CYBERSECURITY PERSPECTIVES

Insights and on-demand education from trusted experts

Cybersecurity education for a connected world

Featured and on-demand programming

Trust is essential.

Imagine the possibilities when intelligent power is fully integrated into homes, buildings, machines and vehicles. Now, imagine the consequences if we reach this level of connectivity without making cybersecurity the number one priority.

A world dependent on connectivity and electrification needs trusted environments. To advance cybersecurity, we're bringing together experts from around the world to weigh in on what strategies are working, what can be done better and what will be required to support a more secure tomorrow.

Cybersecurity Perspectives is a global forum and educational program designed to help advance internet security by combining best practices and direct experiences with leading-edge research and development. Gain insights from our experts, partners and customers on how you can better manage risk to support a more cybersecure future.

Featured keynote speaker

Be sure to join our keynote address at 9:00 a.m. ET on October 26, 2021 followed by two panel discussions.

Craig Gob
Vice President / General Manager
Electrical Engineering Services and Systems Division
Energy Solutions and Services Group, Electrical Sector

EATON Powering Business Worldwide

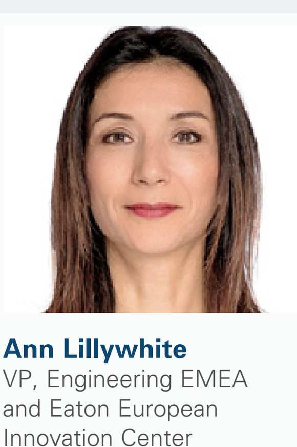
EXPERT-LED PANEL DISCUSSIONS

Explore security trends and the strategies you can implement right now to manage cybersecurity risk and support a more cybersecure future.

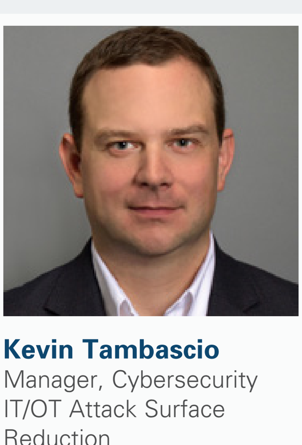
PANEL 1:
The state of cybersecurity in critical infrastructure

As IT and OT converge, there are more interconnections between increasingly distributed networks. A comprehensive understanding of the critical functions, assets, networks and maintenance practices that are critical is key to fully understand potential risks.

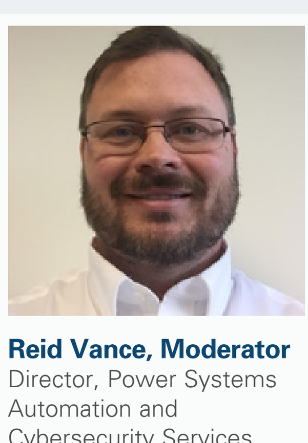
Full lifecycle cybersecurity consideration of how people, process and technology are applied to sustain operations is critical. This session will discuss the state of cybersecurity in critical infrastructure from the asset owner, OEM and OT/ICS solution vendor perspective.



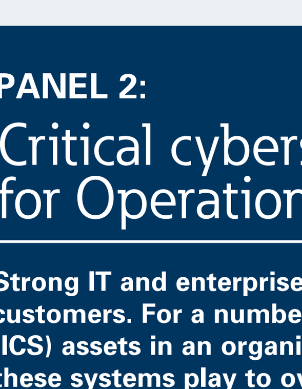
Marty Edwards
Vice President, Operational Technology Security
tenable



Yao Yang Low
Director of Cybersecurity
UL



Jason Christman
VP, Chief Product Security Officer
Johnson Controls



Ann Lillywhite
VP, Engineering EMEA and Eaton European Innovation Center
EATON Powering Business Worldwide

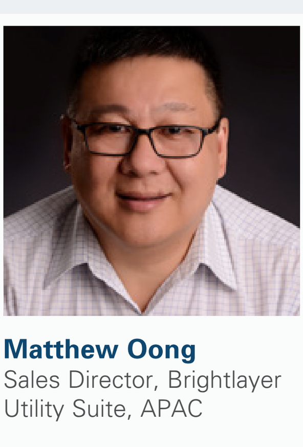
Kevin Tambascio
Manager, Cybersecurity IT/OT Attack Surface Reduction
Cleveland Clinic

Reid Vance, Moderator
Director, Power Systems Automation and Cybersecurity Services
EATON Powering Business Worldwide

PANEL 2:
Critical cybersecurity insights and solutions for Operational Technology (OT)

Strong IT and enterprise cybersecurity programs are crucial to protect businesses, employees and customers. For a number of reasons, the Operational Technology (OT) and Industrial Control System (ICS) assets in an organization are often not fully considered in these programs. The critical role these systems play to overall operations, their complexity, and safety make it difficult to address cybersecurity risks with IT focused technologies and techniques.

Effective OT and ICS cybersecurity services provides many benefits beyond just responding to a "hack" of a system. There are multiple benefits to these services by reducing direct cybersecurity risks, understanding how these systems are coupled to IT networks and improving overall lifecycle maintenance of the system. When delivered with a fundamental understanding of the assets and critical functions involved, these services provide many benefits not only in directly addressing cybersecurity risks, but also in reducing lifecycle maintenance, improving availability and resilience and ensuring the benefits and insights of digitalization that are securely realized.

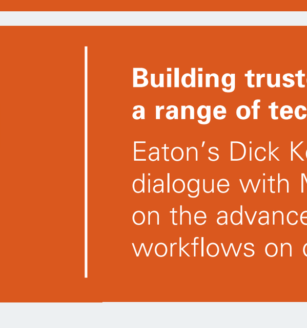


Kevin Chung
Program Manager, North America Utilities / Marketing

Eric Rueda
Business Development Manager, EMEA

Vinod Makam
Sales and marketing manager, Power Systems Automation

Matthew Oong
Sales Director, Brightlayer Utility Suite, APAC



Anthony Ciccozzi
Moderator
Cybersecurity Specialist

EATON Powering Business Worldwide

Access all of our on-demand programming at any time

Protecting IIoT and Endpoint Security

Building trusted, resilient IIoT endpoints requires a range of technologies working in harmony.

Eaton's Dick Kerr and Luiz Huet de Bacellar spearhead a dialogue with Microsoft, Payatu and Synopsys experts on the advanced technologies slated to safeguard workflows on connected networks.

Microsoft — **Joe DiPietro**, Director, Technical Sales

EATON — **Luiz Huet de Bacellar**, Director, Advanced Technologies

Synopsys — **Michael Fabian**, Principal Consultant

EATON — **Dick Kerr**, Vice President and Chief Information Security Officer

Payatu — **Aseem Jakhar**, Co-Founder/Director, Research

Global Cybersecurity Standards

Many countries develop requirements without regard to global conformity.

Eaton's Kevin Lippert and cybersecurity director, Max Wandera, head an informative discussion with UL, IEC and ISAGCA thought leaders on the importance of validating connected products with global standards through international partnership.

UL — **Isabelle Noblanc**, Vice President and General Manager Identity Management and Security

EATON — **Max Wandera**, Director, Product Cybersecurity Center of Excellence

IEC IECEE — **Wolfran Zeitz**, Executive Secretary

EATON, IEC — **Kevin Lippert**, Manager Codes and Standards, Eaton; President, USNC of IEC

ISA — **Andre Ristaino**, Managing Director Global Alliances and Consortia

Cybersecurity in business, applications and markets

Examine how to integrate cybersecurity into existing production and maintenance routines.

Review our sessions:

ENGINEERING RCEP REGISTERED CONTINUING EDUCATION PROGRAM

Attend online classes, complete with professional development hours (PDH) from Registered Continuing Education Program (RCEP) for select technical training.

Note: courses with this logo are eligible for PDH

Securing critical operations: decoupling IT from OT

Designed to help managers of large facilities and critical infrastructures, this session will review ways to reduce risk to your critical operations with industrial network defense techniques. We'll focus on methods and solutions to minimize the impact of IT facing incidents (e.g. Ransomware) to Operational Technology (OT) and Industrial Control System (ICS) networks, limiting your attack surface, securing remote access and lifecycle maintenances practices that enable resilience. A case study will demonstrate the importance of how a cross-functional team of power management and ICS/OT cybersecurity engineers was able to assess a system for risks and address them with targeted solutions.

Securing healthcare infrastructures — devices and systems

A smarter, more automated, and more connected Healthcare infrastructure enables advanced care for patients, increases overall operational efficiencies, and lowers lifecycle maintenance costs through prognostic and predictive maintenance. However, securing this modern Healthcare infrastructure requires a comprehensive understanding of the data protection, safety, and availability requirements and the threats they face.

In partnership with UL, this course is valuable for anyone responsible for designing, maintaining and securing smarter, more automated healthcare infrastructures to protect crucial data, OT networks and life-saving medical devices from compromise.

Securing critical infrastructure networks

Securing critical infrastructure networks Critical infrastructure networks are attractive targets for malicious actors that can cause service disruptions, harm to public safety, financial impact or penetration of a broader network housing valuable information. These networks are often readily exploitable due to some basic cybersecurity design or maintenance gaps. Learn about best practices for critical infrastructure networks that can be applied throughout the system lifecycle, including design, component selection and maintenance. The session provides guidance applicable to a variety of legacy, new and future critical infrastructure networks.

Protect intelligent connected devices with cyber secure remote monitoring

In many segments intelligent connected devices control much of the world's critical infrastructure and they can also expose industries and consumers to cyber threats. According to Gartner, nearly 20% of organizations have observed at least one IoT-based attack in the past three years. In the IT and OT technologies the UPS (Uninterruptible Power Supply) covers a critical role. A UPS is equipment that works continuously 24/7, 365 days per year to secure high quality electrical power to your critical load. The system necessitates regular maintenance to avoid unexpected downtime. Remote monitoring helps to minimize any availability risk—it is like having 24/7 virtual Eaton specialist on site. This session walks you through how to effectively integrate cybersecurity best practices into remote monitoring design to secure your power availability and connected equipment against cyber threats.

Trends in Public Key Infrastructure (PKI) automation

How an organization manages their PKI and obtains security certificates is more important than ever due to the proliferation of M2M interactions between IoT devices, mobile, web, and cloud-based applications and services. This presentation will cover some of the new trends in PKI automation including the use of RESTful API, IT automation software such as Ansible, and the Automated Certificate Management Environment (ACME) protocol in conjunction with nonprofit Certificate Authorities (CA) against cyber threats.

Electric Vehicle (EV) embedded software authentication, secure-boot and FOTA

Today's vehicles have dozens of small embedded computers on board, controlling and monitoring nearly every system. For electrical vehicles, the usage of computers is even more demanding; providing intelligence and control for the powertrain, batteries and even connectivity to public charger stations—basically a point of sale exchanging private and monetary information. This increasingly intelligent and digital design presents cybersecurity challenges and risks. For instance, if malicious software is installed, the results could jeopardize the safety of the vehicle and directly affect the bottom line, with possible irreparable damages to the manufacturer brand. In this session, we explore options to improve vehicle cybersecurity through the implementation of Software Authentication, Secure Boot and FOTA (Firmware Over The Air) updates.

Protecting marine and offshore operations

Did you know that around 90% of the global international trade is transported by the maritime sector? Due to the importance of the maritime industry, the vessels, ports and related systems are getting more and more connected to make the maritime supply chains and operations more efficient. This increased connectivity, along with more automated and interconnected systems have made cybersecurity an important aspect of the day-to-day operations; from malware protection and network segregation to incident response and readiness.

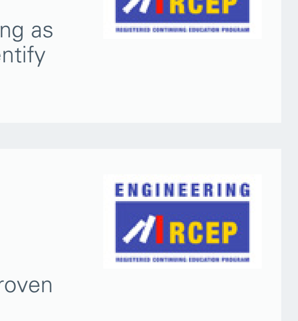
Defense in-depth solutions

You may never be attacked by a serious hacker, but typical control networks are extremely vulnerable to simple day to day security and reliability issues. Human errors, poor network segmentation and unprotected points of entry into the network, 'soft' targets such as un-patched PCs and vulnerable PLCs, can result in significant production losses and even safety issues. New intrinsically safe industrial security solutions have changed the way industrial ethernet security is managed by providing an intrinsically secure solution right out of the box. This provides a simple, effective cybersecurity solution for control and automation engineers which does not require IT skills for configuration and installation, saving significant time and cost investments.

Best practices to secure electrical monitoring systems

An electrical power monitoring system helps to maximize the uptime and safety of a facility by providing real-time remote visibility, alerts and insights to the business operations. The criticality of these systems necessitates regular maintenance to avoid unexpected downtime. This presentation will address how to effectively integrate cybersecurity best practices into your existing maintenance routine to secure your power monitoring system and connected equipment against cyber threats.

Advanced technical cybersecurity topics



Dig deep into the integral technologies needed to bring dependable products and platforms to market.

Review our sessions:

Cybersecurity as part of lifecycle management

ENGINEERING RCEP

Cybersecurity can be effectively integrated into an overall lifecycle maintenance program. An overview of Industrial Control System (ICS) maintenance practices are presented along with recommendations on how to integrate into overall lifecycle maintenance.

Securing legacy systems

ENGINEERING RCEP

For ICS applications, it is not always possible or practical to patch or update a system to address vulnerabilities. Cost, availability, safety, regulatory, personnel, and other factors eliminate upgrading as an option. Basic techniques (assessment, boundary defenses, and ICS specific monitoring) to identify and address cybersecurity on these systems is presented.

Cybersecure supply chain

ENGINEERING RCEP

This session brings to light the cyber risks that can creep into devices, systems, software and services if supply chains do not take care of cybersecurity. In this session we'll dive into various supply chain related cyber risks, complexities involved in mitigating those risks and offer some proven approaches that help protect asset owners, software vendors and device manufacturers.

We'll also explore mitigation tactics like cybersecurity certifications, device security testing & various other techno-legal methodologies to help mitigate the cyber risk along the lifecycle of devices, systems, software and services.

Cyber resiliency

ENGINEERING RCEP

Eaton will discuss the overall cyber risk and resiliency of critical infrastructure, and the role of various stakeholders in cyber resiliency. The presentation will focus on the operational and business impacts of cyber breaches, going through some quick examples of the financial risks for not having adequate investment in cyber measures.

Secure by design

ENGINEERING RCEP

The connected world depends on security. As more and more intelligent connected products enter our everyday life, security becomes essential. The Secure by Design philosophy assures that products incorporate cybersecurity into their design. Secure by Design relies on the Secure Development Lifecycle to incorporate cybersecurity at every step of the development process. With evolving systems becoming ever more complex, cybersecurity is a never-ending journey, and we will show you how to plot your course.

EATON Powering Business Worldwide

A more connected world needs more trusted environments. Explore our approach to managing a defense against emerging cybersecurity threats and view our on-demand global forum and educational program.

Eaton.com/CybersecurityPerspectives