The Safety of Security

Steve Powroznyk - UL Senior Cybersecurity Advisor

Introduction

- Technology Professional for the past +25 years
  - Focus has been large global financials, Technology Resellers (VAR) & Startup security companies
- Enterprise SME
  - Server, Storage, Data Center & Cybersecurity
- Senior leadership
  - Program, Project, Staff & Vendor Management on a global scale

Why UL

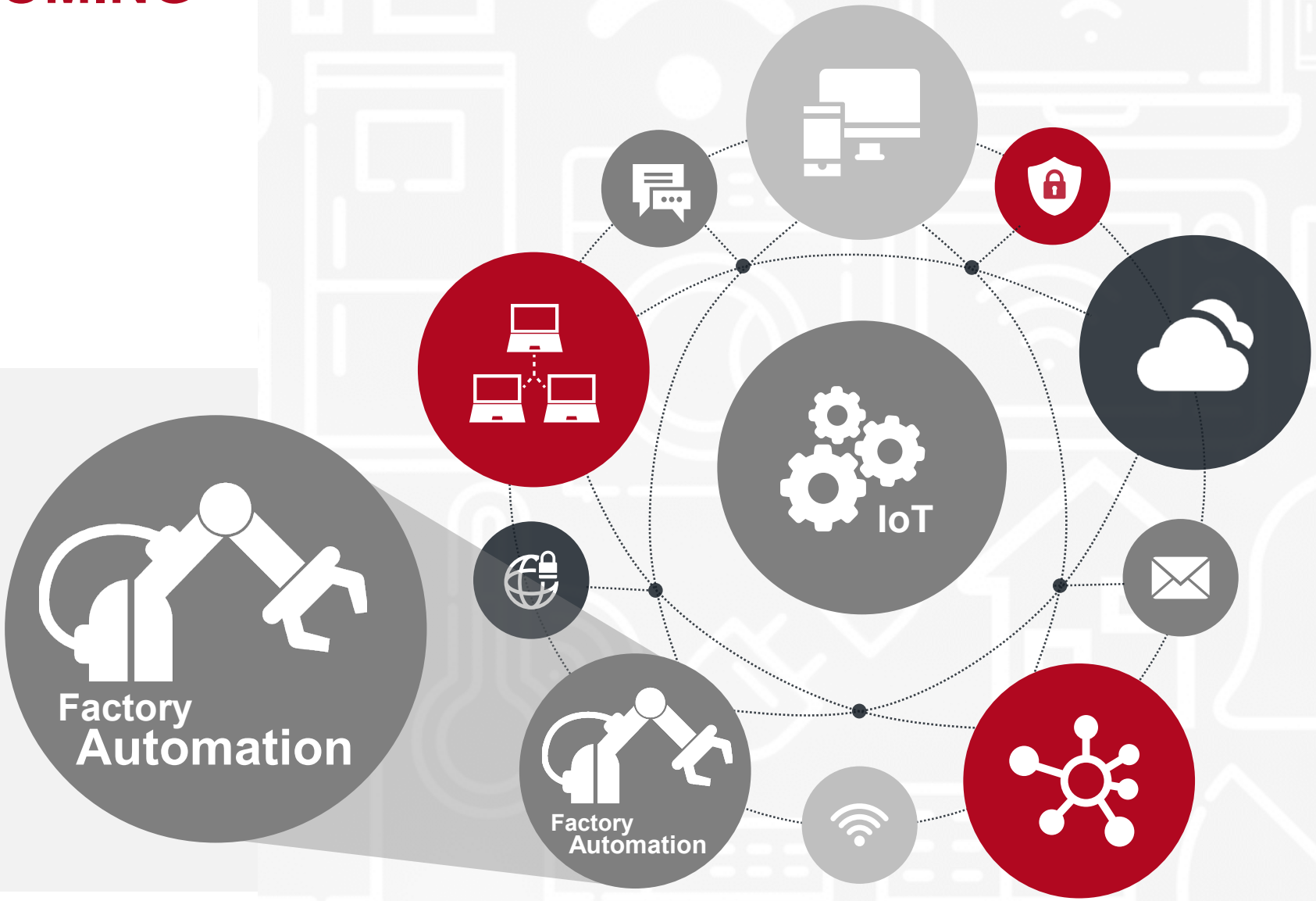
- Since 1894 UL has worked hard to make the world a safer place
- Security is a logical extension of safety
- IoT is a new threat, with new vulnerabilities to creating risk
- Focused in Industrial Control Systems (ICS)
- Interconnected Technologies are growing fast

THE WORLD IS BECOMING MORE CONNECTED

30 BILLION

Connected “things” to be in use by 2020

(Source: Gartner, Inc.)



SECURITY IS NOT PROMISED WITH IOT

83% of companies think

CYBERATTACKS ARE ONE OF THE 3 BIGGEST THREATS

to their organization

(ISACA, 2015, Global Cybersecurity Status Report)

>118,000

KNOWN PUBLIC VULNERABILITIES

(NIST NVD 1/24/19)

CRITICAL INFRASTUCTURE WEAKNESSES

FY 2017 Most Prevalent Weaknesses		
Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: • Maliciously modify, delete, or copy device programs and firmware • Access the ICS network • Steal or vandalize cyber assets • Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors of malicious party access to critical systems • Rogue internal access established

Source: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf

Why Care

- Business Risk
- Brand Value & Impact
- Regulation
  - To date 35 States have considered or introduced 265 bills on Cybersecurity
  - California SB-327: *"Beginning January 1 2020 California requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device."*

Typical Customer Engagements - Use Case #1

- Customer is thinking about IoT
- Early stages of gathering functional requirements
- Development has not started yet

How UL can assist:

- General Education – Help the client understand the security landscape
- Training - SDLC best practices

Typical Customer Engagements – Use Case #2

- Pre-Production of system development
- Finalizing IoT capabilities
- Alpha or Beta

How UL can assist:

- General Education – Help the client understand the security landscape
- Training - SDLC best practices
- Custom Workshop – Specific to the product

Typical Customer Engagements – Use Case #3

- Production system in the field
- Customers have concerns about security
- A breach has taken place

How UL can assist:

- Custom Workshop – Known vulnerabilities specific to the product
- Testing services – penn, fuzz, code analysis, remote management etc..

Typical Customer Engagements – Use Case #4

- Corporate IT Security focused
- External assessment of vulnerabilities
- Data security risk assessment

How UL can assist:

- Training – IT Security best practices, program creation & execution
- Formal ISO27001 Risk Assessment or specific Identity & Access Management engagement
- Testing services – penn, fuzz, code analysis, cryptographic, cloud etc..

UL Cybersecurity Solution

YOUR NETWORK CONNECTABLE PRODUCT AND/OR SYSTEM

Submit product or system for discrete testing (One or more individual tests)

Submit product or system for certification testing (All tests)

Cybersecurity Solutions

TESTING SERVICES

- Fuzz Testing
- Known Vulnerabilities
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates
- Structured Penetration Testing

TRAINING SERVICES

ADVISORY SERVICES

REVIEW SERVICES

YOUR REPORT AND/OR CERTIFICATION

Test Report

Certificate

KEY TAKEAWAYS: ✔ RISK MITIGATION ✔ INNOVATION ✔ COMPETITIVE ADVANTAGE

WHY UL CYBERSECURITY?

- Independent Trusted 3rd Party
- Cybersecurity Expertise
- Full Lifecycle Solutions
- Industry Knowledge
- Standards-Based CAP Program
- Cybersecurity and Safety
- Certification to Standards

CYBERSECURITY FOUNDATION

UL 2900 Series of Standards	IEC 62443 Family of Standards	Over 160 Cybersecurity Tools	Extensive Knowledge of Best Practices

Questions

Steve Powroznyk

steve.powroznyk@ul.com

847.664.6600

PEG PROTECTION ENGINEERS GROUP