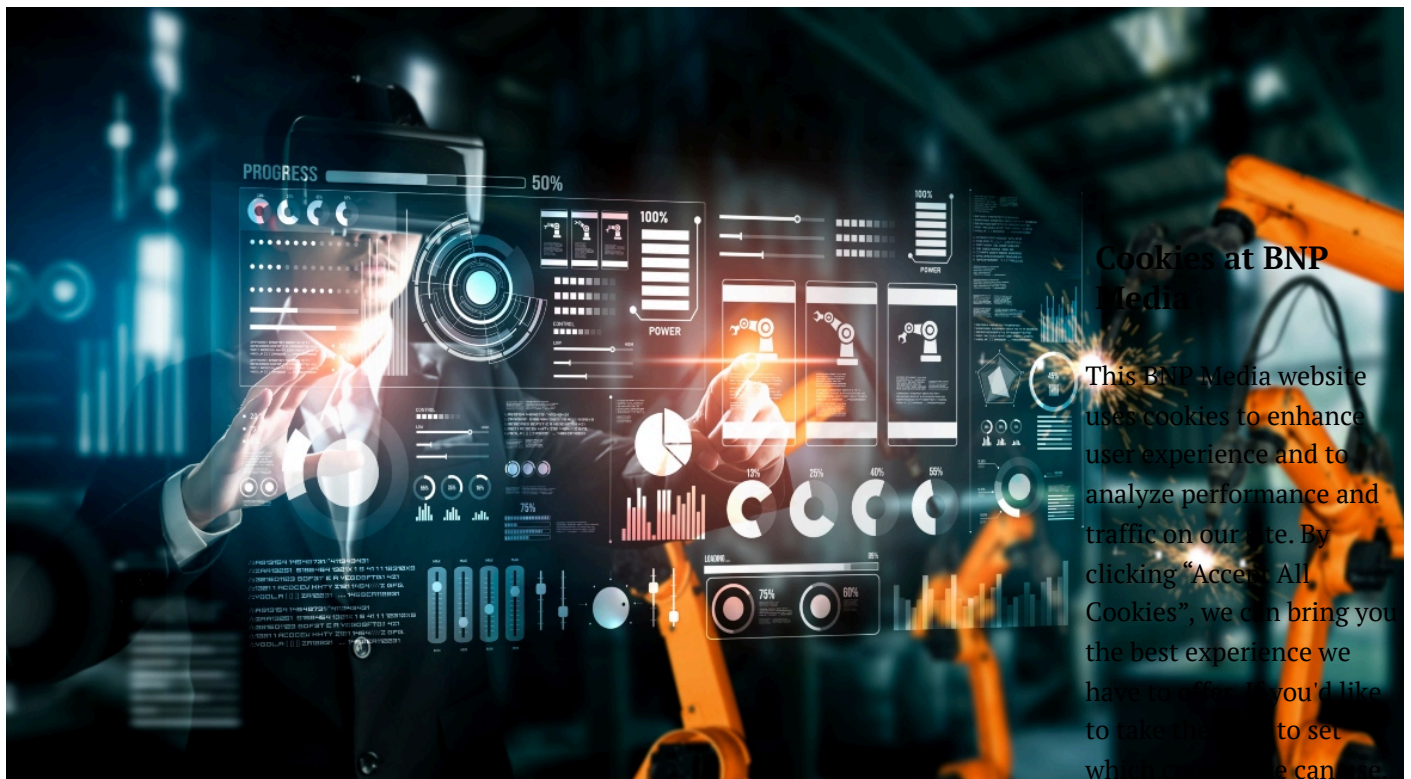


SECURITY

Can we close the gap between functional safety and cybersecurity in OT systems?

Both disciplines are essential to the operation of many critical systems. What will it take to bring them into alignment?

By Dr. Ang Cui



Cookies at BNP Media

This BNP Media website uses cookies to enhance user experience and to analyze performance and traffic on our site. By clicking "Accept All Cookies", we can bring you the best experience we have to offer. If you'd like to take control, to see which cookies we can use,

click 'Manage your Cookies'.

[View our Privacy Policy.](#)

[Accept All Cookies](#)

[Manage your Cookies](#)

March 29, 2022

The intersection between functional safety engineering and cybersecurity makes intuitive sense. Cyberattackers, who increasingly target operational technology (OT) systems, are opportunists who certainly recognize the potential gain of compromising the physical safety of a manufacturing line, a water treatment plant, an oil pipeline, or the antilock braking system of a car, to name just a few deployments where functional safety is essential.

But in fact, there is a large, exploitable gap between what safety systems engineers design and what cybersecurity features of these systems protect against.

The gap exists in part because functional safety and cybersecurity experts begin with different mandates. The safety experts focus on creating a predictable system that responds to faults and resumes safe operation. Cybersecurity experts try to understand how an unpredictable approach could upend that system.

The safety-cybersecurity gap has widened as we push for more connectivity, OT system responsiveness and process visibility. OT systems are changing too quickly for the old models of functional safety and cybersecurity engineering to address these challenges.

Experts in both camps are working diligently to protect the systems that keep critical safety equipment and processes on the knife-edge of reliable operation. But there are several factors to consider on the journey towards a truly integrated discipline that reflects the reality of increasingly digitized OT systems.

Factor 1: Safety and cybersecurity regulations and standards are still synching — and will be for years to come

Product certification expert [Mike Medoff](#) has spent more than a decade working for consortiums that inform standards like IEC 62443 and IEC 61850. He notes that 62443 first took shape in 2002. “That long time horizon allows the standards to be well thought out,” he says. “It also means changes come gradually.”

He also points out that standards that are written too explicitly are quickly made obsolete, so there are many areas where guidance is general and left open to manufacturers’ interpretation. “That’s a plus and a minus. It allows you to keep applying the standard over a longer time period. But it also leaves a lot more up to the person who is reading and applying the standard.”

Furthermore, safety and cybersecurity evolve at their own individual cadences. While Medoff states that there is more collaboration between the bodies creating standards, we’re a long way from true synchronization.

Factor 2: Safety systems are becoming more complex, better connected, and harder to protect

Cookies at BNP Media

This BNP Media website uses cookies to enhance user experience and to

analyze performance and traffic on our site. By

clicking “Accept All Cookies”, we can bring you the best experience.

That’s a have to offer. If you’d like to take the time to set

which cookies we can use,

click ‘Manage your

Cookies’

While Medoff [View our Privacy Policy.](#)

Network complexity presents abundant engineering challenges — and a massive increase in cybersecurity concerns. The safety system that is isolated from the rest of the OT system was often ideal in industrial deployments until operators demanded more access to maintain high performance and harvest data.

In most modern deployments, the safety system shares networks and sensors with other systems, such as DCS or BMS. This led to a massive expansion in the number of system inputs that safety engineers must consider. Additionally, they need to factor in non-standard hacking inputs and potential vulnerabilities that an attacker might exploit. Failure to do so could have liability implications in the event of a failure or system exploitation.

Traditionally, engineers have counted on security elements like access control and encryption to ensure inputs are valid and disruptions will be prevented. But cybersecurity researchers have found many flaws in these controls and in supporting technology, such as IP or the Media Access Control (MAC) layer, which can enable remote code execution and malfeasance that eventually leads to device compromise.

The massive increase in inputs and complexity also changes the terms of one contentious functional safety-cybersecurity debates:

How likely is it that an attacker could defeat a safety system?

Factor 3: The risk of cyberattacks in functional safety systems is growing

The cybersecurity firm Dragos, which investigated the 2017 Triton attack on a Saudi Arabian petrochemical plant, described it as “an escalation” in cyberwarfare, in that it was “specifically designed to target the safety function of the process.” Although the attackers had targeted the plant’s safety system, and the malware used was powerful enough to result in a catastrophic, life-threatening event, their efforts led only to a temporary plant shutdown. Moreover, Dragos concluded a catastrophic outcome was highly unlikely.

Cookies at BNP Media

This BNP Media website uses cookies to enhance user experience and to analyze performance and usage of our site. By clicking “Accept All Cookies”, we can bring you the best experience we have to offer. If you'd like to take the time to set which cookies we can use, click "Manage your Cookies".

[View our Privacy Policy.](#)

But we know more today about how an attacker can change logic controls to “trick” safety equipment that is designed to trip in the event it does not receive a signal of normal operation within a regular timeframe. In other words, a sophisticated attacker could simulate normal operations even when devices or systems were approaching or in an unsafe state.

This has immediate implications for safety engineering. Namely, if safety devices can be disabled *or* manipulated, have we done enough to engineer their cybersecurity features?

How can security and safety experts expand and deepen collaboration?

Functional safety and security experts first need to collaboratively address subsidiary questions, such as:

- What is the real risk of a successful cyberattack on safety systems or equipment?
- How can safety engineers and cyber researchers better coordinate to close the gap between safety and security standards?
- Is it time to consider more robust security at the device level as a necessity rather than an attractive feature in safety systems?

Here are three points cybersecurity experts need to emphasize:

Point 1: We can't wait on regulations and standards. Important as they are, safety and security standards will not address the cutting edge of safety and cybersecurity.

Point 2: Mapping needs to reflect the growing complexity of functional safety systems. As system inputs proliferate, it will be necessary for both disciplines to visualize and create reliable defenses for OT and functional safety systems that reflect rapidly increasing connectivity and complexity.

Point 3: Security researchers need more seats at the table. In general, cyber researchers have had to fight for a seat at the table, even as their work overlaps with and introduces complexity to safety systems.

Conferences where experts from both fields are also lacking — and needed. Without a true integration of the disciplines, industrial deployments will not be protected from the full range of modern threats.

KEYWORDS: [critical infrastructure](#) [cyber security](#) [operational security](#) [regulatory compliance risk management](#)

Share This Story

Dr. Ang Cui is the Founder and CEO of [Red Balloon Security](#), a cybersecurity provider and research firm that specializes in the protection of embedded devices across all industries. In addition to publishing innovative research, Dr. Cui frequently provides commentary and thought

Cookies at BNP Media

This BNP Media website uses cookies to enhance user experience and to

analyze your research and traffic on our site. By clicking "Accept All

Cookies", we can bring you the best experience we

have to offer. If you'd like to take the time to set

which cookies we can use, click 'Manage your

Cookies'.

[View our Privacy Policy.](#)

leadership on the most pressing challenges in cybersecurity today. He earned a Ph.D. in computer science from Columbia University, where he worked extensively in the Intrusion Detection Systems Lab.

Recommended Content

JOIN TODAY

To unlock your recommendations.

Already have an account? [Sign In](#)

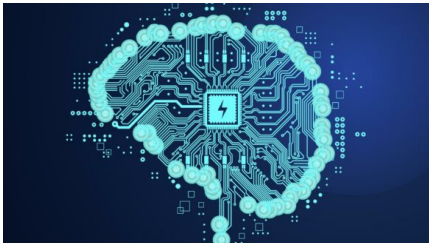


Security's Top Cybersecurity Leaders 2024

Security magazine's Top Cybersecurity Leaders 2024 award...

TOP CYBERSECURITY LEADERS

By: Security Staff



The intersection of cybersecurity and artificial intelligence

Artificial intelligence (AI) is a valuable cybersecurity...

LOGICAL SECURITY

By: Pam Nigro



Assessing the pros and cons of AI for cybersecurity

Artificial intelligence (AI) has significant implications...

LOGICAL SECURITY

By: Charles Denver

BNP Media website uses cookies to enhance user experience and to analyze performance and traffic on our site. By clicking "Accept All Cookies", we can bring you the best experience we have to offer. If you'd like to take the time to set which cookies we can use, click 'Manage your Cookies'.
[View our Privacy Policy.](#)

Related Articles



Three ways that cybersecurity companies can close the gender gap

[See More](#)



Closing the gap between student safety and security in K-12 school transportation

[See More](#)



How security leaders can close the tech talent gap — once and for all

[See More](#)

Cookies at BNP Media

This BNP Media website uses cookies to enhance user experience and to analyze performance and traffic on our site. By clicking "Accept All Cookies", we can bring you the best experience we have to offer. If you'd like to take the time to set which cookies we can use, click 'Manage your Cookies'.

[View our Privacy Policy.](#)

Sign-up to receive top management & result-driven techniques in the industry.

Join over 20,000+ industry leaders who receive our premium content.

SIGN UP TODAY!

Copyright ©2025. All Rights Reserved BNP Media.

Design, CMS, Hosting & Web Development :: ePublishing