

# PowerSession Series

## Emerging Cyber Threats and Actionable Responses

*An Expert Roundtable*

September 23, 2020

Presented by: Energy Central

Thank you to our sponsor:



**OWL**  
Cyber Defense

# PowerSession Series: Emerging Cyber Threats and Actionable Responses: An Expert Roundtable

## Panel Members:



**Massoud Amin**

Professor of Electrical and  
Computer Engineering  
University of Minnesota



**Brian Romansky**

Chief Technology Officer  
Owl Cyber Defense



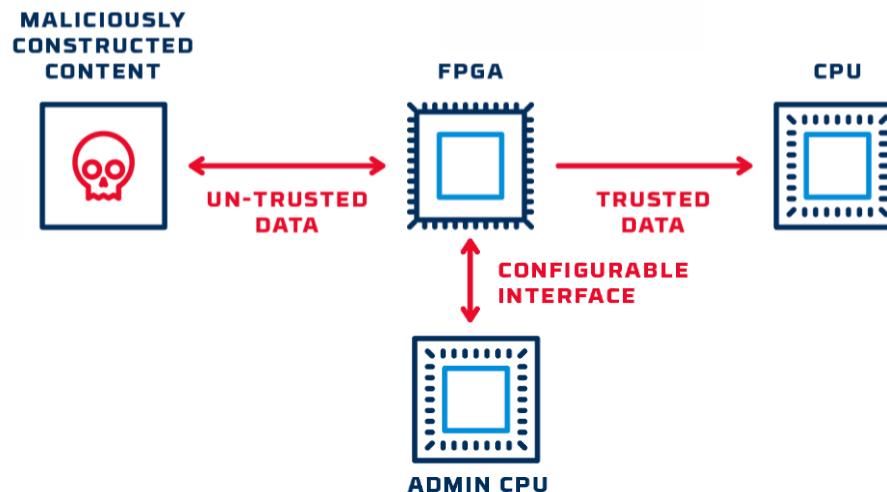
**Andrew Bochman**

Senior Grid Strategist  
Idaho National Laboratory

- Please enter your questions in the chat box on the screen.
- We encourage your participation during our designated Q&A breaks.
- Unanswered questions will be addressed post-event.
- The replay and slides will be available within a week of this session.

# Use Case: Ripple-20 and Protocol Break

- Ripple20 is a set of 19 vulnerabilities found in a widely used TCP/IP
- Attacks take advantage of software vulnerabilities
  - Mal-formed packets can trigger errors in the host CPU, some can execute arbitrary code
  - Several forms can be delivered through a conventional industrial firewall or switch
  - Many legacy systems with this vulnerability can not be updated or patched
- Hardware-based (FPGA) protocol break blocks low-level attacks
  - Hardware packet processor extracts payload-only from incoming traffic
  - A new, valid TCP/IP stack is built to deliver payload to the vulnerable destination system (CPU)
  - Protocol level attacks are blocked - more effective than software-based rules running on a firewall



# PowerSession Series: Emerging Cyber Threats and Actionable Responses: An Expert Roundtable

## Panel Members:



**Massoud Amin**

Professor of Electrical and  
Computer Engineering  
University of Minnesota



**Brian Romansky**

Chief Technology Officer  
Owl Cyber Defense



**Andrew Bochman**

Senior Grid Strategist  
Idaho National Laboratory

- Please enter your questions in the chat box on the screen.
- We encourage your participation during our designated Q&A breaks.
- Unanswered questions will be addressed post-event.
- The replay and slides will be available within a week of this session.

Thank you and thanks to our sponsor!



**OWL**

Cyber Defense