APEC 2027 Industry Session Proposal

Corresponding Organizer: Conor Quinn[redacted]

Type of Proposal: Full Industry Session

Session Size: 4 presentation slots

Session Title: The Need for CyberSecurity in Power Supplies, Converters and Systems

Description of Session: Power supplies, converters and systems support critical infrastructure in many applications. Digital control and communications are now pervasive in these power products and they form part of the attack surface for actors who may intentionally or accidentally cause harm to end systems. This session will address the trends in, emerging standards and solutions for, and use cases pertaining to product cybersecurity in power conversion equipment. The presenters represent a cross-section of the industry including device manufacturers, power supply unit (PSU) providers, and system designers. While concepts for utility-scale security were presented previously, we believe this is the first time at APEC that security of high-performance electronic equipment and its powering infrastructure will be addressed in depth.

Target Audience: Power, firmware and project designers working with digitally configured or controlled power solutions. Users and specifiers of power conversion devices and equipment.

Session Organizers (and proposed session co-chairs):

Primary Contact: Conor Quinn, Senior Director of Technical Strategy
Advanced Energy Industries
[redacted]

Co-Chair: Eric Swenson, Member of Senior Technical Staff
IBM
[redacted]

Session Title: The need for CyberSecurity in Power Supplies and Power Converters

Session Outline

1. The Evolution of Security in Digitally Controlled Power Supplies
   Presenter: Peter Miller, Texas Instruments

   Abstract: Digitally controlled power supplies are nothing new. PMBus was introduced 20 years ago at APEC 2005 and digital control of power supplies dates back to at least 1991 with I2C controlled digipots, but security of digitally controlled power supplies has recently become a hot topic. The presenter will talk about the evolution of security features in Digitally Controlled power supplies, and how some recent events have changes the landscape, and threat

considerations for those security features. From basic write protection to authenticated writes and encryption-based attestation, how has security evolved, what are the available security features, and when and why are they needed?
In this presentation, Peter will talk about how security features have changed over the decades, what threats those security features were intended to address, and what assumptions were made “at the time” for those security features to be “effective enough” as well as some key events that have challenged those assumptions, and how those challenges lead to the next generation of security features.

2. PMBus 1.5 Part IV: New Commands for Securing PMBus
   Presenter: Robert Santucci, Intel

   Abstract: Digital voltage regulators present an attractive target to malicious hackers. Their cyber-physical nature allows hackers the opportunity to physically damage a system via voltage commands, known as permanent denial-of-service. An attacker could mess with OTP/OVP/OCP/UVP protection thresholds to induce shutdowns or permit damage. Unauthorized voltage control may allow predictable encryption keys. With more VRs embedding microcontrollers, unauthorized firmware may allow an attacker to embed vulnerabilities for future use. This presentation reviews new commands defined in PMBus 1.5 Part IV that enable VR attestation, secure firmware updates, and control command access.

   In this presentation, Robert will talk about new features introduced as part of the PMBus 1.5 Part IV specification to harden voltage regulators and PMICs against attack. He will overview the theory and commands used to attest the VR and its firmware contents are as expected by the system designer. He will discuss how those same methods can be utilized to validate a candidate firmware update before accepting it. Finally, he will discuss PMBus command access control, both globally applied to all potential bus host but also how to open commands only for specific bus hosts.

3. Cyber Security Requirements in Open Compute Project’s M-CRPS Power Supply
   Presenter: Donato Kava, Advanced Energy Industries

   Abstract: The Modular Hardware System – Common Redundant Power Supply (M-CRPS), published by the Open Compute Project (OCP), is one of the first industry-standard power supplies to include product cybersecurity requirements. These requirements apply an embedded system's cyber security approach to a hyper scale power supply.

   This presentation will review these security requirements including secure boot, run time attestation, and secure update. We will also discuss the possible interactions with the full system, limitations, and ways to expand future security.

4. Device and component challenges and advances in high voltage conversion
   Presenter: Justin Henspeter, IBM

Abstract: System security is a focus area for all IT infrastructure providers. New system features like pervasive encryption, the transition to cloud-based offerings, and the demand for quantum-safe platforms necessitate increased cryptographic performance and agility. Two topics will be discussed during the presentation.

AC/DC power supply firmware is updateable in situ and requires designs that support secure boot load functionality. IBM's secure boot implementation requires the firmware image to be digitally signed and verified using asymmetric encryption. In addition, the adoption of a cryptography method considered to be quantum-safe by industry standards will eventually be required. Finally, it is vitally important that the source code used to develop power supply firmware is virus free and secure from tampering. This presentation will discuss IBM's view on the current state of the industry and summarize IBM's requirements / expectations regarding secure boot, encryption, and firmware integrity.

Battery backup to the hardware enabled encryption is critical to maintaining encryption keys. This allows the data to be decrypted. If power is lost to the encryption devices, encrypted data is generally unrecoverable. Also, when the host system is in a powered off state, an onboard backup battery supplies power to the tamper detection devices in the encryption hardware, powering the destruction of encryption keys if tampering is detected.

Biographies of session organizers and presenters

Conor Quinn is responsible for Technical Strategy and Technology Planning at Advanced Energy Industries, Inc. He has 30 years of experience in the power electronics industry in various design, management, and technology roles. He is currently a co-chair of the Power Source Manufacturers Association (PSMA) Power Technology Roadmap committee, and on the Steering Committee of the Applied Power Electronics Conference (APEC). He served as General Chair for APEC 2021 and has also served as a board member of PSMA and of the System Management Interface Forum.

Conor holds a BE in Electrical Engineering from University College Cork in Ireland and an MSEE and PhD from the University of Minnesota. He has been awarded 3 patents in the field of power electronics and control systems.

Peter Miller is the current Chair of the PMBus Standards workgroup and a senior customer support and applications engineer for TI's Buck Switching Regulators product line. Peter has more than 20 years of industry experience in power semiconductors, spanning the disciplines of analog IC design, power IC product definition and direct customer support for analog and digitally controlled power products including hardware and firmware PMBus implementations.

Peter Miller holds a Bachelor's of Science and Master's of Science in Electrical Engineering from Worcester Polytechnic Institute.

Robert Santucci is a senior staff engineer and the digital lead for Intel's VR13.HC, VR14, and next generation server motherboard voltage regulators. He has more than 20 years of industry experience in mixed-signal design, including 15 years in digital control of voltage regulators and PMICs.

Robert holds Doctor of Philosophy and Master of Science degrees in Electrical Engineering from Arizona State University. He has Bachelor of Science degrees in Electrical Engineering and in Computer Science from Embry-Riddle Aeronautical University.

Donato Kava is Advanced Energy's Product Cyber Architect focused on bringing hardware layer security and secure by design principles into the digital control logic and production of PSUs.

Kava is a US Navy veteran who served onboard USS Thach (FFG-43) as an electronics technician. He received his BS degree in electrical engineering from the University of Texas at El Paso and his MS degree in computer engineering from Boston University. His past work at MIT Lincoln Laboratory in the Secure and Resilient Systems and Technology Group focused on researching and developing prototypes answering the question of how to securely fabricate and design new microelectronic systems and secure legacy systems.

Eric Swenson is a member of the IBM Senior Technical Staff working as a Power Development Engineer. Eric's current role is the introduction of new technology into IBM power subsystem designs including battery technology to be used in all IBM brands.

He received his Bachelor of Electrical Engineering degree in 1987 and his Masters of Science in Electrical Engineering degree in 1995, both from the University of Minnesota. Eric currently holds 23 patents related to battery technology, DC/DC converter technology, and test methods. He has been working in technology and qualification of AC/DC and DC/DC converters, PDUs, UPSs, and battery technology for 37 years. Eric is also an IBM lead auditor for the manufacturing of power subsystem assemblies and air moving devices. Finally, he is an IBM Lean Six Sigma (LSS) blackbelt specializing in process monitoring and root cause analysis.

Justin Henspeter is a Power Development Engineer at IBM. During his 17-year career with IBM, he has worked in Power Development focusing on the delivery of the AC/DC and DC/DC subsystems used in IBM's Enterprise class servers and Main Frame.

He completed a BSEE with a Minor in Optics at Saint Cloud State University in 2007. In December 2016, Justin obtained his MSEE from Iowa State University with a focus in Microelectronics and Photonics. In the last 5 years, his focus has expanded into systems architecture where he works closely with memory, processor, thermal/mechanical, and software/firmware teams to deliver IBM's Power Systems roadmap in addition to the overall power subsystem architecture of IBM's Quantum Systems One and Two..