OT, IoT, and AD Cybersecurity Landscape

Looking at operational technology, internet of things, and autonomous devices

Lori Flynn, PhD
lflynn@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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 Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM22-0991

OT can be AD, IoT, both or neither

OT, IoT, and AD: specialized hardware + software

Mostly not incorporated into IT security systems. Increasing connectivity to IT systems

OT differences: specialized often proprietary systems, often embedded code, some with limited bandwidth & power, often owners lack ability to inspect source code

OT limited or lacking: software assurance tooling, cybersecurity monitoring, control coordination with intrusion protection systems, analyses of IT system connections impacts both ways, automated alerts when something wrong, alert monitoring, inspection, and fixes

Operational Technology (OT)

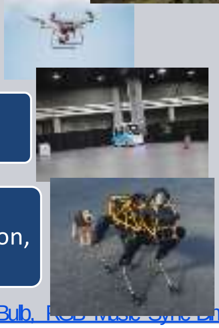
Control or sense the physical world
(vs. IT systems manage data)

- Distributed control systems (e.g., power, manufacturing)
- Supervisory control and Data Acquisition Systems (SCADA, e.g., rail, pipelines)
- Buildings and Physical Access Controls (e.g., HVAC, elevators, door swipe cards)

Autonomous Devices as OT

System moves and can operate without a human in the loop

- Vehicles (cars, trucks, trains)
- Robots (e.g., landmine handlers, environment discovery and manipulation, cleaners)



Internet of Things as OT

Connect things to internet to capture data and send control

- Examples: Light bulbs controllable with apps, air quality sensors

Images:

* Drone Photo by Annie Spratt on Unsplash
* "Testing the SCADA train control system in a power substation in Queens. 10-23-2019" by MTA C&D - EAST SIDE ACCESS is licensed under CC BY 2.0.
* South Houston Nevada Water Plant: "scada" by sam_churchill is licensed under CC BY 2.0
* "File:KUKA Industrial Robots IR.jpg" by Mixabest is licensed under CC BY-SA 3.0.
* "USS Porter fires its Phalanx close-in weapons system" by Official U.S. Navy Imagery is licensed under CC BY 2.0.

*Govee Color LED Light Bulb, RGB Music Sync Dimmable Color Changing Bulbs A19 7W Equivalent 60W, Multi-Color Smart LED Light Bulbs for Party Holiday Bedlamp, Needed APP Control (Not WiFi) by shop8447 is marked with CC0 1.0.
* Greenhouse image: "20110419-RD-LSC-0206" by USDAgov is marked with Public Domain Mark 1.0.
* "Soft toy dog on a robot vacuum cleaner with Simon's Cat cartoon" by marcoverch is licensed under CC BY 2.0.
* "Keolis and Navya Autonomous Shared Ride Vehicle" by Metro Atlanta Transit Productions is licensed under CC BY-SA 2.0.
* "See Spot Run — Dog vs. Robot" by jurvetson is licensed under CC BY 2.0.

The Software Engineering Institute has expertise relevant to these R&D areas.

OT, IoT, and AD: R&D Directions

- Software assurance (SwA) tooling and security frameworks for development and analysis
- Binary analysis and combining binary analysis with source code analysis is especially important to analyze these devices for software assurance
- Coordinated IT/OT security systems that identify systems' cybersecurity and functionality should be monitored and problems identified and addressed
- Security analyses should consider physical dangers and privacy threats. E.g., due to bugs, hacking, or built-in unwanted functionality any of the following could be issues: autonomous weapon firing, loss of critical services, fire, flooding, stalking, surveillance of journalist by a threatening government via IoT systems

References

1. Awuson-David, Kenny, et al. "Facilitate Security Event Monitoring and Logging of Operational Technology (OT) Legacy Systems." International Conference of Reliable Information and Communication Technology. Springer, Cham, 2022.
2. Hahn, Adam. "Operational technology and information technology in industrial control systems." Cyber-security of SCADA and other industrial control systems. Springer, Cham, 2016. 51-68.
3. Filkins, Barbara, Doug Wylie, and A. J. Dely. "Sans 2019 State of OT/ICS Cybersecurity Survey." SANS™ Institute (2019).
4. Garimella, Phani Kumar. "IT-OT integration challenges in utilities." 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS). IEEE, 2018.
5. Salfati, Eran, and Michael Pease. "Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)." NIST Internal Report 8428, (2022).
6. "IT/OT Convergence Moving Digital Manufacturing Forward", Cisco, Whitepaper, 2018. https://www.cisco.com/c/dam/en_us/solutions/industries/manufacturing/ITOT-convergence-whitepaper.pdf
7. Murray, Glenn, Michael N. Johnstone, and Craig Valli. "The convergence of IT and OT in critical infrastructure." (2017).
8. Ron Brash. "What is an OT SIEM and How is it Different from IT SIEM", VERVE, July 2020. https://verveindustrial.com/resources/blog/what-is-an-ot-siem-and-how-is-it-different-from-it-siem/
9. Brian Benestelli and Dan Kambic. "IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems", SEI blog, July 2022. https://insights.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/
10. Will Klieber. "A Technique for Decompiling Binary Code for Software Assurance and Localized Repair ", SEI blog, Oct. 2021. https://insights.sei.cmu.edu/blog/a-technique-for-decompiling-binary-code-for-software-assurance-and-localized-repair
11. Alexander Petrilli. "Scoping IT & OT Together When Assessing an Organization's Resilience", SEI blog, Nov. 2018. https://insights.sei.cmu.edu/blog/scoping-it-ot-together-when-assessing-an-organizations-resilience/