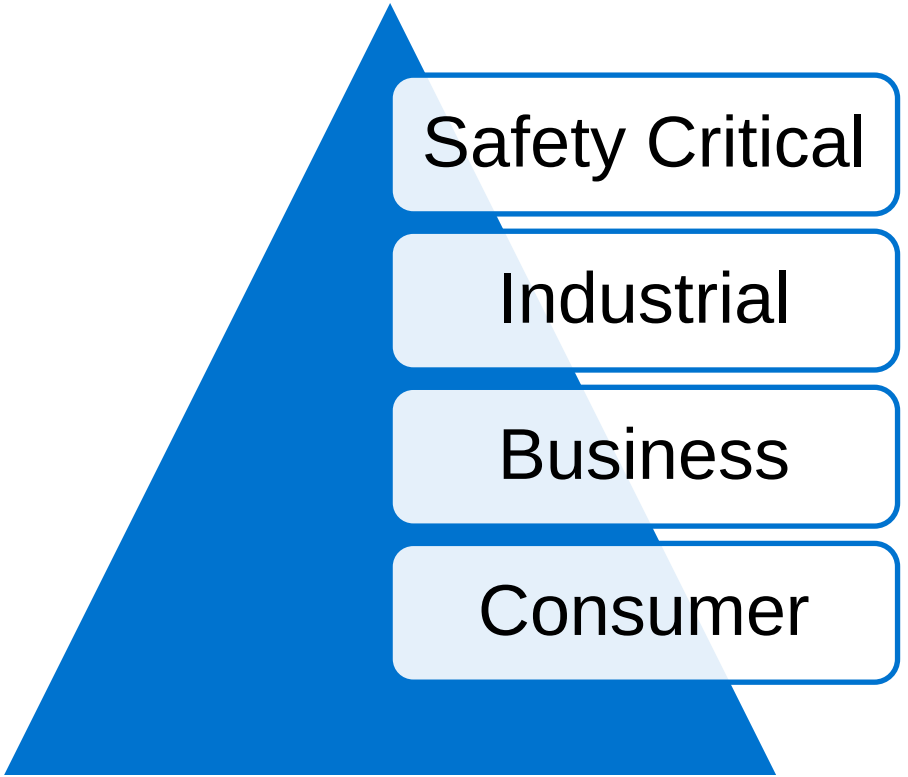
Bad idea: Modbus over mobile networks
If you must, restrict functions at device edge

Better idea: IIoT gateway pattern
(Intermediate PI Connector or Interface node)

Mobile might not be ready for “Safety Critical”

IIoT security challenges are whatever devices cannot do safely

…until they can.

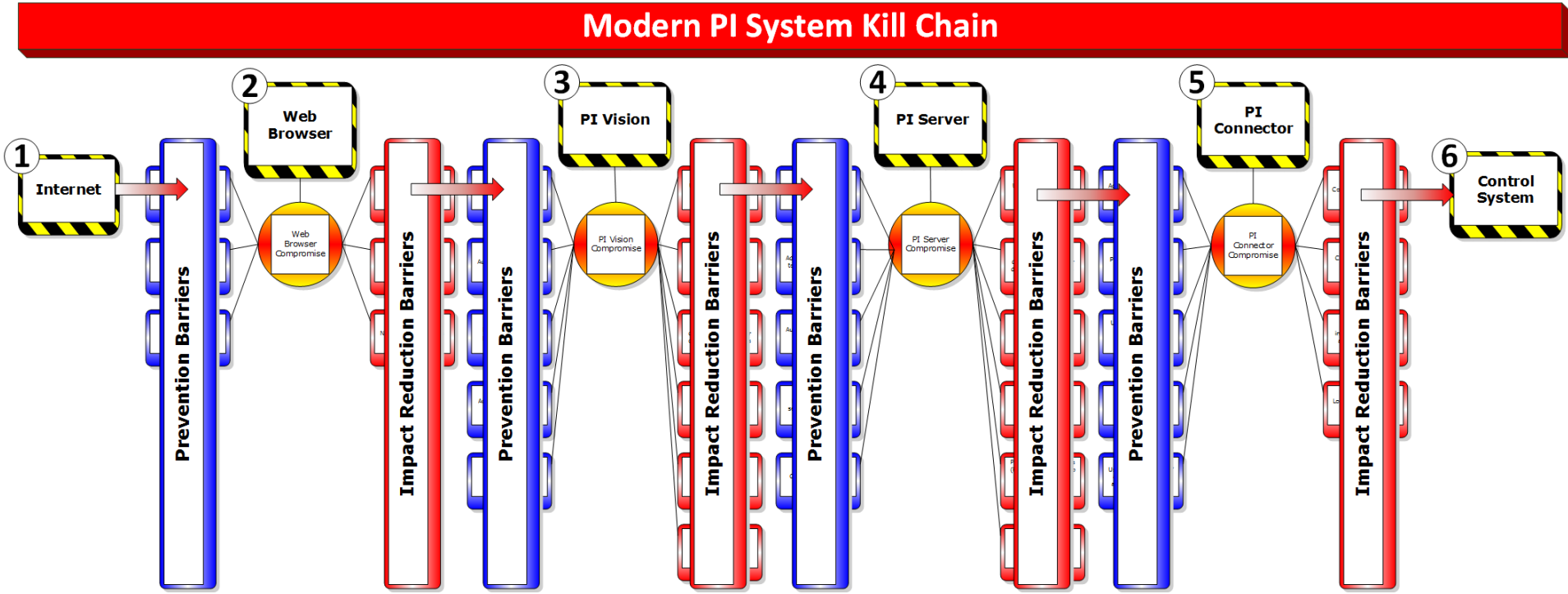


Use a Purpose Built Protocol for Data Collection

- Attack surface
  - Restrict file transfer, KVM access, and scripts
  - Read only mode
- Authentication
  - Device identity, certificate or password
- Message Integrity
  - Tamper detection and fail safe
- Message Privacy
  - Occasionally required and good practice

A ‘Kill Chain’ is recommended

- Attack complexity increases with each layer
- Maximize defender advantage



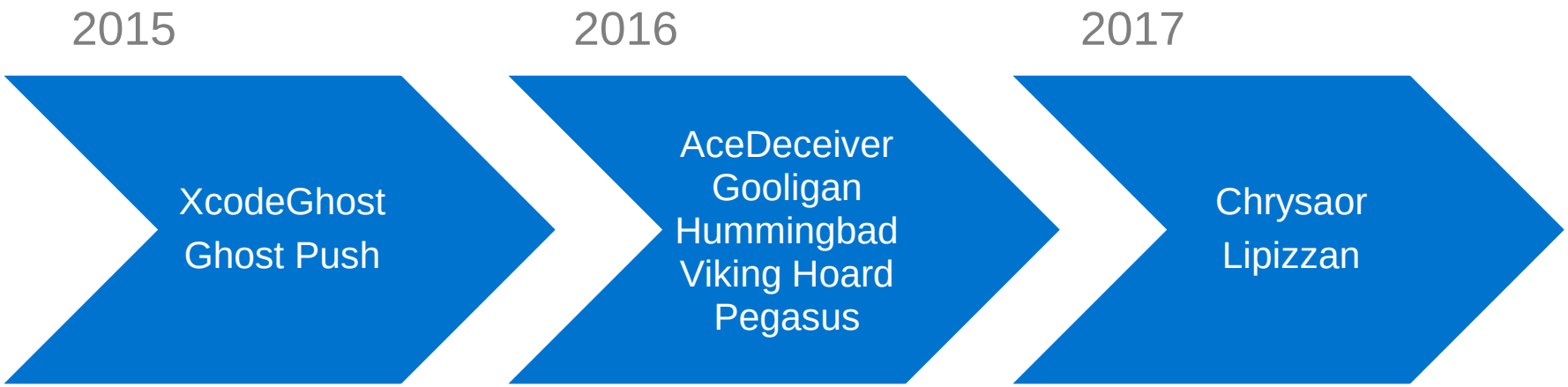
PI Square: [Hardcore PI Coresight Hardening]

Defenses Commensurate with Capability

Industrie 4.0 / IIoT Security Function	Short Life Sensor	Long Life Sensor	Sensor Gateway	Actuator	Actuator Gateway
Health Telemetry					
Network Defenses					
Identity Safeguards					
Device Management					
Data Integrity					

Observed security ‘poverty line’
(eg compromised device management Mirai, StJude)

Malware Targeting Mobile Devices is a Growing Concern



- Ad revenue
- Credential theft

- Credential theft
- Botnet
- Mass surveillance

- Data exfiltration
- Individualized surveillance

Industrial Mobility Security Risks
LOGIIC Project 10

AUTOMATION FEDERATION | The Voice of Automation

1. Common Risks in Native Applications
2. Common Risks in Web Applications
3. Platform Risk
4. Connectivity
5. Nature of Mobility
6. Device Handling
7. Supply Chain Components
8. Installation, Maintenance, and Management

https://www.automationfederation.org/Logiic/LogiicProjects

Common issues for native applications (OWASP M7)

Not using platform security features or security features missing from platform

Examples:

- Certificate validation
- Certificate pinning
- Jailbreak detection
- Debug detection
- Automatic Reference Counting

Common issues for web applications

May require a more sophisticated threat and effort to exploit with high impact

Examples:

- Cross site scripting vulnerabilities
- Session handling and termination risks
- Mishandled cookies

Platform Risks (OWASP M1)

At the time of testing, the attributes of the Android platform led to a greater attack surface than iOS

Examples:

- Transport Layer Security (TLS) version requirements
- Key handling
- Signature verification processes

Connectivity

Perform a risk analysis, based on your own security objectives

Examples:

- Connection to control systems
- Access options for internal and external audiences
- Connectivity for central management

Nature of Mobility (OWASP M2)

Security and operational policy should be considered

Examples:

- Protecting access to high-value data
- Situational awareness from outside the physical boundaries of a control center or site
- Management of numerous mobile devices

Device Handling

Mobile devices can be difficult to fully protect, both physical security and unauthorized view.

Examples:

- Shoulder surfing data or alerts
- Single-user devices may be necessary
- Decommissioning or reuse of a device

Supply Chain Components (OWASP M10)

Neither vendor nor end user may have the ability to mitigate supply chain vulnerabilities

Examples:

- 3rd party components
- Application development tools
- Web frameworks

Lifecycle: Installation, Maintenance, and Management

Installation and ongoing maintenance of any industrial solution should be considered at several levels.

Examples:

- Server
- Application
- Users
- Devices

My internal report card for PI Vision

Risk	Grade	Comment
Native Applications	A	Browser based defenses are enabled
Web Applications	A	PI Vision design incorporates LOGIIC findings
Platform Risk	A	PI Vision runs on iOS
Connectivity	A	Control system safety is a priority for PI Vision
Nature of Mobility	B	Sensitive data is protected, white paper available
Device Handling	C	Assess improvement opportunities with customers
Supply Chain	B	Dependencies are documented and maintained
Lifecycle	B	Single app server scales to 100s of users

Overall findings from multiple assessments…

Mobility for industrial environments can be done securely if technical and design aspects are managed with appropriate security controls.

The PI System and PI Vision Mobile helps safeguard IT and OT assets.

COMPANY and GOAL

1) OSIsoft, makers of the PI System
2) This project is about enabling valuable and safe mobile use cases for the PI System

CHALLENGE

How do we know it's safe enough to use the PI System for mobile use cases?

- Mobile technology is inherently exposed to cyber threats.
- There is a general lack of industry vetted security guidance on IIoT and mobile use cases.

SOLUTION

Assess the maturity of mobile technology as part of an industry consortium project.

- The project reports on security characteristics of multiple mobile security architectures.
- Benchmark methods and effort to harden the PI System for IIoT and mobile use cases

RESULTS

The PI System and PI Vision mobile can be safely deployed for industrial environments.

- Architecture is a defining security characteristic
- Lifecycle support must be considered

References

PI System

- PI Vision 2017: Installation and Administration guide
- KB01631 – Security tips for PI Vision
- Bow Tie: Hardcore PI Coresight (now PI Vision) Hardening
- How secure are your PI Systems? A primer for PI System baselining
- PI Security Audit Tools

Platform

- Claims-Based Architecture
- Windows Security Baselines
- Microsoft Security Guidance for IIS
- Installing an SSL Certificate in Windows Server
- Security Tool Test: Observatory by Mozilla
- OWASP Secure Headers Project

Thank You

Mobile technology is too useful to wait.
Get started now with PI Vision!

OSIsoft®

Contact Information

Brian Bostwick
Brian@OSIsoft.com
Cyber Security Market Principal

Bryan Owen
Bryan@OSIsoft.com
Principal Cyber Security Manager

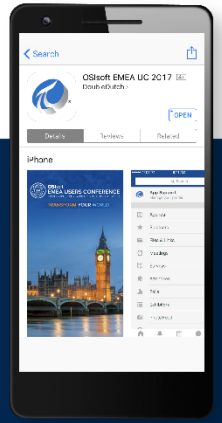
Questions

Please wait for the **microphone** before asking your questions

State your **name & company**

Please remember to…

Complete the Online Survey for this session



Download the Conference App

- View the latest agenda and create your own
- Meet and connect with other attendees

Search **OSIsoft** in the app store

Download on the App Store

GET IT ON Google Play

HTML

감사합니다

Danke

谢谢

Merci

Gracias

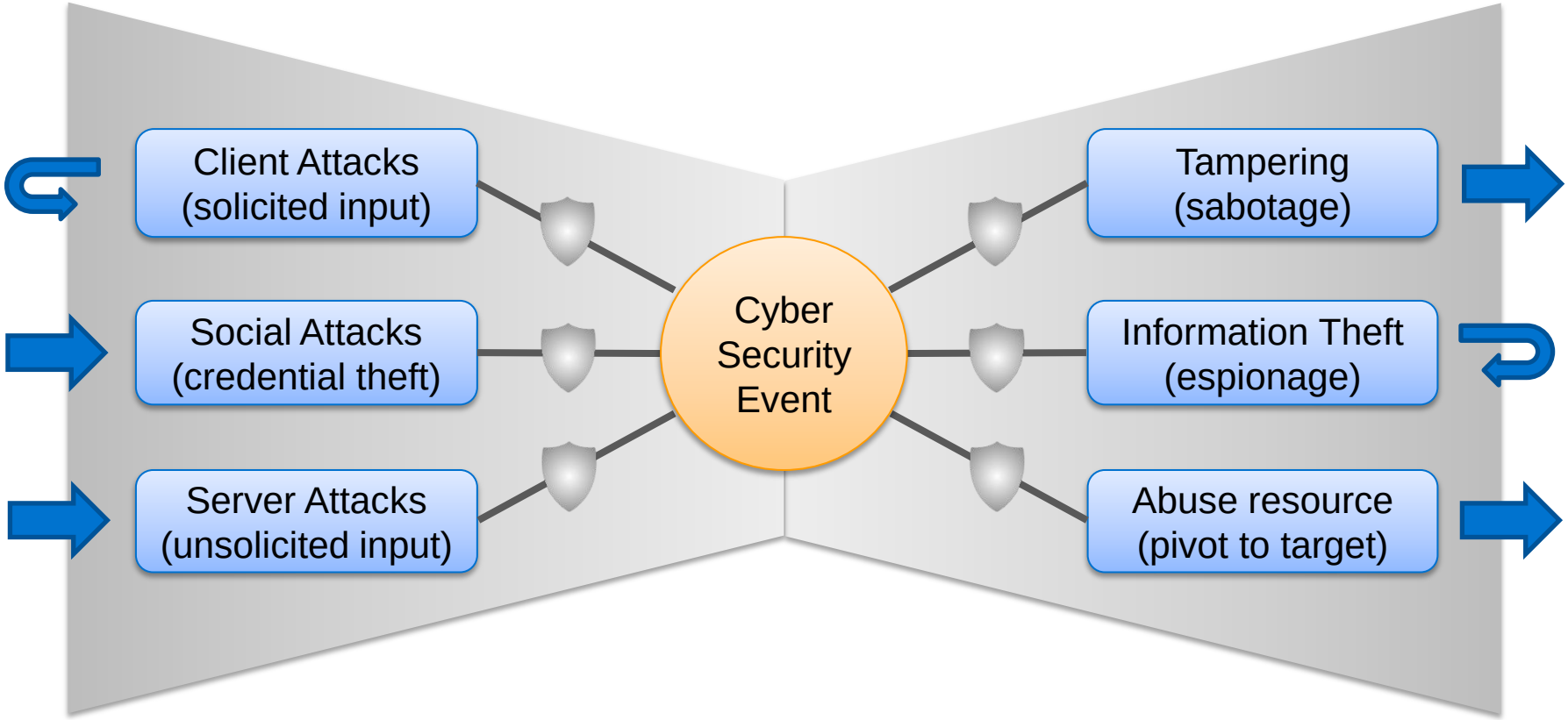
Thank You

ありがとう

Спасибо

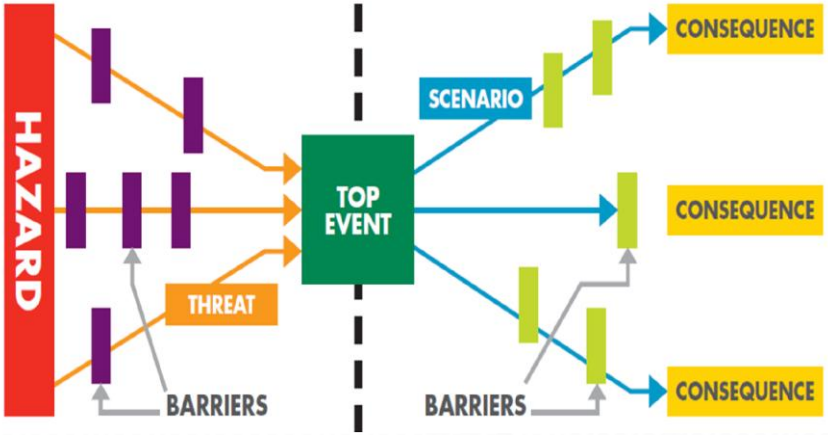
Obrigado

High Level Bow Tie Analysis

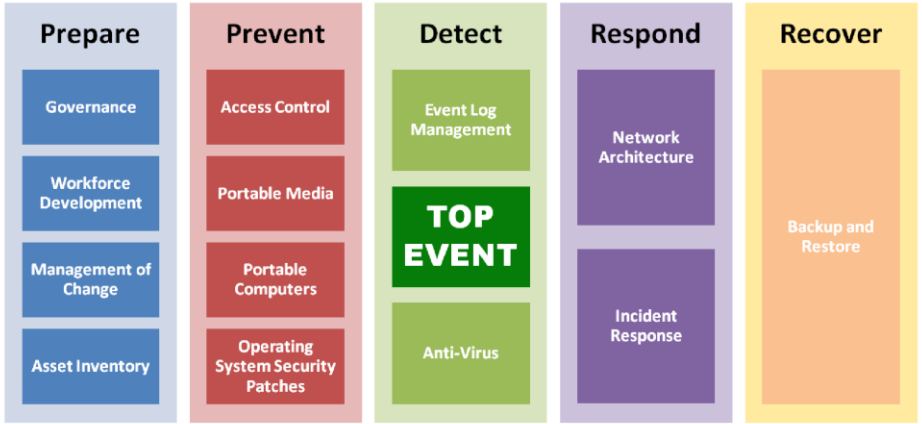


Bow Tie Diagrams: Introduced by Shell

Engineering Bow-Tie Model

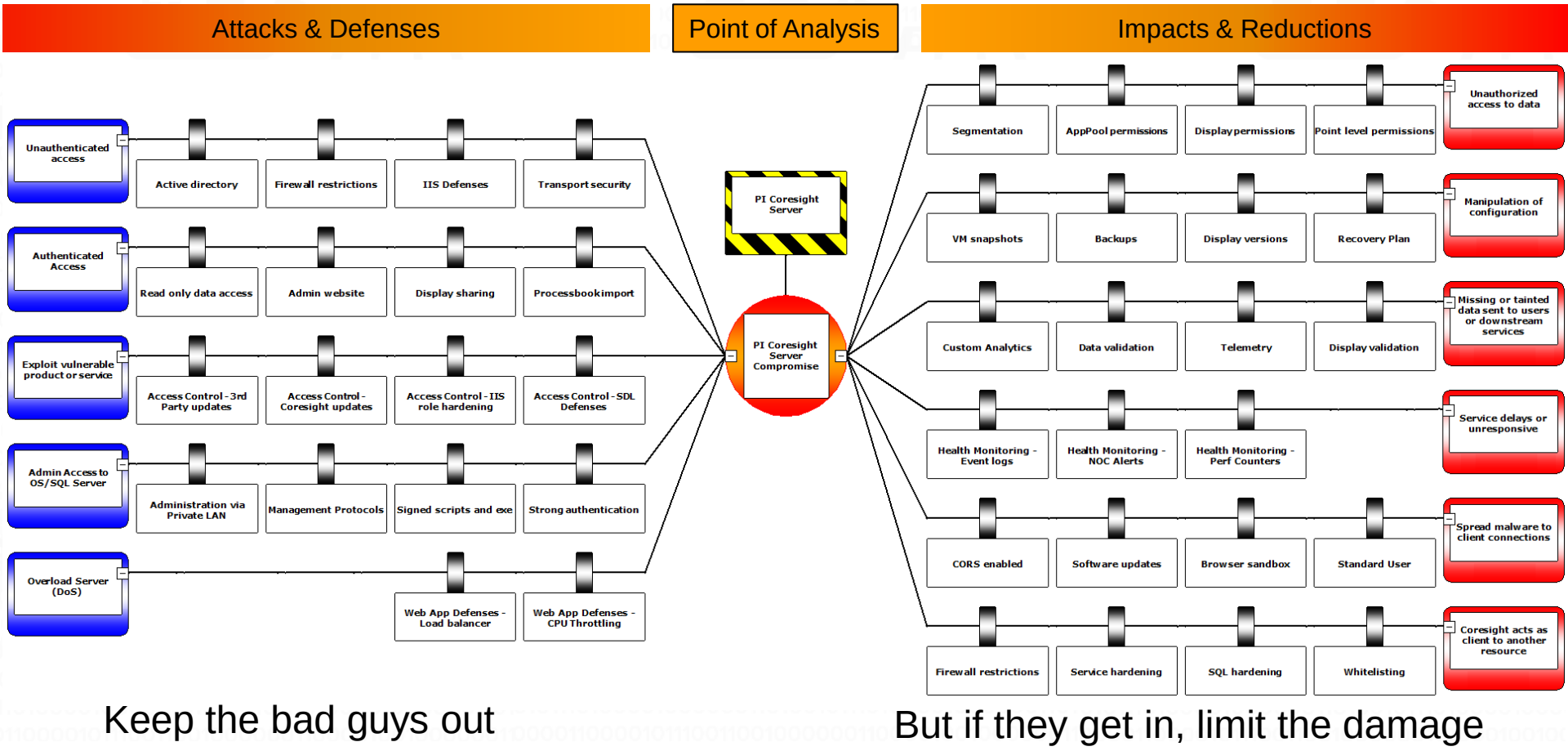


ICS Security Bow-Tie



Evaluating Cyber Risk in Engineering Environments:
A Proposed Framework and Methodology

https://www.sans.org/reading-room/whitepapers/ICS/evaluating-cyber-risk-engineering-environments-proposed-framework-methodology-37017



Keep the bad guys out

But if they get in, limit the damage