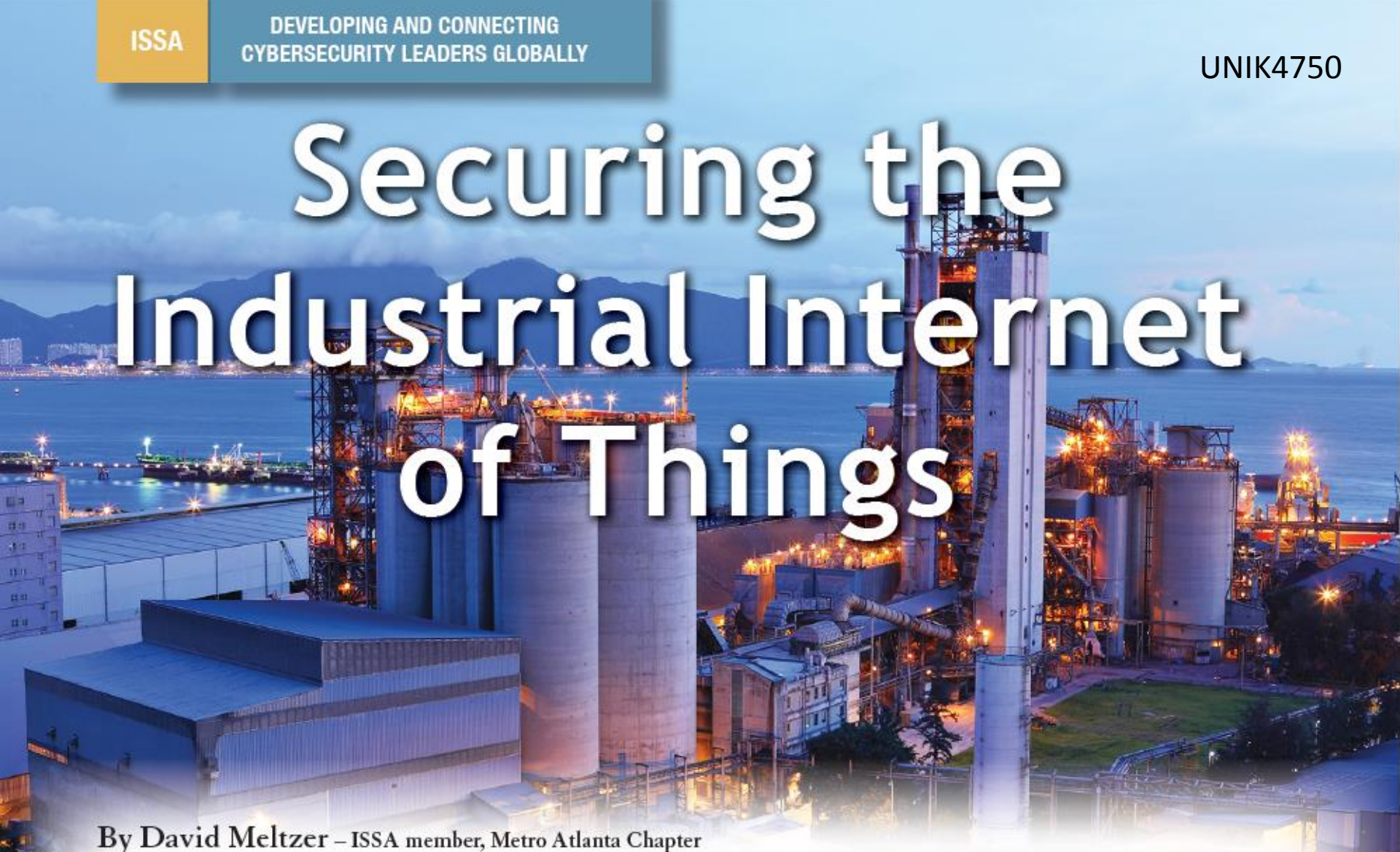
ISSA
DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

UNIK4750

# Securing the Industrial Internet of Things



By David Meltzer – ISSA member, Metro Atlanta Chapter

**This article discusses security aspects of the Industrial Internet of Things—the explosion of IP-connected devices used in such areas as control systems, manufacturing, utilities, and transportation.**

# Presentation overview

- Paper structure;
- Paper content;
- Evaluation of the paper;
- Review of the findings.

# Paper structure

- Abstract
- Introduction
- What are we trying to secure?
- What are the risks?
- What are the solutions?
- What are we headed?
- References

# Paper content: Introduction

Harvard Business Review

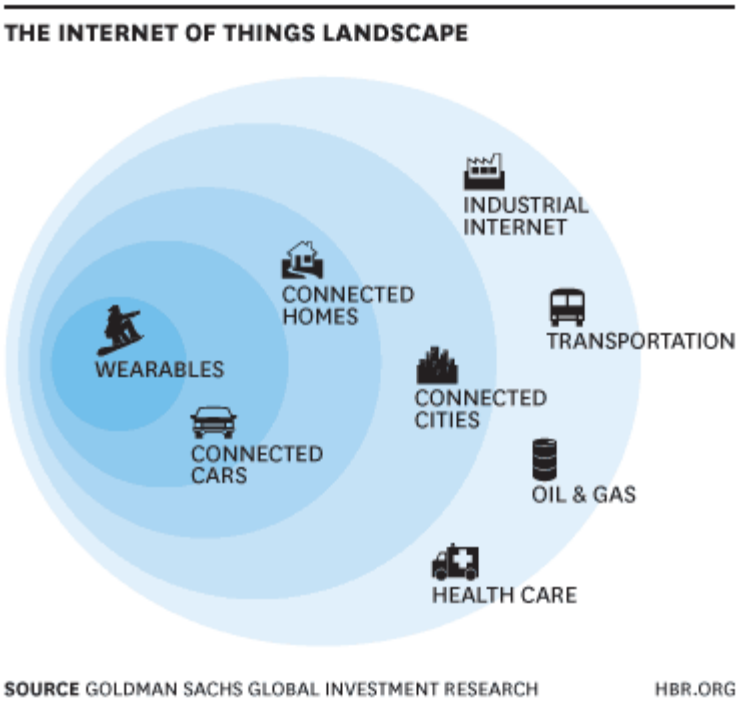
INTERNET

## The Sectors Where the Internet of Things Really Matters

by Simona Jankowski

OCTOBER 22, 2014

**$2 000 000 by 2020**




Within the vast Industrials sector, the IoT represents a structural change akin to the industrial revolution. Equipment is becoming more digitized and more connected, establishing networks between machines, humans, and the internet and creating new ecosystems. While we are still in the nascent stages of adoption, we believe the Industrial IoT opportunity could amount to $2 trillion by 2020. Included within this Industrial category are numerous sectors, from transportation to health care to oil and gas, each of which will be affected.

# Paper content: introduction

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Agenda

## Industrial Internet of Things: Unleashing the Potential of Connected Products and Services

### Risks and challenges

To realize the full potential of the Industrial Internet, businesses and governments will need to overcome a number of important hurdles. Chief among them are security and data privacy, which are already rising in importance given increased vulnerabilities to attacks, espionage and data breaches driven by increased connectivity and data sharing. Until recently, cybersecurity has focused on a limited number of end points. With the advent of the Industrial Internet, these measures will no longer be adequate as the physical and virtual worlds combine at a large scale. Organizations will need new security frameworks that span the entire cyber physical stack, from device-level authentication and application security, to system-wide assurance, resiliency and incidence response models.

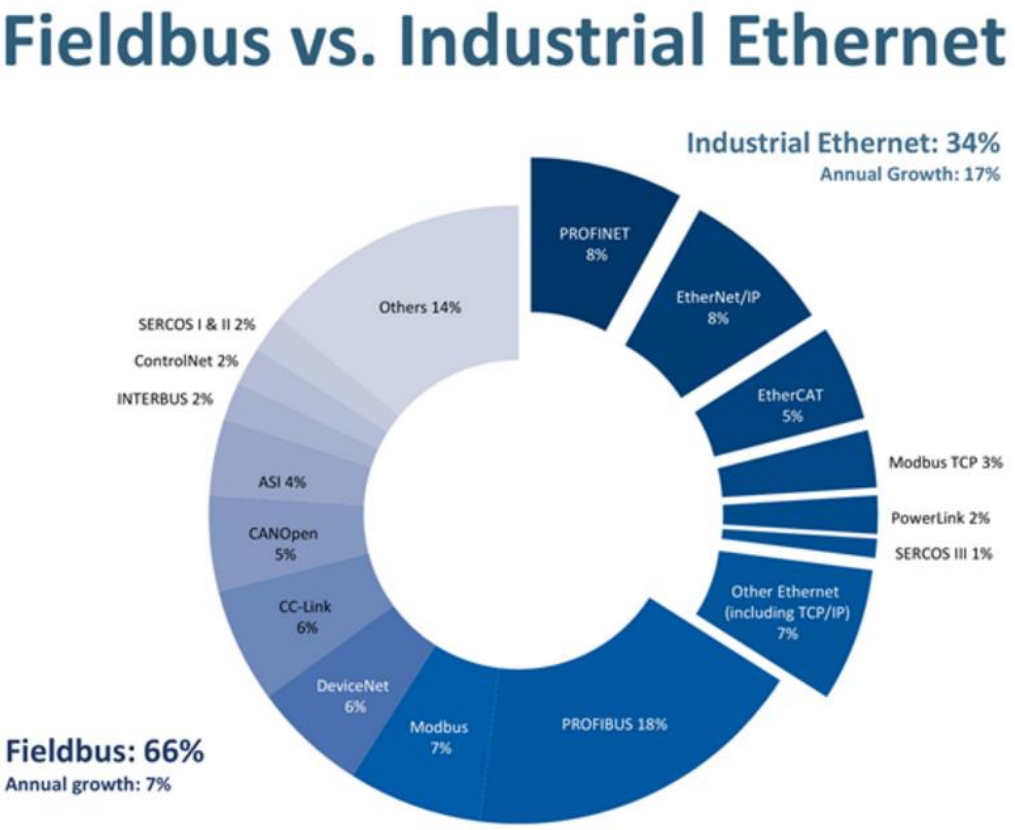
# Paper content: what to secure?

- **Industrial IoT:** the explosion of IP-connected devices used in industrial control systems, manufacturing, utilities and transportation.
- **Evolution:** from no network between components to the Ethernet
- **Layers of security concerns:**
  - Network layer;
  - System layer.

**Ethernet** is a link layer protocol in the TCP/IP stack, describing how networked devices can format data for transmission to other network devices on the same network segment, and how to put that data out on the network connection.

# Paper content: what to secure?

- Network layer of security: **protocols**
  - Modbus,
  - DPN3,
  - IEC 61850,
  - Ethernet/IP,
  - Profinet,
  - Proprietary protocols,
  - …

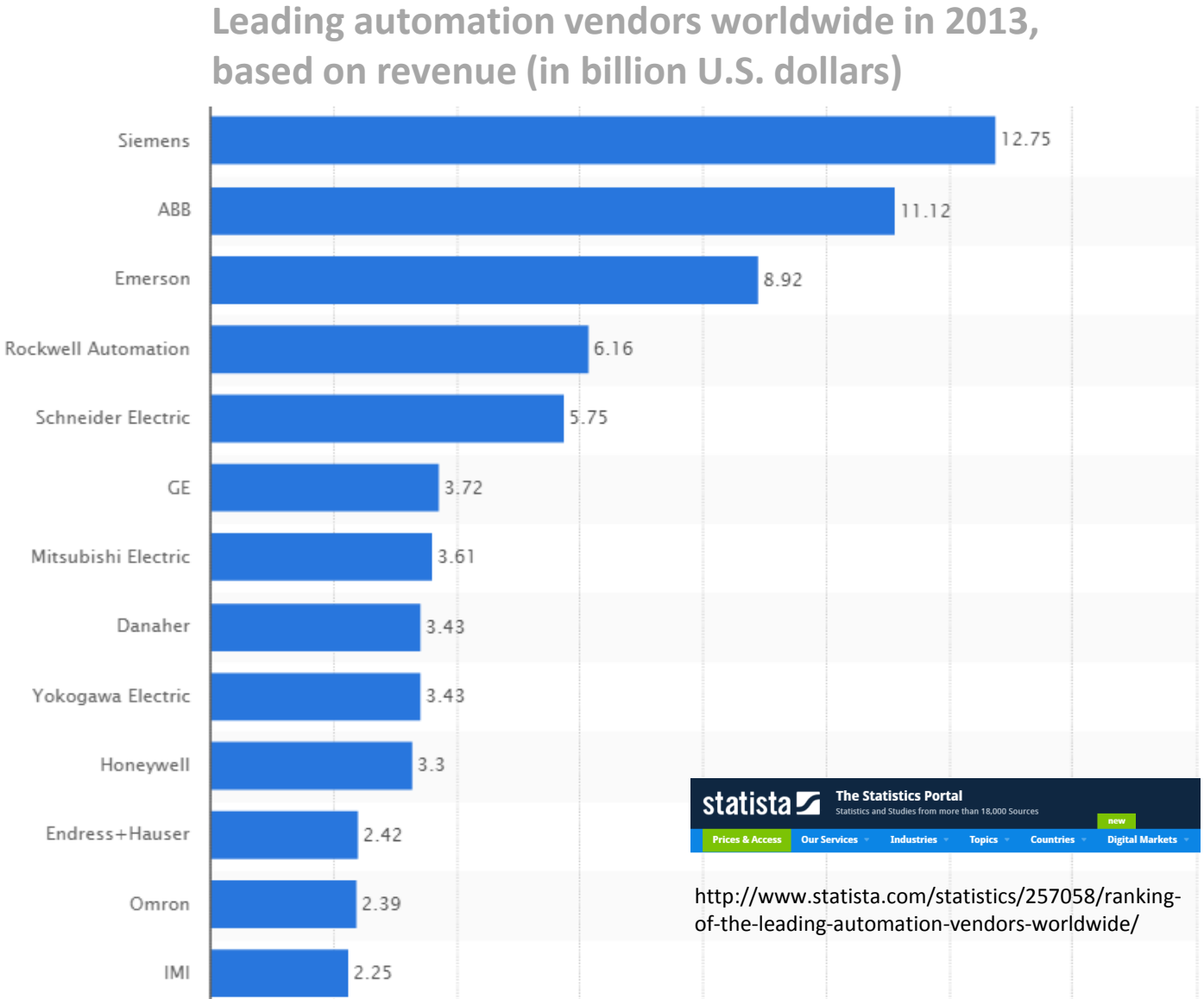



Source: HMS Industrial Networks
http://www.automationinside.com/2015_01_01_archive.html

# Paper content: what to secure?

- System layer of security: **vendors**

The vendors vary depending on industry sector and geography, but there are several leaders.

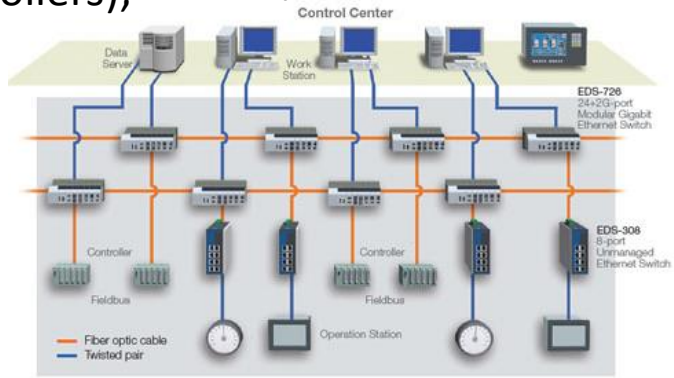



http://www.statista.com/statistics/257058/ranking-of-the-leading-automation-vendors-worldwide/

# Paper content: what to secure?

- Vendors produce millions of industrial **devices:**

PLCs (programmable logic controllers); DCSs (distributed control systems); Sensors;


- **Small fraction** of the devices needs software packages running on <u>standard</u> Windows and UNIX systems.
- **The majority** of devices are small, <u>embedded</u> systems running real-time operating system, communicating using the protocols, and being used for a very specific part of an operation process.
- One-way communication devises (data diodes).
- Remote access devices that work over cellular networks.
- Protocol translating gateways that can speak many of the industrial protocols.

# Paper content: risks

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

ICS-CERT MONITOR

The majority of incidents were categorized as having an "unknown" access vector. In these instances, the organization was confirmed to be compromised; however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network.

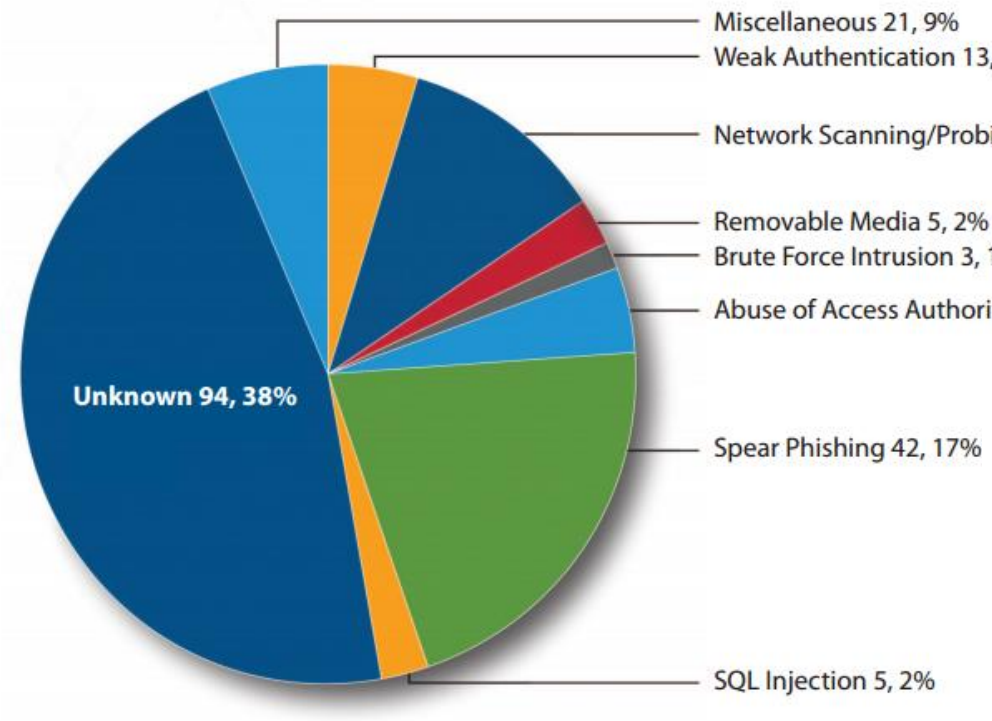



*Figure 2. FY 2014 incidents reported by access vector (245 total).*

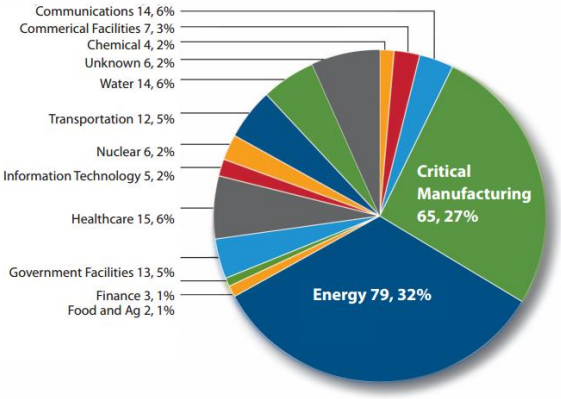
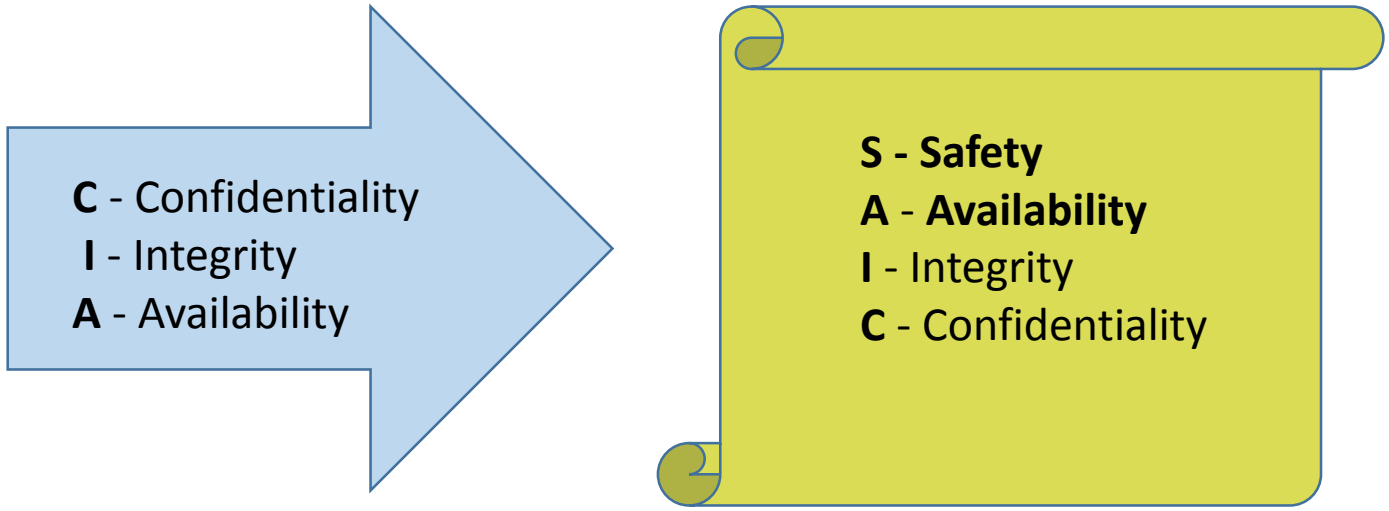



*Figure 1. FY 2014 incidents reported by sector (245 total).*

The 245 incidents are only what was reported to ICS-CERT, either by the asset owner or through relationships with trusted third-party agencies and researchers. Many more incidents occur in critical infrastructure that go unreported. ICS-CERT continues to encourage asset

# Paper content: risks

- One of the fundamental tenets if industrial security is to reprioritize:




- The risk that a sophisticated attack could take a human life is high.
- Extreme focus on availability.

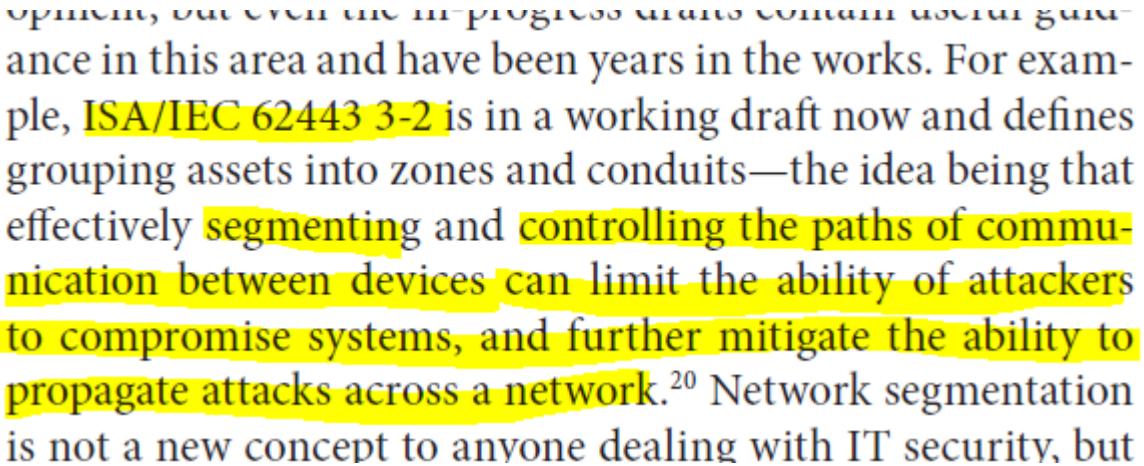
# Paper content: risks

- **Network perspective:**
  - **Vulnerable protocols:** Dozens vulnerabilities have been published against industrial protocols such as DNP3;
  - Lack of secure **design** of network architecture:
    - few network controls,
    - bad segmentation.
  - Industrial **specifics**:
    - highly customized environment,
    - Long life cycles,
    - Extreme focus on availability.
- **System perspective:**
  - Lack the **system controls** such as
    - Authentication, authorization, logging, change management.
  - Vendors have incorporated only the basic security controls into the industrial automaton solutions produced today.

# Paper content: solutions

Common standards for industrial environments:

- NIST SP800-82 R2, *Guide to Industrial Control Systems Security,* 247 pages
- ISA/IEC 62443 (formerly ISA99) - *Security for Industrial Automation and Control Systems*
  - *Example:*



opment, but even the in-progress drafts contain useful guidance in this area and have been years in the works. For example, ISA/IEC 62443 3-2 is in a working draft now and defines grouping assets into zones and conduits—the idea being that effectively segmenting and controlling the paths of communication between devices can limit the ability of attackers to compromise systems, and further mitigate the ability to propagate attacks across a network.[20] Network segmentation is not a new concept to anyone dealing with IT security, but

# Paper content: solutions

- Approaches:
  - Make a **new** deployment with appropriate network and system controllers. Not always possible.
  - Retrofit **existing** environment is difficult due to industrial specifics:
    - Availability is prioritized ->
      normal traffic should pass without delay ->
      any changes should be modeled and tested
      before they meet the production.
    - Need for re-examine traditional controls? ->
      scanning of the system ->
      could cause delays -> DoS -> not possible ->
      modelling.
    - Proprietary protocols? ->
      reverse engineering -> one small misunderstanding -> DoS

# Paper content: conclusions

- Messages for vendors:

There is still a need for new technologies to be developed in the realm of industrial security. Industrial devices need to be built with security requirements in mind. Although automation vendors have already made some progress in this area, much work remains to be done. Endpoint security also needs better technology solutions to effectively address industrial devices.

Security vendors and industrial automation vendors need to cooperate to leverage the existing data collection and analysis systems already in place for process management and expose a security interface to these systems, rather than be forced to choose from the alternative approaches I outlined in the previous section. For example, a security assessment tool could query the API of a supervisory system to gather in-

# Paper content: conclusions

- Messages for industry actors:

to fall under any such incidents. It is very easy for such attacks to be ignored, and with ineffective monitoring where little information about the attack could be gathered to begin with, what exactly has been learned to be shared anyhow? Although public disclosure is not necessarily a helpful solution here, improved sharing of threat intelligence amongst peers and in member organizations such as Information Sharing and Analysis Centers (ISAC) will help better inform our industry about these threats

Addressing security concerns and building more secure industrial environments will help drive and accelerate the growth of the industrial Internet of things. IT security professionals will play a large role in that, and incorporating industrial security into our world view will give all of us a more complete, holistic view of the threat landscape, helping us better evaluate the overall risks to organizations and create better solutions.

# Evaluation: Information about the paper

- **Article** was written for the ISSA Journal.
- **Short:** 6 pages.
- **Author:** chief research officer at Tripwire.
- **Target audience:** non-scientific readers interested in cybersecurity.
- **Message of the article:** to tell people how the things are in IIoT.



# About ISSA

## Developing and Connecting Cybersecurity Leaders Globally.

**ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.**


The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

**Join today.**

### Core Purpose

To promote a secure digital world.

### Mission Statement

ISSA is a nonprofit organization for the information security profession committed to promoting effective cyber security on a global basis.

a) Being a respected forum for networking and collaboration

b) Providing education and knowledge sharing at all career lifecycle stages

c) Being a highly regarded voice of information security that influences public opinion, government legislation, education and technology with objective expertise that supports sound decision-making"



### Sign In

Username

Password

Remember Me

Sign In

Forgot your password?

Haven't registered yet?

### Calendar

more

**3/10/2016 » 3/11/2016**
TECHSEC in Mining 2016

**3/10/2016**
March 2016 CISO Mentoring Webinar Series

**3/14/2016**
Women in Security SIG Monthly Webinar

**3/22/2016**
ISSA Web Conference: Mobile App Security (Angry Birds

# Tripwire Understands Your Needs When It Comes to Security

## CONTINUOUS SECURITY MONITORING

Continuous monitoring is critical to detect threats. We can help >

## NETWORK AND DATA SECURITY

Cyber actors want your valuable data. Protect it. We can help >

## CONFIGURE AND HARDEN YOUR SYSTEMS

Continuous system hardening to protect valuable IT assets.
We can help >

## VULNERABILITY AND RISK MANAGEMENT

Their goal is to find your gaps. Stop them. We can help >

## WEB APPLICATION SECURITY

Hackers can exploit your website and web apps. We can help >

## FILE INTEGRITY AND CHANGE MONITORING

Small changes have big consequences. Spot them fast.
We can help >

## CLOUD SECURITY

Enjoy the benefits of the cloud. Be secure. We can help >

## COMPLIANCE

So many regulations. So few resources. Stay safe.
We can help >

## INCIDENT DETECTION AND FORENSICS

When security is breached, every second counts. We can help >

## IT SECURITY OPERATIONS

Align security performance with business needs. We can help >

## THREAT INTELLIGENCE

Analyze and identify real threats and their impact. We can help >

## SECURITY INTELLIGENCE

Detect indicators of breach, compromise and vulnerability.
We can help >

## MANAGE AND ENFORCE

## INSIDER THREAT

## ENDPOINT DETECTION

# Evaluation: Categorization

- Simple language, generalization of facts;
- No particular goal for research;
- No particular industry or case was studied;
- No particular results achieved;

Conclusion: **non-scientific paper**.

- Interesting to read;
- Wide (not deep) overview;
- References to sources we can trust;
- Concise.

Conclusion: **good article**.