<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Speaker/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-9:15 am</td>
<td>Welcome &amp; Opening Remarks</td>
<td>Tim Conway &amp; Robert M. Lee @robertmlee, Summit Co-Chairs, SANS Institute</td>
</tr>
<tr>
<td>9:15-10:00 am</td>
<td>Keynote</td>
<td>Keeping the Lights on in a Dangerous World</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adam S. Lee, VP &amp; CSO, Dominion Energy Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adam will share his experiences and wisdom from over two decades leading</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operations countering terror threats, hostile foreign intelligence operations,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cyber attacks, and criminal enterprises, to managing security for a $100 billion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>energy company which serves as the power company to the Pentagon.</td>
</tr>
<tr>
<td>10:05-10:45 am</td>
<td>Security Worst Practices</td>
<td>David Foose @davefoose, Ovation Security Program Manager, Emerson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We hear all the time about “best practices,” but this presentation will present</td>
</tr>
<tr>
<td></td>
<td></td>
<td>war stories that are examples of organizations approaching various security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>problems the wrong way – that is, “worst practices” in security. We’ll walk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through the reasons why these events occurred and look at improvements that can</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be made going forward to make sure they don’t happen again.</td>
</tr>
<tr>
<td>10:45-11:15 am</td>
<td>Networking Break</td>
<td></td>
</tr>
<tr>
<td>11:15-11:55 am</td>
<td>5 Blind Men and an Elephant called ICS</td>
<td>Eric Byres @ICS_Secure, CEO, aDolus Inc.</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Security</td>
<td>Industrial companies depend on their vendors to supply valid software and firmware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for control system implementation and upgrades. If this chain of trust is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>compromised, then malicious software can be introduced that alters core system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>functionality, potentially impacting critical operations and human safety.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unfortunately, there are currently few safeguards in place to protect IIoT and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICS devices against the introduction of counterfeit firmware and software.</td>
</tr>
</tbody>
</table>
session, we discuss the five key supply chain risks to ICS software and firmware, showing specific examples of each of these threats. We’ll introduce a framework funded by the DHS to safeguard against ICS supply chain attacks. Finally, we’ll show you how to satisfy security requirements like NERC CIP-013, without introducing onerous or error-prone processes: * Verification of software integrity and authenticity: Learn how to ensure that your staff are not loading counterfeit or tampered software and firmware into critical systems. * Vulnerability detection and disclosure: Learn how to generate a Software Bill of Materials (SBoM) to reveal unexpected sub-components that may contain vulnerabilities or malware. * Validation of firmware versions: Learn how to ensure that firmware is an up-to-date version, tested and approved by the vendor rather than an unauthorized or obsolete version. * Validation of certificate-chains: Learn how to detect fraudulently signed packages masquerading as authentic, avoiding Stuxnet-style attacks where private keys have been stolen. * Detection of blacklisted products: Learn how to uncover sub-components in software from prohibited suppliers.

11:55 am – 12:25 pm
The Current Status of Industrial Control Systems in Developing Countries: A Case Study of Argentina and Latin America

Almada Pablo Martin, Director of ICS/IoT Services, KPMG

While developed countries such as the United States have led the way in the cybersecurity of critical infrastructure, developing countries have fallen behind due to socioeconomic conditions, lack of investment, and difficulties in developing the skills needed in this area. This presentation examines Latin America’s critical infrastructure situation, with Argentina as a case of study. The presentation will start with a brief overview of current cyber regulation and national initiatives, then turn to examining the status of principal industries in the region, with a focus on the energy industry. Finally, we will look at lessons learned from underdeveloped countries, taking into account that industrial control system (ICS) best practices and regulations are often based on ideal scenarios that are not always feasible in developing nations. To address this challenge, the presentation will examine case studies in critical infrastructure cybersecurity and the steps that Argentina and other countries in the region need to take to improve ICS security in the context of the developing world.

12:25-1:30 pm Lunch

1:30-2:00 pm
At Least We Can Agree on This: Working with Legal to Improve Cybersecurity in Standard Agreements

Brent Foster, Founder, Extensible Security

In this interactive session, attorney Brent Foster will share tips to help your attorneys and agreements better secure your environment. Which agreements matter, and what linguistic “red flags” may leave you vulnerable if – or when – a crisis strikes? How can you convince legal to be more cooperative (after all, isn’t
everyone on the same side)? Brent will demystify the legalese to help you understand your risks and recourse, and present you with actual industry agreements so you can try your hand at redlining before you have to do the real thing.

2:05-2:35 pm

**Clean Up Your MES: The Bridge between IT and OT**

**Khalid Ansari @Khalid_Ansari**, Automation & MES Engineer, Qatar Aluminum Ltd.

This talk is directed primarily at owner-operators from the manufacturing sector, although other industries may benefit as well. Khalid Ansari will summarize his experience as an owner-operator and the challenge of securing a manufacturing execution system (MES). The presentation will begin by briefly describing what an MES is, using aluminum smelter as an example. An MES bridges IT and OT networks, typically interfacing with ERP on the IT side and automation layer on the OT side. The MES is the air-gap myth-buster, so it is critical to secure it. The presentation will discuss network segmentation, security options available for legacy OPC-DA and current OPC-UA interfaces; and look at other security controls that may be deployed to increase the security posture of a typical MES. The presentation will conclude by emphasizing the need for strong and verifiable disaster-recovery and business-continuity plans for situations when the MES goes down.

2:35-3:05 pm

**Networking Break**

3:10-3:50 pm

**Go-To Analysis for ICS Network Packet Captures**

**Gabriel Agboruche @ICS_Gabe**, Senior ICS/OT Security Consultant, Mandiant

Your plant's production line went down, your corporate IT Historian stopped receiving data from your ICS Historian or you just want to gain a greater understanding of what is happening in your ICS environment. You then go ahead and passively collect a day's worth of network packet data (PCAP), now what? The answer to that "now what?" is the analysis process for peering into the actual activity that's taking place on your ICS network. This presentation will equip individuals with some go-to analysis techniques for ICS network packet capture data.

3:55-4:25 pm

**Save the Day: Build an Incident Response Program Now**

**Steve Winterfeld**, Advisory CISO, Akamai

This talk is about building an Incident Response (IR) program based on North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), and National Institute of Standards and Technology (NIST) compliance frameworks, that is operational and effective. It will cover the pillars you need for a program, including framework for governance, the plans needed for execution, and
how to conduct exercises for validation. We'll talk about the need for plans vs playbooks, IR process, best way to be compliant, and industry frameworks. Finally, we will explore how to manage across the key leadership stakeholders, as well as how to prepare for both internal and third-party incidents for multiple scenarios.

### 4:30-5:10 pm

**ICS Threats and Mapping to ICS ATT&CK**

Robert M. Lee [@robertmlee](https://twitter.com/robertmlee), Summit Co-Chair, SANS Institute

This presentation will introduce the ICS ATT&CK framework as a tool for guiding security approaches for ICS security such as threat detection strategies. The presenter will take a few examples of active ICS threats and utilize models such as the ICS Cyber Kill Chain, the Sliding Scale of Cybersecurity, and Collection Management Frameworks in combination with ICS ATT&CK to give the attendees a repeatable way to guide their security approaches for the next year.

### 5:10-6:10 pm

**ICS Summit Networking**

Join our event sponsors and your fellow attendees for a little more post-Summit networking.

### 6:15-8:15 p.m.

**Summit Night Out**

**Let’s Split!**

Hop on the complimentary bus and join us for bowling, billiards, and a buffet at [Splitsville Luxury Lanes](https://splitsville.com) in Disney Springs! Dinner, drinks, bowling, and round-trip transportation are provided. If you prefer to strike out on your own after bowling to explore more of [Disney Springs](https://disneyworld.disney.go.com), you’re welcome to do so.

---

**Tuesday, March 3 #farsighted**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-9:20 am</td>
<td>Lifetime Achievement Award</td>
</tr>
<tr>
<td>9:20-10:00 am</td>
<td><strong>Keynote &amp; Demo</strong></td>
</tr>
<tr>
<td></td>
<td><strong>The PLC Made Me Do It!</strong></td>
</tr>
<tr>
<td></td>
<td>Tim Conway, Summit Co-Chair, SANS Institute</td>
</tr>
<tr>
<td></td>
<td>Jason Dely <a href="https://twitter.com/JasonJDely">@JasonJDely</a>, ICS Team, SANS Institute</td>
</tr>
<tr>
<td></td>
<td>Jeffrey Shearer, ICS Team, SANS Institute</td>
</tr>
</tbody>
</table>

ICS security programs are typically implemented to provide technical and non-technical controls to the process environment so the ICS can behave in a reliable and predictable manner. ICS-focused attacks have a sliding scale of effect with the largest effect being hardware manipulation to cause product quality issues, product manufacturing disruption or the highest effect of all - loss of life. Recent real-world
attacks have shown the effects of ICS hardware manipulation and the impacts it can have on a country's physical and psychological well-being. This presentation and demonstration will walk through some common attack techniques observed in ICS environments, detecting those attacks, and some approaches to consider as adversaries will continue to adapt to a defender's capabilities in the future.

<table>
<thead>
<tr>
<th>10:00-10:30 am</th>
<th>Networking Break</th>
</tr>
</thead>
</table>
| 10:30-11:10 am | **2020 ICS Cyber Attack Trends**  
Sarah G. Freeman, ICS Cybersecurity Analyst, Idaho National Lab |
| 11:15-11:55 am | **Mission Kill: Process Targeting in Industrial Control System Attacks**  
Joe Slowik @jfslowik, Principal Adversary Hunter, Dragos |

Typical conceptions of industrial control system (ICS) targeting focus on direct disruption of organizations through specific action resulting in complete operational loss, such as opening breakers to interrupt the flow of electricity, or tripping a safety system to shut down a plant. Yet further analysis of ICS events over time indicates adversaries are pursuing far more ambitious attack patterns. Following the 2015 Ukraine power event, ICS-focused attacks began to shift from direct disruption to changing, modifying, or otherwise undermining fundamental ICS processes by either staging more serious attacks or identifying specific process “pain points” with outsized value to the victim environment. There is clear evidence that adversaries are learning about process and operational dependencies in industrial environments and how they can be leveraged to achieve maximum impact. This presentation will examine three case studies: the 2016 Ukraine event, the 2017 TRISIS event, and the 2019 attack on the Abqaiq oil processing facility in Saudi Arabia (relevant for targeting purposes even though it was not a cyber attack). In each case, attackers identified specific operational pain points (protective relays, safety instrumented systems, hydrodesulfurization facilities) to create cascading or outsized impacts from specific device compromise (or destruction). Given these developments, ICS security operations need to move beyond the realm of being IT-centric to fusing IT visibility with industrial process awareness. From a defensive point of view, understanding the process environment and identifying critical path nodes for the defended facility is vital to ensure appropriate defense where it matters most. By understanding how
attackers have evolved, ICS and critical infrastructure defenders can better position themselves to counter future attacks.

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
</table>
| 11:55 am – 12:25 pm | **Cyber Guardian Exercise: A Case Study in Brazil to Address Challenges in Cybersecurity and Protect Critical Infrastructure**  
*Maxli Barroso Campos*, Cybersecurity Analyst, Cyber Defense Command, Brazilian Army  

This presentation will outline how the Cyber Guardian Exercise is establishing the principles of cyber protection for important national and critical infrastructure sectors in Brazil by building a strong cybersecurity community based on the exchange of experiences and a strong partnership between all parties involved. In 2019, 38 government and military agencies, defense-related firms, academic entities, and representatives from the financial, energy, telecommunications, and other critical sectors participated in Cyber Guardian 2.0. This presentation will examine the lessons learned from exercises using virtual and constructive simulation techniques to protect the financial and nuclear sectors from cyber attacks; virtual simulation using the Cyber Operations Simulator Program; and constructive simulation using a crisis management office for information technology, media, legal, and senior management issues. The presentation will also look at initiatives undertaken to improve cyber protection of critical infrastructure for national defense.

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:25-1:30 pm</td>
<td><strong>Lunch</strong></td>
</tr>
</tbody>
</table>
| 1:30-2:15 pm | **Nation-State Supply Chain Attacks for Dummies and You Too -or- Chipping Cisco Firewalls**  
*Monta Elkins [@MontaElkins], Security Researcher*  

Back in October 2018, Bloomberg recounted a Chinese supply-chain attack on Supermicro motherboards used in servers for Amazon, Apple, and more than 20 other companies. [https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companiesHere](https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companiesHere) is how I replicated it, on a Cisco firewall, with a shoestring budget, and how you can too. Sponsored by TDi technologies. [https://www.tditechnologies.com/](https://www.tditechnologies.com/)  


<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
</table>
| 2:15-2:50 pm | **Vulnerabilities on the Wire: Mitigations for Insecure ICS Protocols**  
*Michael Hoffman*, Principal ICS Security Engineer, Shell |
Insecure Modbus TCP and other legacy ICS protocols are still widely used in many ICS verticals. Due to extended operational ICS component life, these protocols will be used for many years to come. The question now is what can asset owners and operators do to secure their environments today? This presentation attempts to answer that question by examining the viability of deploying PLC configuration modifications, programming best practices, and network security controls to show that it is possible to increase the difficulty for attackers to exploit these systems and mitigate the effects of attacks based on insecure ICS protocols. Student kits provided in SANS ICS515 and ICS612 courses form the backdrop for testing and evaluation of ICS protocols, device configurations, and network security controls.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:50-3:15 pm</td>
<td>Networking Break</td>
</tr>
<tr>
<td>3:15-3:45 pm</td>
<td>“Project Runaway:” How the World’s Largest Manufacturers Are Unknowingly Leaking Their Secrets Online</td>
</tr>
<tr>
<td></td>
<td><strong>Matan Dobrushin</strong>, Head of Research, OTORIO</td>
</tr>
<tr>
<td></td>
<td><strong>Yoav Flint Rosenfeld</strong> @YoavFlint, Head of Services, OTORIO</td>
</tr>
</tbody>
</table>

Project files are the blueprints of the industrial process. They can contain network configurations, screen definitions, hardware and software configurations, and the actual automation logic of the controllers. Access to project file means access to knowledge about the most important elements of the production floor. Because of their sensitivity, these files should be kept in a well-secured location such as an internal vault. However, the growing need to share and collaborate with suppliers makes it difficult to keep track of the files, and the data can end up in the wrong hands. A large amount (>500!) of highly confidential industrial data is located on an Internet research site and available to every registered user. The data involve multiple manufacturers, suppliers, and orchestrators from different sectors and geographical locations. The amount of the data and the companies involved suggests that the widespread availability of such data is not a one-time event but rather a systematic issue caused by the security tools that are not protecting companies as they should. This presentation will explain the basic components and structures of certain project files; outline the threat landscape connected to the data and the inherent insecurity of the supply chain; show how an attacker might use these data to target a company’s operations and processes; look at what can be derived from automation logic by examining past research and proposing new approaches; share statistics about the amount of companies, sectors, and geolocations of the affected companies; and propose options to address the potential sources of the leaks and put in place different security methods to fix the problem.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:50-4:20 pm</td>
<td>Where Did You Come up with That Idea? Sharing is the Key</td>
</tr>
</tbody>
</table>
**Justin Opatrny**, Manager, Cyber Security Engineering, General Mills, Inc.

**Sanford Rice**, Manager – Technical Control Systems, Atmos Energy

Threats to ICS environments continue to advance requiring us as defenders to keep up with all the things (threats, training, technology, etc.). No one person or organization can do it all, leaving many opportunities to try, learn, develop, and most importantly, SHARE. This talk will cover a variety of methods for how individuals can contribute back to the overall ICS security community and beyond. Whether the contribution is big or small, from our individual critical infrastructure vertical or not, we are all in the same fight.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
</table>
| 4:25–5:00 pm | **Demo**  
RADICS: The DARPA Project to Restart the Power Grid after a Significant Cyber Attack |
|        | - Gary D. Seifert, EE PE, ICS Cyber, Microgrid, Power Systems, and Energy Systems  
- Tim Yardley, Principal Research Scientist, University of Illinois Urbana-Champaign Information Trust Institute |
|        | The Department of Defense (DOD) shares the national concern regarding a cyber-attack on the U.S. power grid. As such, the Defense Advanced Research Projects Agency (DARPA)’s Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program has challenged researchers over the past 4 years to develop technologies to enable the black start recovery of the U.S. power grid amidst a cyber-attack on the electrical sector’s critical infrastructure. Early into the RADICS program, researchers moved from simulated and synthetic data to practical exercises around cyber-physical systems to validate their research. Additionally, the RADICS team integrated utilities and cyber first responders as another validation vector and research relevance. In November 2018, RADICS supported Department of Energy’s (DOE) Liberty Eclipse exercise, and measured the challenges around black start restoration during cyber-attack, and has continued its partnership with DOE into the National Level Exercise in 2020. This presentation will discuss the results of the program, our efforts to transition these vital technologies to private and public sector stewards, our lessons learned in cyber incident response for electric power systems, and the importance of exercising our cyber recovery capabilities as a nation. |
| 5:00–6:00 pm | **Networking Reception Hosted By** SANS SECURITY AWARENESS |
| 6:00–8:00 pm | **GIAC Reception** |
This exclusive event brings together a recognized community of ICS security professionals (holders of GICSP, GRID, and GCIP certifications) for an evening of drinks, hors d'oeuvres, and networking.
Gabriel Agboruche @ICS_Gabe
Gabriel Agboruche is a Senior ICS/OT Security Consultant working for Mandiant FireEye. Traditionally educated as an Electrical/Nuclear Engineer, Gabriel transitioned to the security field shortly after the outbreak of Stuxnet where his commercial nuclear plant environment went through a drastic security transformation thrusting him into the midst of the ICS Security.

Pablo Alamada
Pablo is a Director at KPMG Argentina’s IT Advisory practice and has over 13 years of experience in different domains of Cyber Security. He is currently specialized in Industrial Cyber Security. Pablo has remarkable experience providing consulting services in the Cyber Security space for different industries and organizations mainly in the manufacturing, Oil & Gas, Energy and industrial sectors. He has developed experience in Cryptography, Cyber Security Architecture, Secure Code and Technical Assessments. He also specialized in Industrial Control Systems Cyber Security and Embedded Systems Cyber Security. Pablo has acquired a deep knowledge through specialized courses and trainings, such as Ethical Hacking, ISO 27000, SCADA/ICS, Cryptography, Risk Management and Web Application Assessment.

Khalid Ansari @_Khalid_Ansari
Khalid is an Automation and MES engineer with 20+ years of experience spanning the spectrum from software development to integration to owner-operations. For the past few years, he has been actively involved in strengthening his plant’s ICS security. He holds the GICSP certification.

Maxli Barroso Campos
Maxli holds a Master’s in Systems and Computation from UNIFACS, CISSP and GICSP. In 2019 took the ICS515 course in Orlando. He is Head of the Systems and Security Division of the Cyber Defense Command and is coordinator of the Cyber Guardian Exercise Study Group.

Eric Byres @ICS_Secure
Eric Byres is an expert in ICS and IIoT security. Experienced in controls engineering, security research and corporate management, he blends deep technical knowledge with business experience. He has led international standards development, and created the Tofino Firewall, the world’s most widely deployed ICS security appliance. Today he leads aDolus Inc.

Tim Conway
Tim serves as the Technical Director - ICS and SCADA programs at SANS, and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Additionally, performing contract and consulting work in the areas of ICS cyber security with a focus on energy environments. A recognized leader in CIP operations, he formerly served as the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), and was responsible for
Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric.
Recognizing the need for ICS focused cyber security training throughout critical infrastructure environments and an increased need for NERC CIP hands on training, Tim authored and instructs the ICS curriculums newest course ICS456 - Essentials for NERC Critical Infrastructure Protection.
Outside of SANS, Tim continues to perform contract and consulting work in the areas of ICS cyber security with a focus on the energy sector.

Matan Dobrushin
Matan is a cyber security researcher with military leadership experience in a cyber security unit.

Monta Elkins @MontaElkins
The award-winning Monta Elkins, considered by his friends to be the Chuck Norris of ICS Cybersecurity, is a security researcher/consultant and SANS ICS instructor. He has presented at more cyber security conferences than he can remember including Defcon, CS3STHLM, ICSJWG... His talk is sponsored by TDI Technologies Inc.

Yoav Flint Rosenfeld @YoavfFlint
With over 20 years of experience in cyber security as a pen tester, security consultant, SOC manager and threat intelligence manager, Yoav heads Otorio services (penetration tests, incident response, SOC, threat intelligence) with specific industrial focus. He created and managed the first Meetup in Israel for cyber analysts.

Dave Foose @davefoose
David Foose is the Security Solutions Program Manager at Emerson Automation Solutions, Power & Water Solutions. In this role, David is responsible for setting the direction of Emerson’s security solutions business including establishing product and service roadmaps, providing sales support and leading the Ovation Cyber Emergency Response Team. David frequently presents on the topics of cybersecurity and industrial control system protections at industry conferences and trade shows and is active in the threat intelligence community ensuring Emerson is able to provide timely notification to its user base regarding current threats and malware campaigns. Previously, David was the Ovation Security Technology Development Manager responsible for the overall design, development and implementation of security controls for the Ovation control system as well as Emerson’s Power and Water Cybersecurity Suite. Prior to joining Emerson in 2008, David worked for more than 10 years in a commercial IT environment as a network administrator responsible for security hardware and software evaluation. David’s educational background includes a Bachelor’s degree complemented by a Master’s of Science degree in IT Security and Assurance from Robert Morris University along with several industry certifications focused on the security and defense of Industrial Control Systems. David resides in Gibsonia, PA with his wife Jaime and two daughters Paige and Piper.

Brent Foster
Brent started his professional career at a law firm where his clients included a number of privately held asset owners along the Gulf Coast. After looking around the office and realizing what he had to look forward to... he went in house at Third Coast, an asset owner providing toll manufacturing services to the chemical industry. Shortly after coming on board, he became responsible for their IT & OT security in addition to legal and tax. He founded Extensible Security in order to focus on ICS security, but still does some legal and tax work for long time clients.

Sarah G. Freeman
Sarah Freeman is a cyber security analyst at INL.

Michael Hoffman
Michael Hoffman holds a global role in Shell as a Principle ICS Security SME and has over 19 years of experience between ICS Security, Controls and Automation, and Instrumentation. He is currently enrolled in the STI MSISE program and holds over 9 GIAC certifications.

Adam S. Lee
Adam S. Lee is Dominion Energy's vice president and chief security officer. He directs the development and implementation of corporate security strategy and policies which protect the company’s physical and cyber assets, valued at $100 billion and spanning 18 states. He is Dominion Energy’s security and intelligence liaison with the U.S. government and federal, state, and local law enforcement agencies. Lee joined the company in this role in 2018.
Before joining Dominion Energy, Lee served as Special Agent in Charge of the Federal Bureau of Investigation’s Richmond Division. In 2018, he retired from the FBI after a career spanning 22 years in counter-terrorism, counter-intelligence, and cyber investigations and operations, in addition to specializing in cases involving political and governmental corruption, the Foreign Corrupt Practices Act, and antitrust violations. Lee previously served as the FBI’s executive over its national Public Corruption Program, overseeing the FBI’s most sensitive criminal investigations involving elected and appointed officials across the spectrum of government.

Robert M. Lee @robertmlee
Robert is a recognized pioneer in the industrial security incident response and threat intelligence community. He gained his start in security as a U.S. Air Force Cyber Warfare Operations Officer tasked to the National Security Agency where he built a first-of-its-kind mission identifying and analyzing national threats to industrial infrastructure. He went on to build the industrial community’s first dedicated monitoring and incident response class at the SANS Institute (ICS515) and the industry recognized cyber threat intelligence course (FOR578).

Justin Opatrny
Justin Opatrny has over 18 years of IT and cyber security experience at General Mills, Inc. with the last
seven years focused as the Cyber Security Engineering Manager responsible for designing and building
cyber security solutions for ICS and OT systems globally.

Sanford Rice
Sanford Rice is a Control System and SCADA engineer with 25 years of experience in Oil and Gas with the
last 10 years focused on ICS cyber security and system resiliency. Sanford is the lead ICS architect for the
Atmos Pipeline Texas division of Atmos Energy based in Dallas, Texas.

Gary Seifert
Gary D. Seifert, P.E., E.E. is a seasoned electrical engineer rich in experiences as a senior program
manager and systems engineer concentrating on renewable energy integration, resource assessment,
SCADA cyber security, high reliability power and control systems, military power system integration,
IEEE 1547 Standard development, and micro-grid integration. Gary has been a private consultant since
2014 and is providing engineering consulting support to international and US government teams
(including DARPA RADICS and DOE’s CYOTE) and specializes in ICS Cyber security, SCADA systems
assessment and design, microgrids and renewable energy integration. He was at the OSIsoft federal
systems group for two years and was at the Idaho National Laboratory for 31+ years providing design,
SCADA Cyber testbed, systems integration and energy research in Idaho Falls, Idaho.
Mr. Seifert has managed technical tasks for a multitude of federal and military agencies and installed
total energy and water systems and incorporated renewable energy at high levels of penetration while
preserving performance. He has been a leader in the development of wind and solar energy and brings
that expertise to a new generation of smart microgrid integration while preserving and enhancing
reliability and availability.

Joe Slowik @jfslowik
Joe Slowik currently hunts ICS adversaries for Dragos. Previously he worked at Los Alamos National
Laboratory and served as a US Navy Officer.

Steve Winterfeld
Steve Winterfeld is the Advisory CISO at Akamai. He has served as Director of Incident Response and
Threat Intelligence at Charles Schwab, Director of Cybersecurity for Nordstrom and CISO for Nordstrom
bank. Additionally, he has supported multiple DOD and government agencies such as NERC while at
Northrop Grumman. He has spent over 10 years building security programs to protect companies and
their customers. Steve has published a book on Cyber Warfare and holds CISSP, ITIL and PMP
certifications.

Tim Yardley
Tim Yardley is a Principal Research Scientist and Associate Director at the Information Trust Institute
(ITI). His primary duties focus on defining the strategic vision and direction for fundamental and applied
research in emerging technology throughout the ITI portfolio. Mr. Yardley works in various research
areas and also acts as the industry lead in structuring research partnerships with ITI. His research is focused on trustworthiness and resiliency, particularly with regards to cybersecurity in critical infrastructure such as the electric power grid. Mr. Yardley is the Principle Investigator in a wide variety of projects, totaling over $40M in cutting-edge research. The DARPA RADICS program funds one of Mr. Yardley’s core thrusts, focusing on enabling the verification and validation of mission-critical cybersecurity tools in the electric power grid via testbed technology. Overall, Mr. Yardley’s work is focused on advancing the state of cyber security protection and mitigation methods such that they provide actionable intelligence and guidance on what to do with the information.