INL/MIS-22-69053-Revision-0

Bridging the ICS 'Communication Gap'

September 2022

Keith D Mecham

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-22-69053-Revision-0

Bridging the ICS 'Communication Gap'

Keith D Mecham

September 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

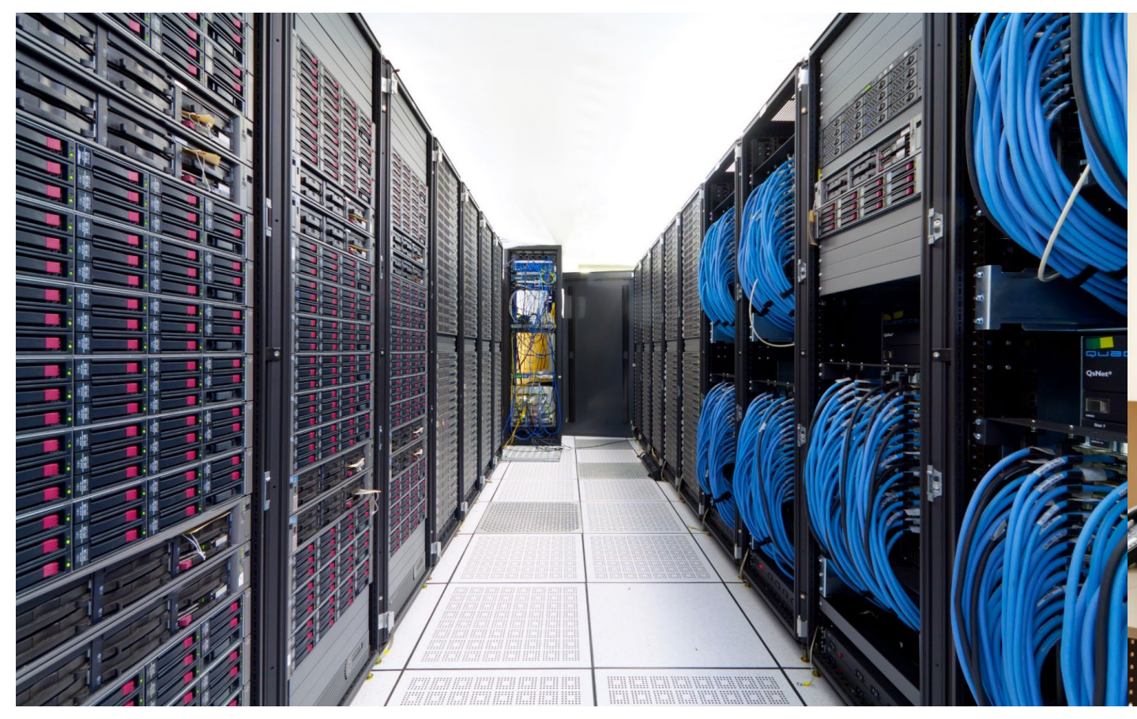
Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Bridging the ICS ‘Communication Gap’

Protocol Analytics Enabling Forensics of Industrial Control Systems

What networks within Critical Infrastructure can we monitor and protect today?

- A multitude of cybersecurity platforms and tools are available to monitor standard ‘IT-based’ networks



Information Technology (IT):

- *Cloud & data centers*
- *Servers & workstations*

Operational Technology (OT):

- *Control centers*
- *Engineering workstations*

What about Industrial Control Systems (ICS)?

- Some ICS devices communicate over Ethernet and can be protected with existing OT cybersecurity tools
- Other ICS networks are based on serial or industrial Ethernet protocols, which differ significantly from Ethernet in IT
  - ***Existing cybersecurity tools can’t protect these networks***

ICS networks (‘subnetwork’ within OT):

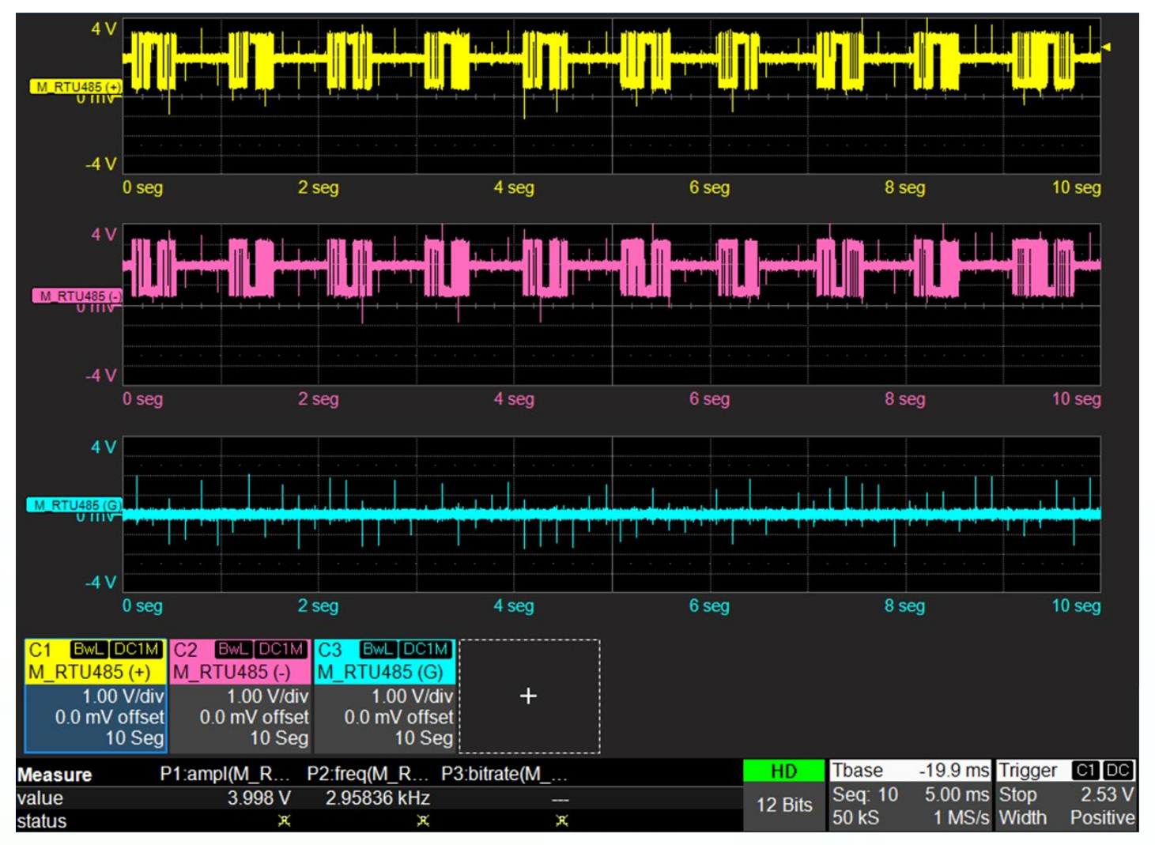
- *ICS devices: PLCs, HMIs, etc.*
- Safety systems
- Embedded controllers
- Smart sensors & actuators

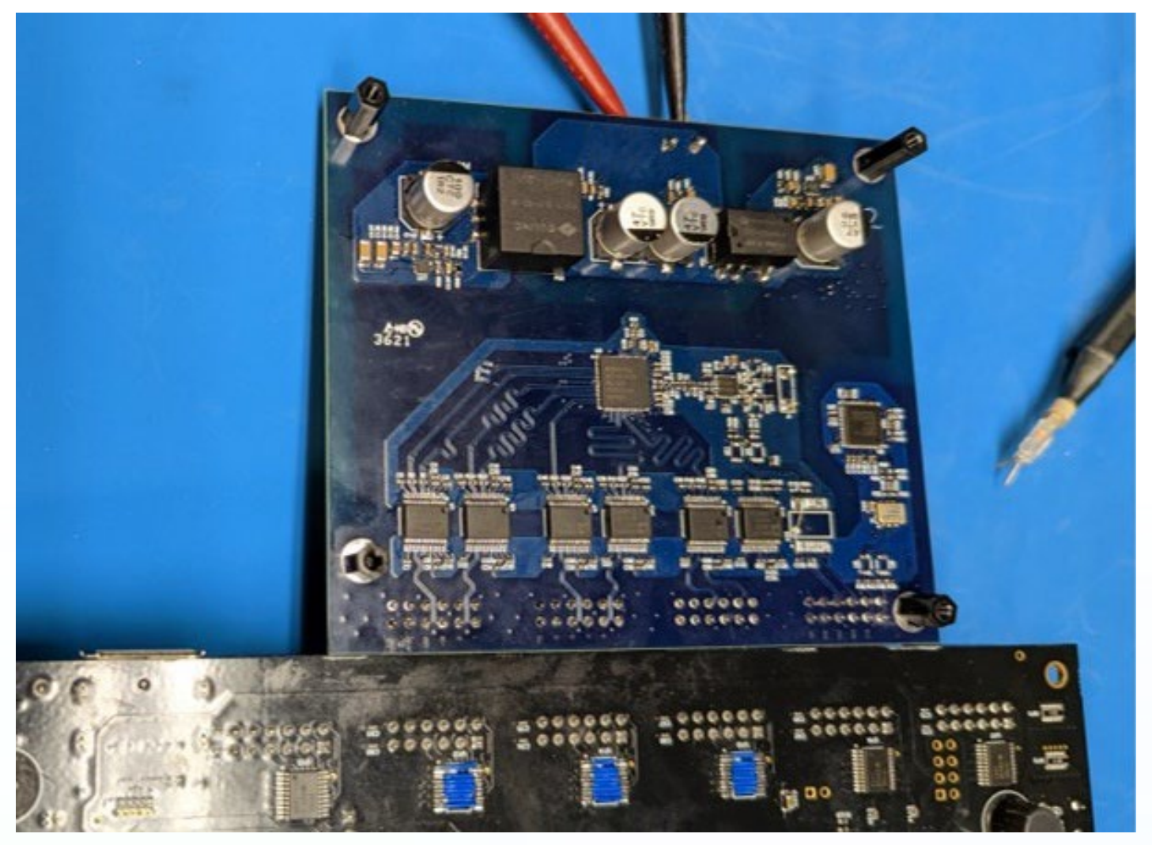
Technical challenges impede the development of cybersecurity tools for ICS environments:

- 40+ communication protocols with significant differences:
  - Physical & electrical properties, signal encoding schemes
- Performance degradation or disruption of ICS devices and networks can cause physical processes to fail

PAFICS researchers set out to discover how overcome technical challenges in the lab…

- Research focused on 13 ‘key’ ICS protocols representing the spectrum of electrical, physical, and signal variations
- Researchers worked to capture, identify, and decode known data communicated between ICS devices:
  - Captured signals with a high bandwidth digital oscilloscope
  - Analyzed captured signals, identified defining characteristics
  - Developed protocol signatures and identification algorithms
  - Discovered how to build decode algorithms for each protocol
- Algorithms were then validated through bench-top testing:
  - Evaluated the effectiveness of identification algorithms
  - Analyzed output from decode algorithms and verified accuracy



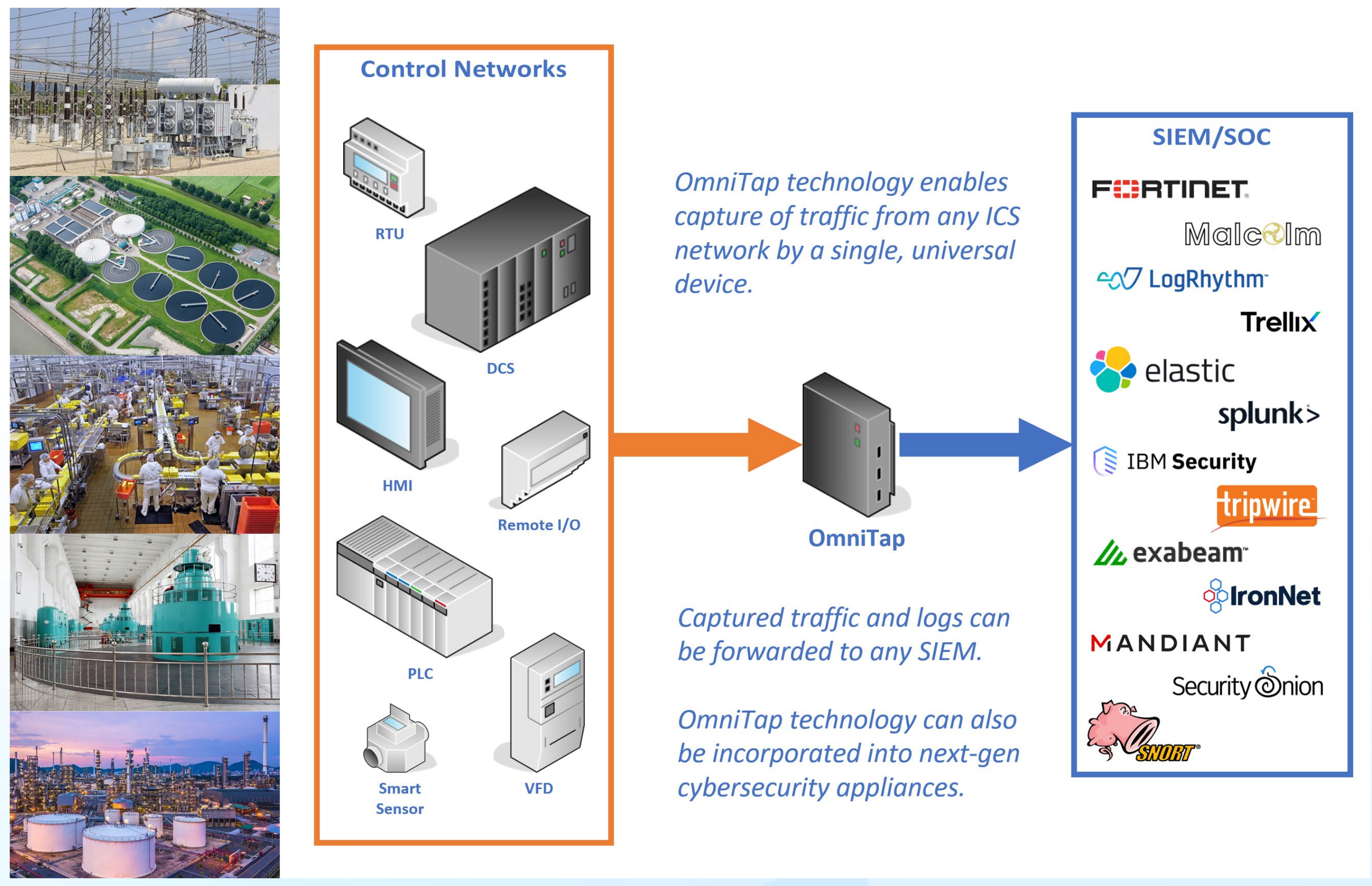


…And develop the technology to capture all ICS communication with a single device

- Analyzed available data to formulate requirements for a passive, disruption/distortion free, capture interface
- Developed a prototype capture device compatible with most if not all ICS communication protocols
  - Selected a commercial FPGA/CPU SOM with carrier PCB
  - Developed a passive input circuit with broad electrical compatibility
  - Incorporated input circuit into a prototype capture PCB
  - Tested prototype with representative signals to validate performance
- Implemented identification & decode algorithms on CPU/FPGA
- Tested the prototype hardware on live communication between ICS devices, iterating through several of the ‘key’ protocols
  - Additional testing at scale remains to be completed in the future

Technology resulting from PAFICS, called ‘OmniTap’, is patent pending and is being licensed for commercialization

- OmniTap technology makes development of a universal ICS capture/translation device possible
  - U.S. provisional patent (Nov 2021),
  - U.S. patent and PTC to be filed Nov 2022
- Commercial License with GoldenWolf LLC is in progress:
  - INL researchers in will participate in development
  - Easy to deploy device captures, translates, and forwards traffic to existing cybersecurity tools
  - Universal compatibility with ICS protocols, serial & Ethernet-based, up to 1Gbps (copper media only)



OmniTap technology enables capture of traffic from any ICS network by a single, universal device.

Captured traffic and logs can be forwarded to any SIEM.

OmniTap technology can also be incorporated into next-gen cybersecurity appliances.

OmniTap will shift the ICS cybersecurity paradigm:

- Enable existing cybersecurity tools to monitor and protect ICS networks
- Go beyond ‘Defense in Depth’ toward comprehensive ICS cyber-defense
- Align IT, OT, and ICS best security practices
- Embrace connected control devices such as IIoT, armed with tools to keep them secure
- Mitigate ICS market fragmentation, encouraging new cybersecurity tool development

PAFICS LDRD 20A44-032FP
Keith Mecham (PI), Daniel Hearn, Devin Vollmer, Tanmay Bhagwat, Ted Tracy
LRS: INL/MIS-22-69053

Battelle Energy Alliance manages INL for the
U.S. Department of Energy’s Office of Nuclear Energy

Idaho National Laboratory

Work supported through the INL Laboratory Directed Research& Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517

www.inl.gov