RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: SEC-F04

# 2015 Industrial Control System Vulnerability Trends


**Amol Sarwate**

Director of Vulnerability Labs
Qualys Inc.
@amolsarwate

RSAConference2015

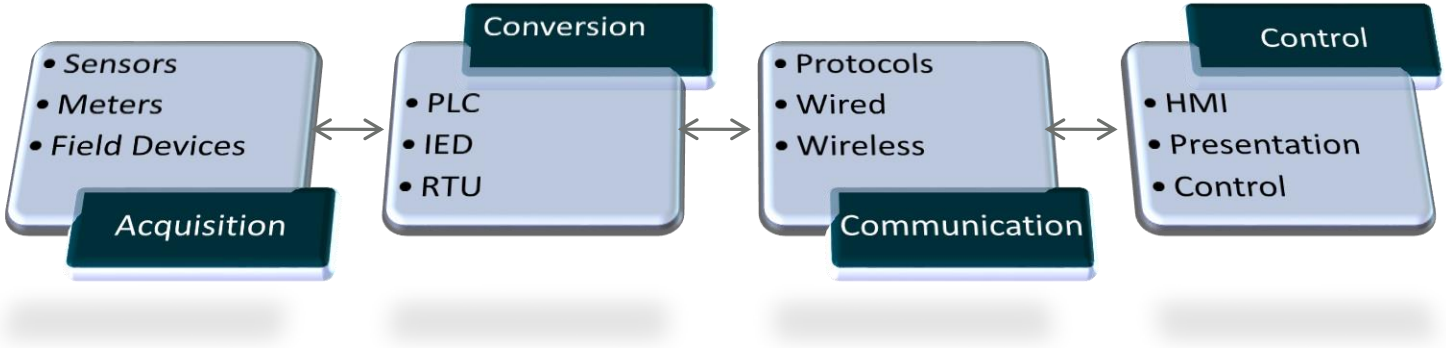
Singapore | 22-24 July | Marina Bay Sands

# Agenda

## ICS – Inside Out
## Vulnerability Analysis
## Recommendations

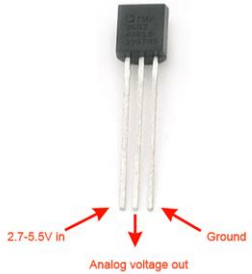
# Industrial Control Systems from Outside

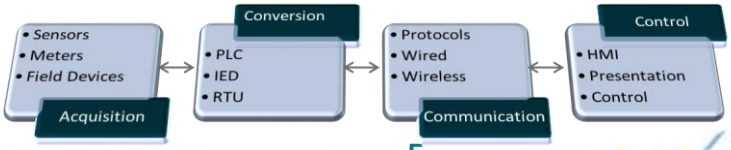
# Industrial Control Systems from Inside



# Data Acquisition

Convert parameters like light, temperature, pressure or flow to analog signals

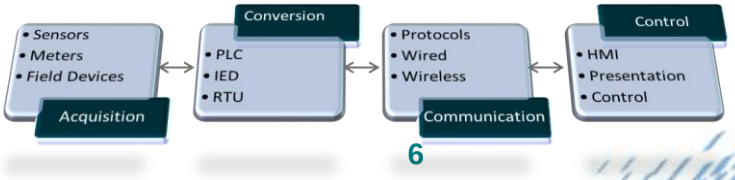


# Data Conversion

Converts analog and discrete measurements to digital information

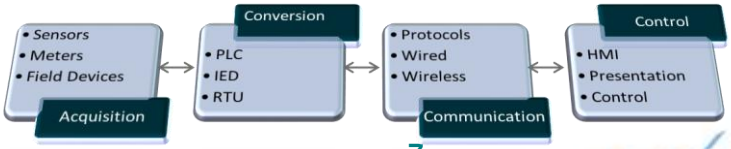


# Communication

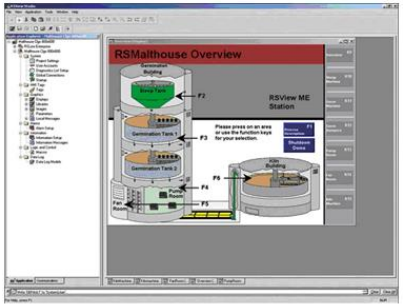


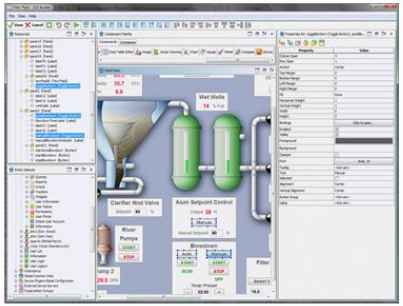
| Modbus | DNP 3 | OPC |
|---|---|---|
| ICCP | ControlNet | BBC 7200 |
| ANSI X3.28 | DCP 1 | Gedac 7020 |
| DeviceNet | DH+ | ProfiBus |
| Tejas | TRE | UCA |

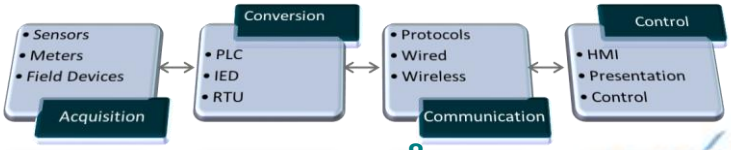


# Presentation and Control

Control, monitor and alarming using human machine interface (HMI)





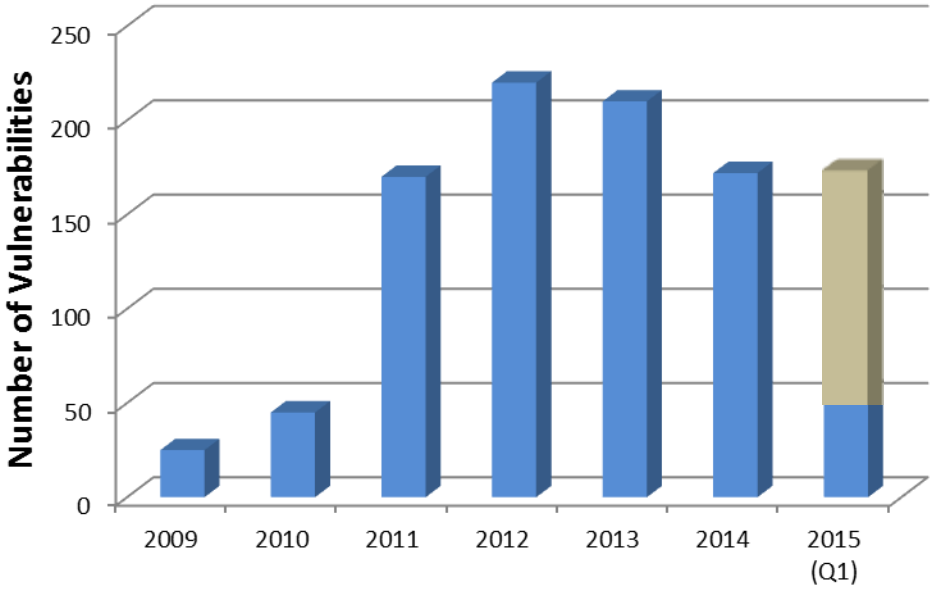
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

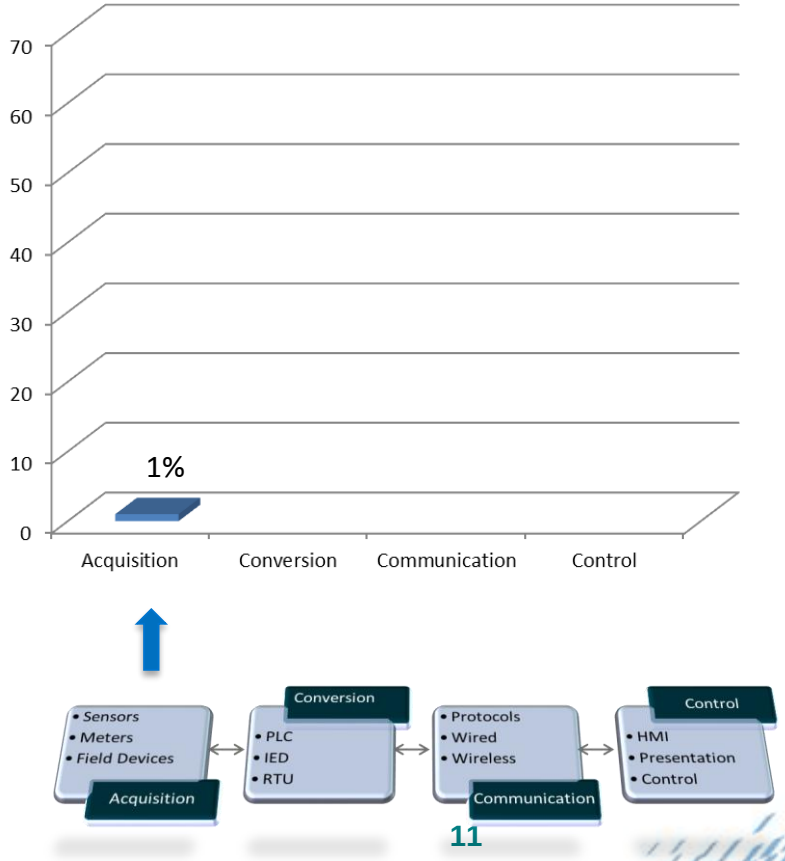
# Agenda

## ICS – Inside Out
## Vulnerability Analysis
## Recommendations

# 2009 - 2015 ICS Vulnerabilities

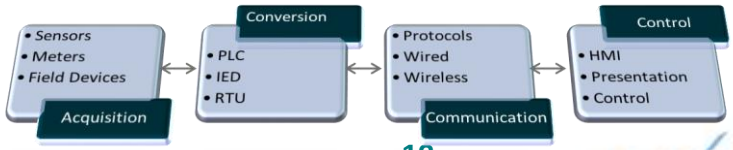


# 2014 - 2015 Data Acquisition Vulnerabilities

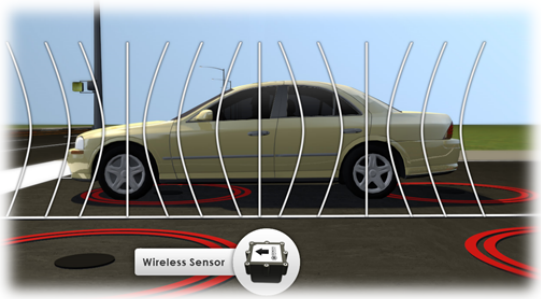


# 2014 and 2015 Data Acquisition Vulnerabilities

- Requires physical access
- Field equipment does not contain process information
- Eample: Information like valve 16 or breaker 9B

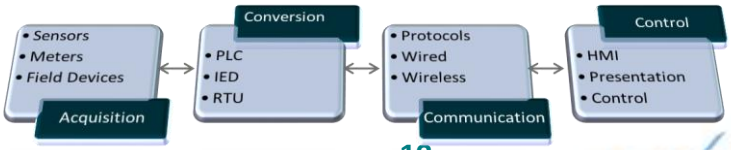


# Sensys Traffic Sensor Vulnerabilities

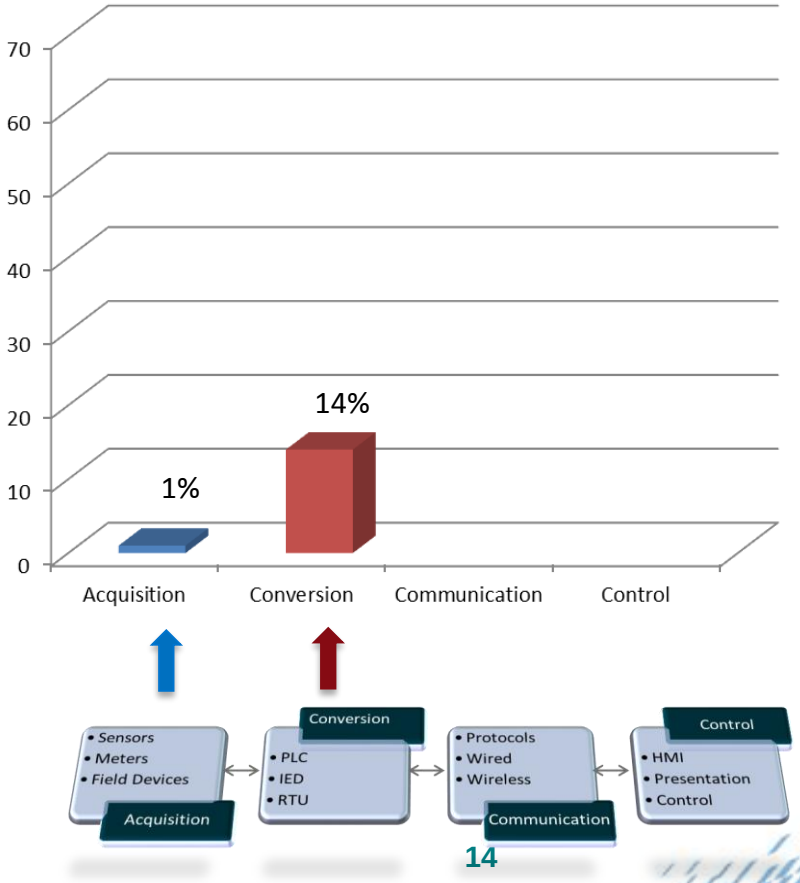



**Fix available from Sensys**

- CVE-2014-2378: Traffic sensors accept modifications without sufficient check
- CVE-2014-2379: Unencrypted wireless traffic between a traffic sensor and an access point could be intercepted and replayed.
- Access: AV:A, AC:H, Au:N
- Impact: C:C, I:C, A:P, C:P, I:P, A:P

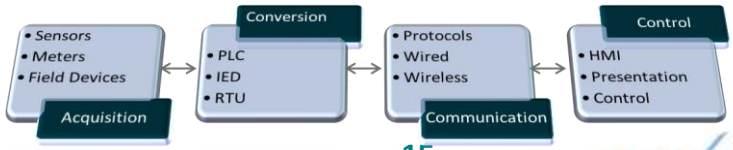


# 2014 - 2015 Data Conversion Vulnerabilities



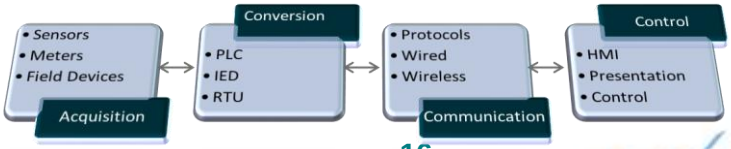
# Festo CECX-X-(C1/M1) Controller Vulnerabilities

- CVE-2014-0769: Two unauthenticated ports (Port 4000/TCP debug service port and Port 4001/TCP log service port) could allow attacker to change configuration and remove log
- CVE-2014-0760: FTP backdoor
- Access: AV:N, AC:M, Au:N
- Impact: C:C, I:C, A:C
- Exploit code available

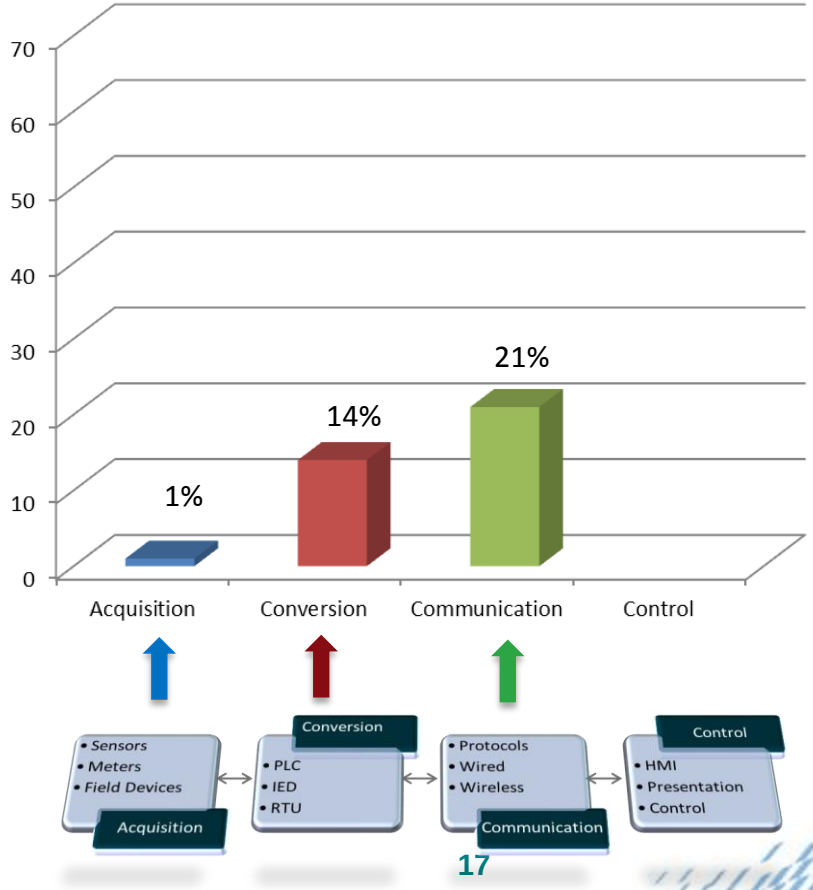


# OleumTech WIO Family Vulnerabilities


- CVE-2014-2361: Key Management Error – Possible to steal site security key when connecting to BreeZ (AV:L)
- CVE-2014-236: Cryptographically weak pseudo-random number generator
- CVE-2014-2360: Radio receiver crashes on receiving a specially crafted packet.
- Access: AV:(N/L), AC:L, Au:N
- Impact: C:C, I:C, A:C



# 2014 - 2015 Communication Vulnerabilities



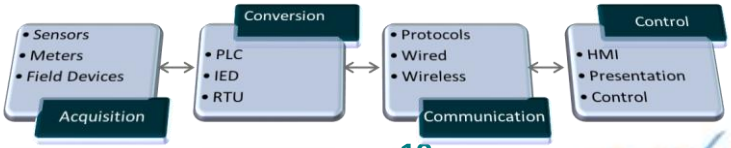
# 2014 - 2015 DNP Vulnerabilities

- CVE-2014-5410: Rockwell Micrologix 1400 DNP3 DoS Vulnerability
- CVE-2014-0761: CG Automation (ePAQ-9410) Improper Input Validation Vulnerability
- CVE-2014-2342: Triangle MicroWorks Uncontrolled Resource Consumption
- CVE-2013-6143: Schneider Electric Telvent SAGE RTU DNP3 Improper Input Validation

Rockwell Micrologix 1400

Schneider Electric
Telvent SAGE

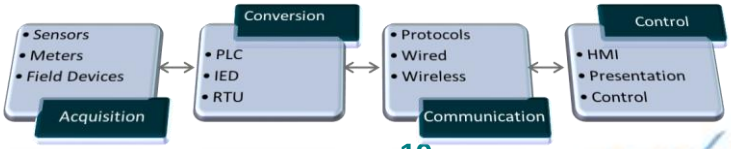

CG automation ePAQ-9410



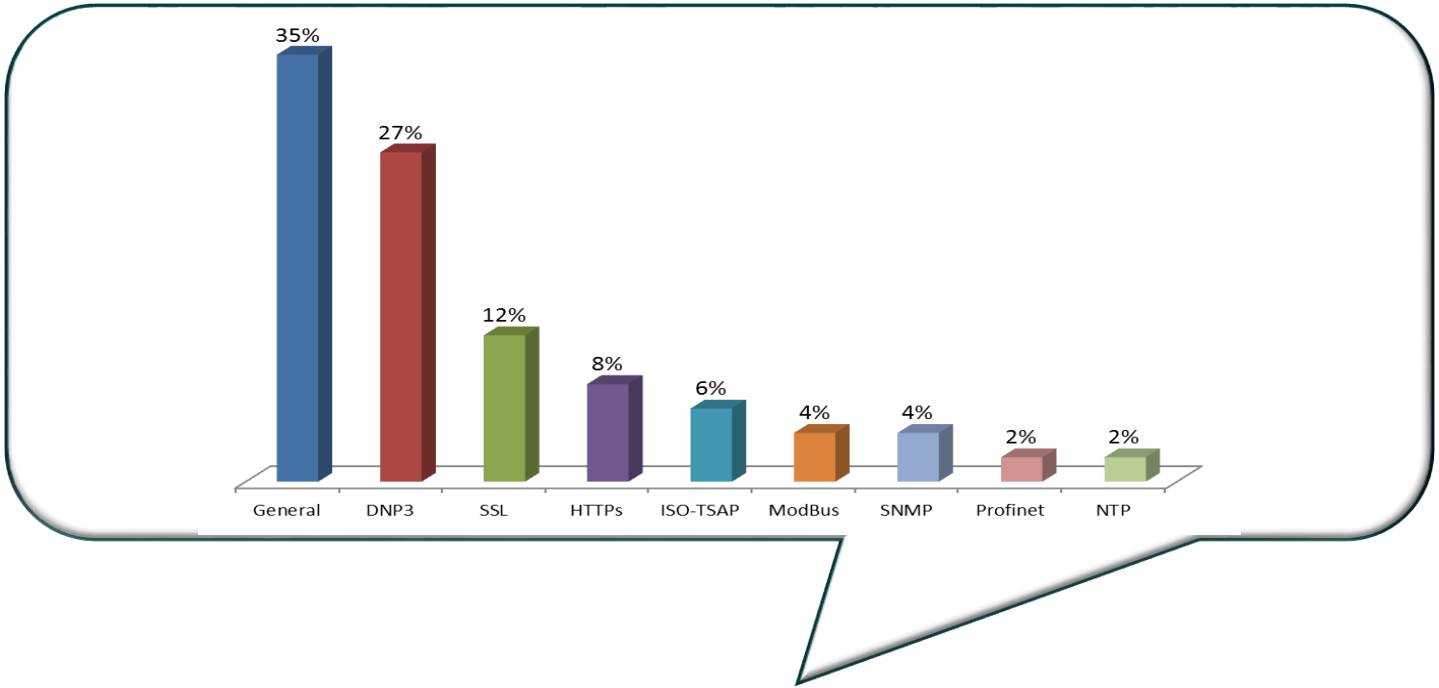
# 2014 - 2015 SSL Vulnerabilities

- CVE-2014-0224: Siemens OpenSSL MitM attack in ROX, APE, S7-1500, CP1543-1
- CVE-2014-0160: ABB Relion 650 Series OpenSSL Vulnerability (FTPS)
- CVE-2014-0198: Siemens S7-1500 OpenSSL WebServer DoS
- CVE-2014-3470: Siemens WinCC OpenSSL DoS

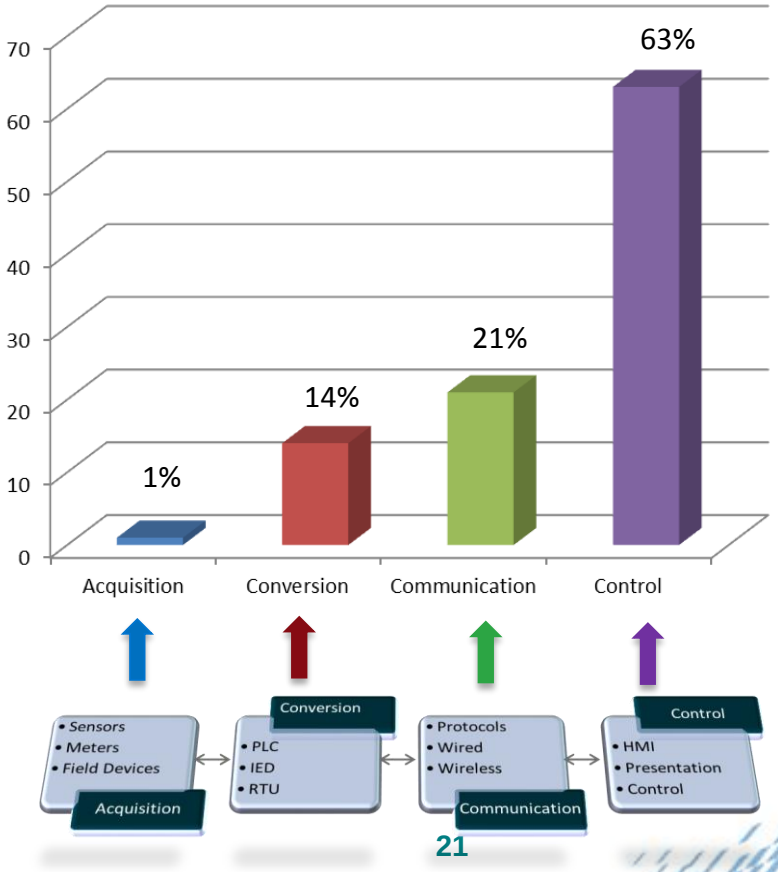
ABB Relion 650 Series



# 2014 - 2015 Communication Vulnerabilities

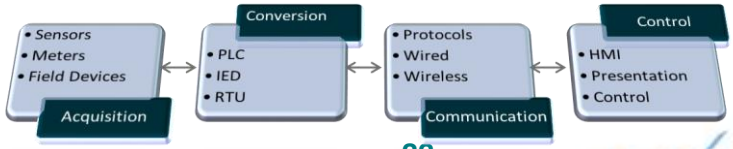


# 2014-2015 Presentation & Control Vulnerabilities

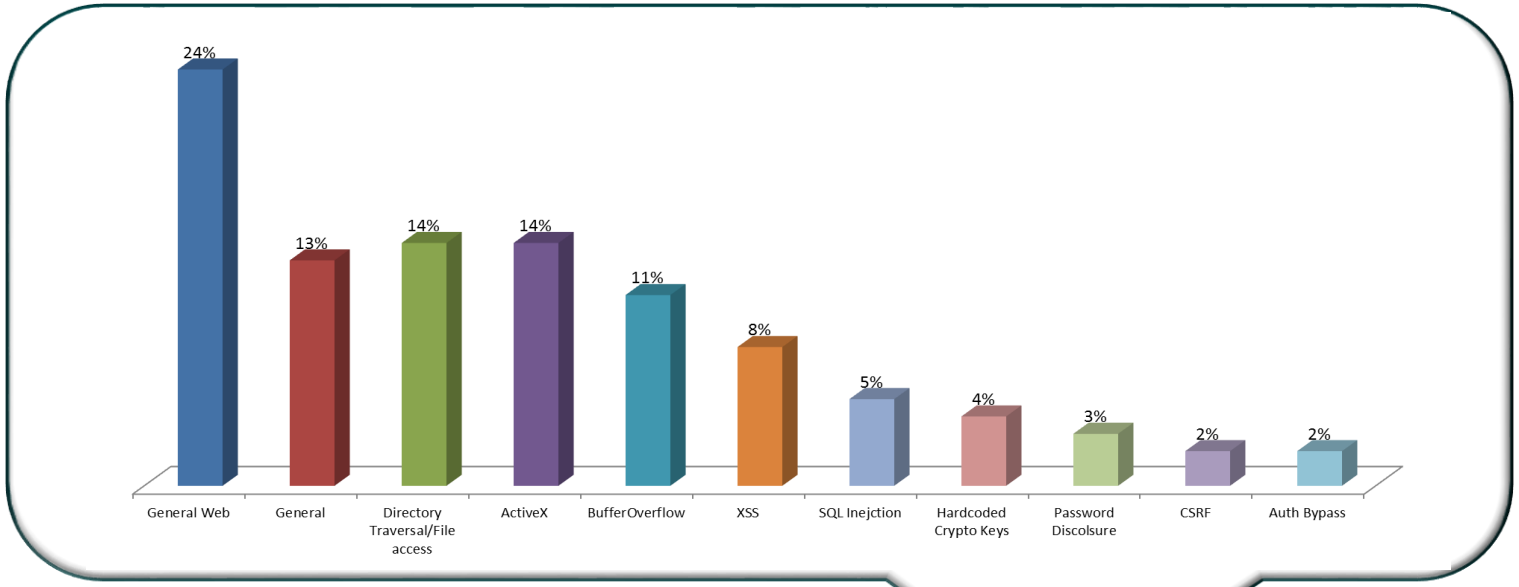


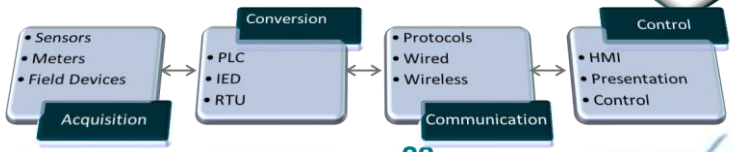
# 2014-2015 Presentation & Control Vulnerabilities

- CVE-2014-5436: Honeywell Experion PKS *Directory Traversal*
- CVE-2014-8388: Advantech WebAccess Stack-based *Buffer Overflow*
- CVE-2014-5417: Meinberg Radio Clocks LANTIME M-Series *XSS*
- CVE-2014-2374: Accuenergy Acuvim II *Password Disclosure*
- CVE-2014-2358: Fox DataDiode Proxy Server *CSRF* Vulnerability
- CVE-2014-2376: Ecava Integraxor SCADA Server *SQL* Injection
- CVE-2014-2353: Cogent DataHub *XSS* Vulnerabilities
- CVE-2014-0771: Advantech WebAccess Multiple *ActiveX* Vulnerabilities
- CVE-2014-0753: Ecava IntegraXor *DLL Injection* and Overflow Vulnerability
- CVE-2014-0751: GE Proficy *Path Traversal* Vulnerability



# 2014-2015 Presentation & Control Vulnerabilities



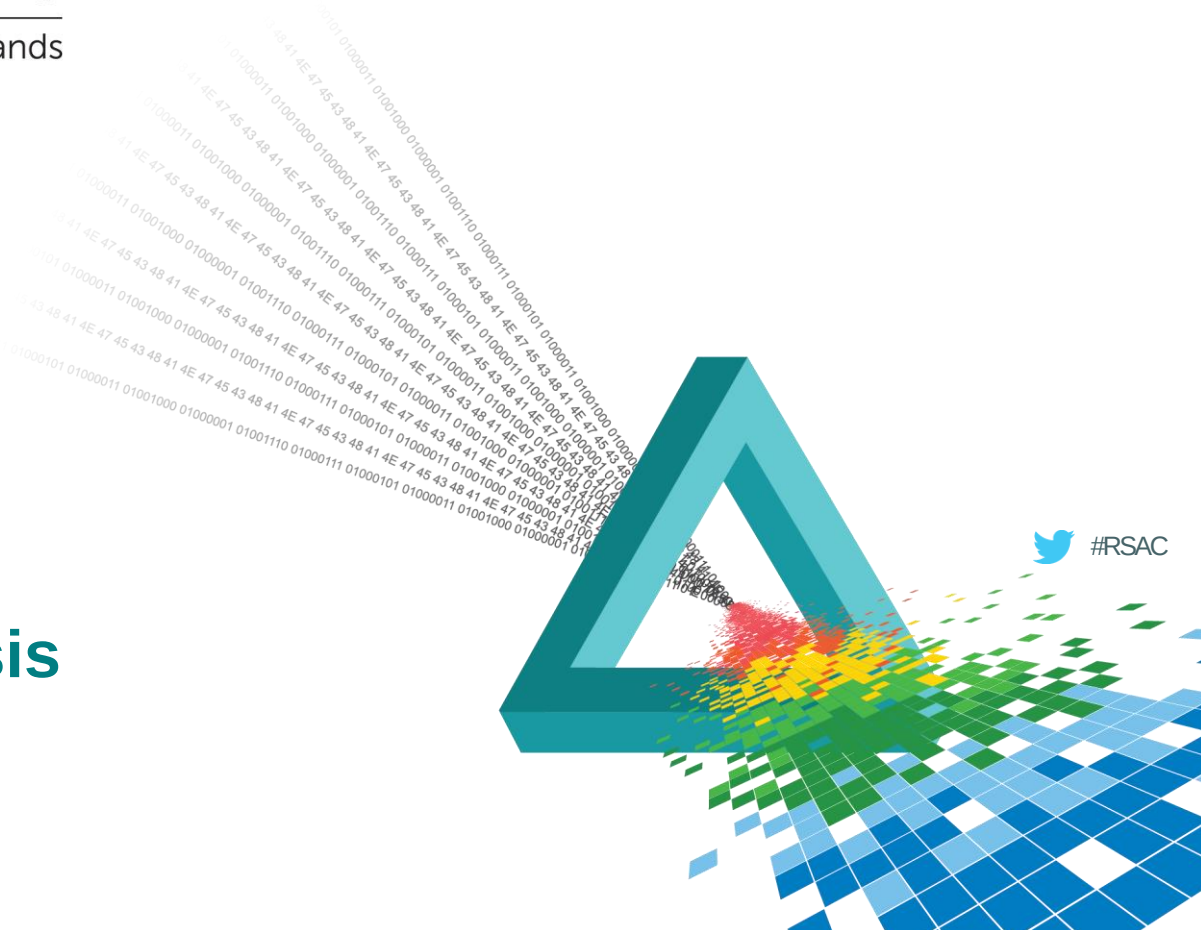

QUALYS® CONTINUOUS SECURITY

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

# Agenda

## ICS – Inside Out
## Vulnerability Analysis
## Recommendations



# Challenges and Recommendations

## Control system exposed to the Internet

Recommendation

- Next Week:
  - Check if you system is accessible from other parts of the corporate network or the Internet!
- Next Month:
  - Create a network architecture diagram
  - Check if existing architecture diagram is up-to-date and reflects reality
  - Policy for Remote Connectivity
- Next Quarter:
  - Network Segmentation, Firewalls and DMZs

# Challenges and Recommendations

**Risk from *off-the-shelf* software** **(operating systems, databases, web servers, browsers and others)**

Recommendation

- Next Week:
  - Subscribe to vulnerability feeds like ICS-CERT
- Next Month:
  - Create an inventory of *off-the-shelf* system components
  - Request a list of third party components from your vendor
- Ongoing:
  - Apply experience from IT network security

# Challenges and Recommendations

## Patching, Passwords and Configuration

Recommendation

- Next Week:
  - Demand quick patches from ICS vendor
  - Familiarize yourself with reboot procedures and test them if possible
- Next Month:
  - Formulate strategy for updates and patches
  - Enable authentication and authorization per user
- Next Quarter/Year:
  - Budget a small lab for patch testing. Use factory floor maintenance window

# Challenges and Recommendations

**Older ICS Protocols built for performance (not security)**

Recommendation

- Next Week:
  - Create inventory of all ICS protocols used in your system
- Next Month/Quarter:
  - Enable newer versions as many protocols now support built in security
  - Policy for modernization and upgrades
  - Secure wireless connections

# Recommendations

Ongoing:

- Security Training for Engineers, Technicians, Administrators, and Operators
- Conduct  Vulnerability and Risk Assessments
- Complying with Security Standards for your industry

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

# Thank You

**@amolsarwate**