Thursday, March 4 – all times in Eastern Standard Time (UTC – 5)	
10:00 – 10:15 am	*Opening Remarks* **Robert M. Lee** @RobertMLee, Senior Instructor, SANS Institute **Tim Conway,** Certified Instructor, SANS Institute
10:15 – 11:00 am	**Keynote: 2020 Year in Review** **Robert M. Lee** @RobertMLee, CEO and co-founder, Dragos
11:00 – 11:15 am	**Break**
11:15 – 11:45 am	**Correlating Alarm and System Events for Security Monitoring in ICS Environments** **Uduak Daniels**, Cybersecurity Specialist, Saudi Aramco The objective of this presentation is to highlight the benefits of leveraging process alarm events for security event correlation, significantly improving both the detection and analysis of relationships between events generated from various industrial control systems (ICS). Currently some asset owners have currently implemented Security Information and Event Management (SIEM) technologies in their ICS environments, with varying returns on investment (ROI). A significant challenge with this technology implementation in ICS environments has been the lack of the inclusion of process automation application logs in the security event correlation effort. This lack of ICS system event visibility slows down the security event correlation process, and presents inefficient alerting increasing the time required for analysis and response. The collection, normalization and correlation of application, system, and network logs have been the foundation of most if not all IT SIEM implementations. Unfortunately, in most ICS SIEM implementations, these benefits have been missed due to the lack of clearly defined logging requirements for process automation systems and applications. Fortunately, Open Platform Communication (OPC), as part of its specification, defines alarms and events that contain a wealth of ICS event information, which when carefully correlated with operating system and/or network device events, can be leveraged for event correlation to address the defined inefficiencies.
11:50 – 12:20 pm	

	Exorcising the Ghost in the Machine: A Critical Evaluation of ICS-Focused Supply Chain Attacks **Joe Slowik** @jfslowik, Senior Threat Researcher, DomainTools Supply chain attacks appear to be among the most concerning threat vectors for many organizations - yet most descriptions of such threats appear to either ignore or be ignorant of the steps required to actualize an implant for offensive purposes. First, this talk will work to disambiguate two distinct attack types often lumped together: software/hardware supply chain attacks via modification, and trusted third-party/vendor/contractor compromise to facilitate access to supported organizations. This distinction is very important and looking at these two event types as event equivalents is deeply confusing. After setting the groundwork for discussion, physical or software supply chain attack (e.g., modification of device hardware, firmware, "adding a rice-sized chip" to a motherboard, or altering source code) functionality and execution will be analyzed in detail: how these attacks work in practice, and what actions and accesses are required to make these attacks useful. Based on this exploration, defenders will gain insight into the true scope and meaning of such attacks, specifically: how such attacks are overhyped; why such attacks are extremely difficult to execute; and how multiple defensive measures exist to detect or mitigate against such attacks. From this analysis, defenders and information security stakeholders will learn how to precisely orient the risk of supply chain compromise events and exorcise the persistent threat of a “ghost in the machine”.
12:25 – 12:55 pm	**2021 is CCE's Coming Out Year** **Andy Bochman** @andybochman, Grid Strategist, Idaho National Lab More than a decade ago, legendary SANS ICS Security program leader Mike Assante began thinking that no matter what cyber tools an organization deployed, and no matter how well it ran its security operations, adaptive, well-resourced attackers could and would get through the best defenses, almost always undetected. Mike didn't like this one bit and pledged to do something about it. In recent years, his former colleagues at INL have brought the methodology he pioneered, Consequence-driven Cyber-informed Engineering, to maturity with support from DOE, DoD and DHS. And they've used it to engineer out much of the cyber risk at selected critical infrastructure and military sites. Now with Countering Cyber Sabotage (the first CCE book) just published, and with the CCE @ Scale partner program ramping up throughout 2021, INL is ready to give the SANS ICS community a closer look at CCE than ever before.
1:00 – 2:00 pm	**Lunch**
2:00 – 3:00 pm	**A CISO View on the Journey of OT/ICS Cybersecurity**

	Moderator: Dr. Paul Stockton @paulnstockton, Co-Chair for the Department of Energy's subcommittee on Grid Resilience for National Security, Former Assistant Secretary of Defense for Homeland Defense **Panelists: Annessa O. McKenzie,** VP of Supply Chain & Chief Security Officer, Calpine **Dr. Reem F. Al-Shammari,** CISO of Kuwait Oil Company, Kuwait Oil Company **Mikhail Y. Falkovich**, Director IT at Con Edison **Thomas L. Kuczynski**, VP of IT at DC Water & President at Blue Drop, LLC In this moderated panel discussion three CISOs representing asset owner and operators from different sectors will talk about their companies' journey into building an OT/ICS cybersecurity program covering people, process, and technology. They will take questions on the challenges they see, the role and responsibilities of different parts of the value chain, the wins they've had, and the lessons learned not only in communicating to practitioners but also in educating their boards of directors and other executives. Their firsthand lessons learned will offer actionable guidance to attendees and openly discuss the victories and hardships they've faced.
3:05 – 3:35 pm	**Are you under ATT&CK? How to gain OT visibility necessary for MITRE ATT&CK for ICS coverage.** **Mike Hoffman** @ICSSecurityGeek, Principle Industrial Consultant, Dragos Asset owners and operators are faced with the difficult challenge of adequate network visibility, host log visibility, and ICS device log visibility. This talk will pull together Crown Jewel Analysis and Collection Management Framework concepts to help asset owners and operators focus their monitoring strategy to align with known adversarial tactics and techniques.
3:40 – 3:55 pm	**Break**
3:55 – 4:25 pm	**A tale of two wireless RTUS – sinking titanic and ransoming it.** **Ron Brash** @ron_brash, Director of Cyber Security Insights, Verve Industrial Protection As a technical follow up to my SANS oil & gas session – tale of the lost RTUs, I am going to discuss how a Software Bill of Materials (SBOM) for two commonly used cellular Remote Terminal Units (RTUs) resulted in disclosures using merely their firmware to guide a research process to "sink the titanic". But! Why stop there? Well, recently, there has been some small-scale ransomware attacks targeting relatively commodity Network Area Storage (NAS) devices such as those by QNAP or NetGear, and so I thought it would be fitting to see how a ransomware strategy plays into a threat scenario with often directly connected remote devices

	often seen on Shodan. Using the same target devices, I will use their "sinking" to my advantage, and leverage that information to build malicious firmware, access functionality on hardware using a low-cost probe/logic analyzer and look towards the future – ransoming an embedded ICS device. It may not be a completely greenfield strategy, but it might be among the first to be explored in a public scenario. Attendees should walk away with an understanding of: * How the research target was selected, and how a SBOM lead to this further research * How to scope hardware and begin the process using a scope or serial adapter to find an entrance * How firmware was created and uploaded to the research targets * How ransoming is a definitive possibility when dealing with embedded systems * And some observations about reducing risks in this scenario for OEMs and & asset owners
4:30 – 5:00 pm	**Future Outlook is a bit Cloudy** **David Foose** @DaveFoose, Ovation Security Program Manager, Emerson Love it or Hate it, organizations are moving more of their infrastructure outside their physical control. These same organizations are looking towards their operational environments to see similar benefits in both cost and efficiencies. From diagnostics, control centers, to full SCADA in the cloud, we will explore actual steps in installations entities have been implementing. We will go over what has worked, what has not been realized, and what trends we are seeing as we digitally transform our plants.
5:00 – 5:15 pm	**Break**
5:15 – 5:45 pm	**Lurking Beneath the Surface... Uncovering Hidden Components in ICS Software** **Eric Byres** @ICS_Secure, P.Eng, ISA Fellow, CEO, aDolus Technology inc Today's ICS software is never written from scratch. Vendors focus development resources on core competencies and prefer to buy (rather than build) components available off the shelf, such as license managers, installers, and cryptographic libraries. This strategy, while efficient in terms of development effort, entwines the vendor's security posture with multiple suppliers and open source projects. Ultimately, it makes it difficult to know what exactly is included in a package. This lack of component visibility directly impacts asset owner vulnerability management processes. For example, in 2019, ICS were exposed to critical vulnerabilities found in the VxWorks TCP Stack. Vendors had used this component in their ICS products, but most operators were unaware of this. Searching vulnerability databases didn't reveal the problem as the vulnerabilities were listed under WindRiver products rather than ICS vendor products.

	Automated vulnerability tools using NVD lists failed to detect this issue in deployed products.
5:50 – 6:20 pm	**Lessons from Two Years of ICS Security Assessments** **Don C. Weber** @cutaway, Principal Consultant and Founder, Cutaway Security, LLC ICS environments are under the gun and under the spotlight. Organizations are working hard to determine the best methods for improving security and asking vendors to help them. This presentation will cover two years of ICS security assessments, conducted by Cutaway Security, in a variety of industrial sectors. We will breakdown our assessment process and the common issues it identified during these engagements. Our goal is to provide attendees with an understanding of the common problems that happen before, during, and after an assessment.
6:20 – 6:30 pm	Day 1 Wrap-Up

Thursday, March 4 – all times in Eastern Standard Time (UTC – 5)	
9:00 – 9:15 pm	*Intros* **Peter Jackson**, Instructor, SANS Institute
9:15 – 9:45 pm	**The Collision of ICS Safety and Security in 2021** **Peter Jackson**, Engineering Manager – Cyber, SGS ECL The history of safety in industrial control systems (ICS) is rich. We have learnt over decades to build in safety by design as part of good engineering practice. Security in ICS is less mature but there are good things happening with owner/operators, consultants, vendors, and standards to move this forward and grow in maturity. With more than three years since the first known safety instrumented system (SIS) malware (TRISIS/TRITON), this talk is a look back to where we've come from, a check-in on where we're at and a look forward to the future of safety and security in ICS. It should be easy to prioritize safety and security when they align – why don't we? And what about when they don't align?
9:50 – 10:20 pm	**Re-evaluating ICS/OT Procurement Language** **Sarah Freeman**, ICS Cybersecurity Analyst, Idaho National Laboratory As demonstrated during the events of 2020, supply chains for almost every product and service have become globalized. Additionally, in spite of several efforts to improve the robustness of supply chain lines, COVID-19 has

	demonstrated the "failure of imagination" of supply chain engineers to identify potential areas of weakness. In December 2020, the cybersecurity community experienced the SolarWinds hack and, although not the first, the implications of this supply chain attack will likely ripple for years to come. In spite of these events, however, a substantial foundation for supply chain security exists. Previous research by DHS, Idaho National Laboratory and SANS, for example, laid the groundwork by defining base language for procuring secure software and hardware for ICS. DHS's Cyber Security Procurement Language for Control Systems (2009) and SANS Application Security Procurement Language (2009) serve as a starting point for vendor and asset owner discussions on product security. Still, as supply chain attacks have continued to evolve since 2009, it is necessary to reevaluate these efforts and their language to identify and address gaps in supply chain security. This presentation is intended to provide the audience with an overview of relevant federal and private sector efforts to define a secure supply chain (e.g., Section 889 of NDAA 2019, Securing the United States Bulk-Power System (EO 13920), etc.) highlight key supply chain attacks (e.g., Havex, NotPetya, RubyGems, etc.), and identify gaps in existing approaches. Some recommendations for product end-users will be identified. This talk is not intended to be prescriptive, but to highlight areas for additional discussions and research.
10:25 pm – 10:55 pm	**E-MIMICS: Extended Malware in Modern ICS** **Seth Enoka** @seth_enoka, Senior Industrial Incident Responder, Dragos In 2017, the Dragos team looked at public data sources such as VirusTotal to identify malware and (in many cases) legitimate ICS files within those databases to encourage a discussion around security in modern ICS. Three years later, there is a wealth of new information available in public datasets that you can again use to immediately inform your cyber security postures and strategies. This presentation relates to research conducted recently into ICS-targeted malware, using a much larger dataset from VirusTotal and covering a longer timeframe than the original Project MIMICS. Several new activity groups and adversaries have been identified since 2017, many of which are known to specifically target ICS and OT environments aiming to cause loss of view, loss of control, or loss of life. So, it's time to revisit this research, determine if the findings still hold true, and develop a strategy for mitigating the risks of malware in modern ICS.
11:00 – 11:30 pm	**Secure System Engineering - Tales from Rail Industry** **Saravanakumar Gunaseelan**, Cybersecurity Lead, TfNSW Increasing attacks on industrial control system (ICS) environment have forced communities to invest significant efforts to uplift their cyber defence capabilities. However, the nature of ICS operations brings along inherent limitations to the extent of security controls that could be utilized or enforced. It implies that security should be weaved in as part of the engineering design for ICS. This presentation walks through an approach to factor in security as part of system

	engineering, based on lessons learnt during implementation of a complex ICS infrastructure. It discusses cybersecurity assurance regime that should be considered across each phase of system engineering, to achieve an operationally reliable, safe and efficient system. It also exemplifies how IEC 62443 standards could be leveraged for such complex engagements.
11:30 – 11:45 pm	Wrap-Up

Day 2

Friday, March 5 – all times in Eastern Standard Time (UTC – 5)	
4:00 – 4:15 am	*Intros* **Kai Thomsen** @kaithomsen, Certified Instructor, SANS Institute
4:15 – 4:45 am	**DX Security of Factory Automation** **Hiroshi Sasaki**, CISSP Special Expert, Industrial Cyber Security Center of Excellence (ICSCoE) Challenges and good practices of ICS security of Factory Automation (FA) is introduced. Recently, almost all Japanese manufacturers are going to promote the convergence of IT and FA system, accelerated by COVID-19 situation. However, they struggle to move forward due to a lot of challenges such as the flat network architecture of FA system, lack of awareness of OT people, lack of process of incident handling etc. I have supported several manufacturers in Japan by holding the OT security workshop which makes the executive, IT and OT people understand each other of the challenges and consider how to promote DX in Factory Automation.
4:50 – 5:20 am	**TTPs from ICS cyber range** **Salimah Liyakkathali,** CyberSecurity Technology Engineer, iTrust (Centre for Research in Cybersecurity), Singapore University of Technology & Design iTrust is a host of several world-class testbeds such as Secure Water Treatment, Water Distribution and Electric Power and Intelligent Control grid. Annually, iTrust organizes an ICS cyber range, Critical infrastructure Security Showdown (CISS), where the red teams and blue teams were invited to attack these testbeds and detect those attacks. Last year, CISS was moved to an online platform and this has allowed more participants from varies countries from different background. The red teams were given a unique opportunity to attack a realistic water treatment plant to cause process anomalies. This has given us insights to understand composite Tactics, Techniques and Procedures (TTPs) that can be used for enhanced Operation Security (OpSec). Hence, this presentation focuses

	on the (TTPs) observed during the event. Attack scenarios and examples are shared with the community that consists of the attacks that lead to disruption of the operation.
5:25 – 5:40 am	**Break**
5:45 – 6:15 am	**Cybersecurity FAT/SAT Testing – Pitfalls and Wins** **Dieter Sarrazyn,** Freelance SCADA/ICS/OT Security Consultant, Secudea Everybody knows and understands that factory acceptance testing and site acceptance testing must be done to make sure a project or system has been implemented as agreed within the design specifications. However, as cybersecurity is more and more important, cybersecurity testing during fat and sat test cycles should be performed as well. However, this most of the times not performed due to various reasons. Or when it is done, it is not done extensively enough to cover everything. In this presentation the various pitfalls and wins of cybersecurity fat/sat testing will be explained further. After this presentation you will better understand the why, what, when, how and receive information to be able to start a scada vendor cybersecurity validation process.
6:20 –6:50 am	**ICS Pentesting During COVID: Lessons Learned from Pentesting Operational Environments Halfway Around the World** **Chris Robinson**, ICS Security Principal Consultant, Blackberry Performing a penetration test of any environment has inherent risks but those risks increase in an ICS environment with safety and reliability requirements. On top of that, performing a penetration test of an ICS environment from halfway around the world presents some challenges. This presentation will focus on some of the lessons learned from performing a remote penetration test on two operational environments.
6:55 – 7:25 am	**Engineering for Resilience** **Johannes Braams**, Senior advisor ICS Cyber Security, Royal HaskoningDHV Complex systems, such as Tunnel systems, are usually designed and built using Systems Engineering techniques. As the Tunnel Technical Installations tend to encompass several computer and PLC based systems, all interconnected via networks, securing them is vital for the safe and secure operation of the tunnel during it's lifecycle. This talk discusses how we can take cybersecurity into account during the various stages of the requirements formulation, design-, build-, test- and exploitation-stages of these systems.

7:30 – 7:45 am	Wrap- Up
7:45 – 8:00 am	**Break**
8:00 – 8:45 am	**SANS ICS Awards:** **Assante Scholars Recognition** Alan Paller, Founder, SANS Institute **CTF Winners Announcement** Robert M. Lee @RobertMLee, Senior Instructor, SANS Institute **ICS Security Lifetime Achievement Award Presentation** Tim Conway, Certified Instructor, SANS Institute
8:45 – 9:00 am	*Opening Remarks* **Robert M. Lee** @RobertMLee, Senior Instructor, SANS Institute **Tim Conway,** Certified Instructor, SANS Institute
9:00 – 9:45 am	**Keynote** **Anne Neuberger**, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology on the National Security Council
9:45 – 10:00 am	**Break/Transition to Vendor Track**
10:00 – 10:30 am	**ARMOR for OT Security Leaders** **Jason Christopher** @jdchristopher**,** Certified Instructor, SANS Institute As OT security leaders, we need to be experts on ICS technology trends, cyber security threats, and process engineering impacts—all while managing daily alerts, cultural silos, and disparate resources from our IT-centric peers. The real-world implications can be painful. To minimize that pain, leaders should put on some ARMOR, or Augmented Risk Management for Operational Resilience. Building on the concepts from the 2020 DISC-SANS presentation "The ICS Security Crucible," this talk deep-dive into the programmatic elements needed to link OT security to other business objectives. This ARMOR can be adapted to any industrial organization, regardless of size or sector, as presented in several use cases from real industry examples. Similar programs are already used in mature aspects of industrial organizations, including safety and finance, to secure budgets, track progress, and highlight concerns to executives and boards. As OT security continues to mature, leaders will need to tackle difficult business-level topics, beyond their daily tasks, to make meaningful changes. While not easy, ARMOR will help. So suit up and get ready for battle!

10:35 – 11:05 am	**The SolarWinds Hack Can Affect Control Systems - what can be done** **Joe Weiss,** Managing Partner, Applied Control Solutions A highly sophisticated Russian Intelligence group has compromised the SolarWinds Orion platform. The SolarWinds advisories and webinars have focused on the IT networks, network visibility, and data exfiltration/compromise. However, SolarWinds is also used to directly monitor and CONTROL SNMP devices including building power and cooling systems used in control centers, data centers, laboratories, Ethernet OT network switches etc. The control system issues are not being adequately addressed. The presentation will address the control system issues and possible long-term control system fixes.
11:10 – 11:40 am	**Unit Operations for ICS security professionals (one big and expensive "Lego")** **Oscar J. Delgado-Melo** @lijantropique, Process Engineer, ICS Student ICS security teams usually include security professionals and operations personnel (i.e., engineers, operators, and technicians) with diverse and particular backgrounds. Effective team communication requires some "common ground" where Operations personnel understand basic network concepts (e.g., data flow, network areas, subnets), and security professionals understand basic process concepts. While it is not mandatory to become Process Engineers (PE), security professionals will benefit from a refresher of how a PE study a new process and which tools they use.
11:45 am –12:00 pm	**Break**
12:00 – 12:30 pm	**Cyber-Physical Safety Systems for Water Utilities** **Andrew Hildick-Smith**, Principal, OT Sec, LLC **Gus Serino**, Principal ICS Security Consultant, Dragos Anyone responsible for the reliable, safe, and cyber-secure operation of a water utility should assume they will be breached at some point. If the adversary is targeting the control system, it is likely that they can find a way in. If they spend the time to fully understand the system and its physics, they may also find a way to physically damage the water infrastructure. A core goal of every water utility is to maintain basic service. Armed with a manual operations plan and an incident response plan, a utility that is dealt a severe cyber blow can maintain service and minimize recovery time, as long as they can prevent physical damage to their system. This talk will discuss operational vulnerabilities in water systems that could lead

	to physical infrastructure damage. It will then present possible cyber-physical safety systems designed to mitigate the risk of cyber-attacks leading to physical damage. Where process response is slow enough, out-of-band monitoring can provide protection. The talk will close with advice on how to initiate and lead a similar program in your utility. Network-independent cyber-physical safety systems are similar to equipment protection systems but are considered safety systems because of their ultimate role in protecting public health. Important advantages of this approach include: system retrofitting that provides an element of robust cyber security and operator error protection, low cost opportunities, and solutions that can be designed and implemented by in-house staff without cyber security skills.
12:35 pm – 1:05 pm	**Building Cyber Security in the Water and Wastewater Industry** **Kenneth G. Crowther**, Product Security Leader, Xylem Inc **Estelle Feider-Blazer**, Strategy and Market Analyst , Xylem Inc The water and wastewater sector is moving towards digitization due to the millions of dollars of savings derived from remote monitoring, predictive maintenance, and improved control Digitization of water and wastewater infrastructure can potentially help resolve problems of access to clean water, sanitation, and sustainability if we can find the right partnership model to build security in while controlling costs. However, due to the highly distributed nature of water and wastewater operations (municipal treatment, industrial wastewater treatment, agricultural, commercial buildings, etc.), the smaller average size of operating companies, and the cost constraints, the emerging technology and architecture is increasingly appearing more like an internet of things than traditional industrial control systems (ICS) following a Purdue model-type segmentation. A survey by BRIDGE Energy Group of over 20,000 water and wastewater utility employees showed that cyber threats are among their top fears of what could adversely impact operations, which threatens to slow the acquisition of digital technologies that could improve maintenance cycles and make water more accessible. Historically in the water and wastewater sector, security of operational technology (OT) has relied on preventing network connections between control operations and enterprise networks – the “air-gap.” However, now the air-gap is being bridged by new digital solutions that connect directly to mobile devices or cloud-based analytic platforms to improve plant performance. Traditional information technology (IT) cybersecurity measures cannot be used due to the mixture of new and legacy equipment and a lack of network visibility present in the water and wastewater industrial space. This is a unique opportunity for ICS security community to expand security guidance for a high variety of architectures and to contribute to processes for delivering those technologies as they emerge. This presentation delves into the threat landscape, threat actors, and solution horizon for cyber security in the water and wastewater sector. We provide an overview of cyber attacks against utilities in the water and wastewater sector,

	discuss the threat actors that are targeting critical infrastructure and the rate at which they are broadening their focus to include water and wastewater systems, and discuss the new hacking techniques that are emerging for exploiting industrial automation and controls systems. We use MITRE ATT&CK for Industrial Control Systems to standardize the descriptions of the most likely tactics and techniques that will be used against water and wastewater industrial automation and control systems. These techniques provide a foundation to prioritize mitigation activities. We show how the responsibility for these mitigations is distributed across the community of product makers, integrators, operators, and maintenance. For example, the product maker must create secure methods for firmware updates, disable-by-default insecure features, enable logging, provide secure deployment guidance, etc. However, the operators need to ensure they have a log collection framework and access to incident response capabilities. We outline a partnership responsibility roadmap that covers the product maker during secure development, the integrator or system operator during secure deployment and installation commissioning, and the operator of the system, as well as addressing mitigations required for system upgrades and maintenance. The desired outcome of this presentation is to discuss cybersecurity priorities based on evidence of actual targeting relevant to the water and wastewater industry and its emerging technologies, and to present a partnership model that describes how a community works together to enable secure digitization of water and wastewater infrastructure.
1:05 –2:00 pm	**Lunch**
2:00 – 2:30 pm	**How to Use Security Architecture to Build a Defensible ICS Network** **Bruce Large**, OT Security Lead, CyberCX In this presentation Bruce will deep-dive into Architecture, which is the first category of Rob M. Lee's Sliding Scale of Cyber Defense paper. The presentation will step through the planning, establishing and upkeep activities relating to cyber security architecture and provide reference materials and worked examples. Bruce will share his experiences and lessons learnt from his time as a Telecommunications Engineer working with SCADA systems and more recently as an OT Cyber Security Specialist. Bruce has racked and stacked, supported, designed, commissioned, and architected solutions and he is keen to bridge the gap from the theoretical to the practical. This presentation will work through Network Security architectures for SCADA and DCS environments.
2:35 – 3:05 pm	**BRIC-ing the Supply Chain: Managing ICS Product Security in a Fragmenting World** **Maggie Morganti**, Product Security Researcher, Schneider Electric

	It is no secret distrust between "cyber superpowers" has led to calls for a fragmented internet, which would allow them to (theoretically) isolate traffic within their borders. However, these goals don't end at the firewall. Digital separation includes supply chain autonomy as well. Global ICS vendors know the challenges this will present from a personnel and production standpoint. But we must also examine what implications this will have on how large vendors manage their security, implement controls, adopt new technology and handle vulnerabilities. Additionally, what new challenges will face independent researchers face and what consequences will this have on coordinated disclosure?
3:10 – 3:40 pm	**Killing Time** **Tim Conway**, Certified Instructor, SANS Institute **Jeff Shearer**, Instructor, SANS Institute
3:45 – 4:00 pm	Day 2 Wrap – Up

Time Zone	Day 1 - Event Hours	Day 2 - Event Hours
Pacific Standard Time (PST) UTC - 8	6:00 am (Thu) - 9:45 pm (Thu)	1:00 am (Fri) - 1:00 pm (Fri)
Central Standard Time (CST) UTC - 6	8:00 am (Thu) - 8:45 pm (Thu)	3:00 am (Fri) - 3:00 pm (Fri)
Eastern Standard Time (EST) UTC - 5	9:00 am (Thu) - 11:45 pm (Thu)	4:00 am (Fri) - 4:00 pm (Fri)
Greenwich Mean Time (GMT) UTC + 0	2:00 pm (Thu) - 4:45 am (Fri)	9:00 am (Fri) - 9:00 pm (Fri)
Central European Time (CET) UTC + 1	3:00 pm (Thu) - 5:45 am (Fri)	10:00 am (Fri) - 10:00 pm (Fri)
India Standard Time (IST) UTC + 5:30	7:30 pm (Thu) - 10:15 am (Fri)	2:30 pm (Fri) - 2:30 am (Sat)
Singapore Time (SGT) UTC + 8	10:00 pm (Thu) - 12:45 pm (Fri)	5:00 pm (Fri) - 5:00 am (Sat)
Japan Standard Time (JST) UTC + 9	11:00 pm (Thu) - 1:45 pm (Fri)	6:00 pm (Fri) - 6:00 am (Sat)
Australian Eastern Daylight Time (AEDT) UTC + 11	1:00 am (Thu) - 3:45 pm (Fri)	8:00 pm (Fri) - 8:00 am (Sat)

Speaker Biographies

Andrew Hildick-Smith
Andrew is an engineer that worked at a large metropolitan water utility for 30 years. He was responsible for the SCADA system for 17 of those years and championed its cyber security. In 2006 he was on the Organizing Committee for the first SANS SCADA Security Summit.

Andrew Bochman
Andy helps decision makers in government and industry made good (or at least better) decisions about their cyber risks and what they can do about them.

Anne Neuberger
Ms. Anne Neuberger is the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology on the National Security Council. Previously, she served as the National Security Agency's (NSA) Director of Cybersecurity, where she led NSA's cybersecurity mission, including emerging technology areas like quantum-resistant cryptography. Prior to this role, Ms. Neuberger led NSA's election security effort and served as Assistant Deputy Director of NSA's Operations Directorate, overseeing foreign intelligence and cybersecurity operations. She also served as NSA's first Chief Risk Officer, Director of NSA's Commercial Solutions Center, Director of the Enduring Security Framework cybersecurity public-private partnership, and the Department of the Navy's Deputy Chief Management Officer. In 2017, Ms. Neuberger was awarded a Presidential Rank Award for her service at the NSA. Before her Government service, Ms. Neuberger was Senior Vice President of Operations at American Stock Transfer and Trust Company, where she directed technology and operations.

Annessa O. McKenzie
Annessa McKenzie joined Calpine Corporation in 2015, and currently serves as VP of Supply Chain and Chief Security Officer, responsible for setting Cyber and Physical security strategies across all functional business units within Calpine as well as the overall strategy for IT Compliance, Business Continuity, Supply Chain and Facilities. Annessa's focus has been establishing long-term investment roadmaps, assessing IT/OT and Operational risk by Business Unit and deploying value-added zero-trust security architectures with compliance in mind across the organization. Annessa has volunteered as the Houston FBI Infragard Power & Utilities Sector Chief since 2015.

Prior to joining Calpine, McKenzie held the role of Chief Information Security Officer at Baker Hughes where she was responsible for a multi-national team focused on cyber-defense, securing digital oilfield operations, security of future oilfield product designs and consulting with Baker Hughes' global oilfield customers; PricewaterhouseCoopers' advisory practice and the U.S. Drug Enforcement Administration HIDTA task force.

McKenzie holds an MBA and a Bachelor's degree from Louisiana State University, as well as CISSP, CRISC and CISA certifications.

Annessa McKenzie was named one of Houston's top millennial women to watch in 2019 by the Houston Chronicle and in 2020 was nominated as Orbie awards' 2020 Houston CIO of the Year

https://www.linkedin.com/in/annessa-mckenzie-mba-cissp-cisa-crisc-4b59b75

Bruce Large
Bruce is the Operational Technology (OT) Cyber Security Lead at CyberCX and he has worked across IT and OT roles in network and system engineering. Bruce is passionate about cyber security architecture and sharing cyber security concepts to the broader technical community. Bruce also considers himself an infrastructure tourist.

Chris Robinson
Chris Robinson graduated from the United States Naval Academy with a B.S. in Computer Science and served over 6 years in the United States Navy. He also earned a M.S. in Computer Science from San Diego State University. Throughout his career, Chris has filled many different IT positions and is currently an ICS Security Principal Consultant for Cylance in Houston, TX where he regularly works on a variety of ICS security projects. By working for an owner/operator and with many clients as a consultant, Chris has learned first-hand the operational constraints and unique requirements for securing ICS environments. Chris teaches ICS410 and is a course author for ICS612.

David Foose
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

Dieter Sarrazyn
Dieter is a freelance OT security expert who working extensively on industrial control system security including more than 10 years in a large electricity generation company. He performs SCADA security assessments, provides assistance in securing SCADA environments and helps customers to manage their suppliers' security through doing security requirements management and security FAT and SAT tests. These activities are always part of a larger program, aimed at reducing business risks.

Don C. Weber
Don C. Weber, the Principal Consultant and Founder of Cutaway Security, LLC, has devoted himself to the field of information security since 2002. Don, a Certified SANS instructor, is currently focused on security research, assessments, and program maturity for operational environments.

Eric Byres
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's led international standards development, and created the Tofino Firewall, the world's most widely deployed ICS security appliance. Today Eric leads aDolus Inc.
Estelle Feider-Blazer

Estelle Feider-Blazer is a Market and Strategy Analyst for Xylem. Previously she has worked as an Acoustic Engineer for the US Navy and a Safety Systems Engineer for Karma Automotive. She holds a MS in Energy Systems Engineering and BS in Mechanical Engineering from the University of Michigan.

Gus Serino
Gus Serino, an Industrial Cybersecurity Consultant at Dragos, is a Professional Engineer (PE) in Control Systems with 22 years in the design, implementation, programming, and security of ICS/OT. He holds a Water Treatment Operators License, several GIAC Certificates, and is a GIAC advisory board member.

Hiroshi Sasaki
Joined McAfee Japan in December 2012 after working for 14 years as a developer of industrial control system. Aiming to foster culture of industrial cyber security, providing enlightenment such as lectures, writing and consulting services.
From May 2016, assigned as a part-time IT Security Officer of Ministry of Economy, Trade and Industry(METI), and from July 2017, assigned as a part-time subject matter expert in the Cyber Technology Laboratory of the Industrial Cyber Security Center of Excellence, supporting the development of the industrial cyber security industry.

Jason Christopher
Jason D. Christopher is the Principal Cyber Risk Advisor for Dragos, Inc. focusing on ICS monitoring technology, threat intelligence, and incident response. Previously he was the Chief Technology Officer for Axio. His experience includes providing technical leadership on security and resilience issues, and the development of technology platforms for security metrics and benchmarking.

Prior to Axio, Jason led the research for cybersecurity metrics and information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cybersecurity capability and risk management at the US Department of Energy, where he managed the Cybersecurity for Energy Delivery Systems Operations program, which included the Cybersecurity Capability Maturity Model and other collaborative efforts.

Joe Slowik
Joe Slowik currently focused on network-based attacks and infrastructure for DomainTools while performing ICS training and consulting for Paralus. Previously, Joe was a threat researcher at Dragos, led incident response operations for Los Alamos National Lab, and worked various cyber missions for the US Navy.

Joe Weiss
Joe Weiss is an expert on instrumentation, controls, and control system cyber security. He authored Protecting Industrial Control Systems from Electronic Threats. He is Managing Director of ISA99, a registered professional engineer in California, and has CISM and CRISC certifications.

Johannes Braams
Johannes Braams is a driven, professional consultant and project manager with more than 5 years of experience in cyber security in ICS and 18 years of experience in business and IT-projects.
He can easily and quickly assimilate new knowledge which is illustrated by getting his GICSP-certificate

within the first year of working in cybersecurity (2015) and supplementing that with his CISSP certification in 2020. Johannes' main focus nowadays is on (cyber)resilience by design as he's convinced that by incorporating requirements on cyber security and cyber resilience into the design face of a project better results can be achieved in the end. It is key to deliver "just enough" security and resilience in order to bring the level of risk down to the level which is required by the customer.
As a project manager Johannes is capable of translating business requirements and wishes into IT. He delivers optimal quality within the boundaries that are set by time and budget. He likes to take the project team on a journey from the conception of the project towards the realization of the results. Meanwhile he makes sure that the right things are done well.
He feels comfortable with complex projects that look like a puzzle at first.

Dr. Kenneth G. Crowther
Dr. Kenneth Crowther is the Product Security Leader (PSL) for Xylem Applied Water Systems. He was PSL for GE Global Research and Principle Engineer at MITRE. He teaches risk management at UVa and Georgetown, holds a PhD in Systems Engineering from UVa, and a BS in Chemical Engineering from BYU.

Maggie Morganti
Maggie Morganti is currently a Product Security Researcher at Schneider Electric. She previously worked researching cybersecurity for power systems at Oak Ridge National lab and as an ICS Threat Intelligence Analyst at FireEye. Maggie is an IEEE member and holds a BS in Intelligence Studies from Mercyhurst University.

Mark Carrigan
Mark Carrigan joined PAS in 2000. As Chief Operating Officer, Mark leads the technology and operations organizations. During his tenure at PAS, Mark has held a variety of positions including Senior Vice President of Technology, Managing Director for the Middle East and Global Sales Leader. An industry veteran, Mark has extensive experience in international business, engineering, sales and technical consulting in the processing industries. Mark holds a Bachelor of Science degree in Mechanical Engineering from the University of Michigan.

Mike Hoffman
Mike Hoffman has over 20 years of experience covering ICS Security, Controls & Automation, and Instrumentation. He is currently a Principal Industrial Consultant at Dragos and has over 11 GIAC certifications. Mike is enrolled in the STI MSISE Program and is working towards becoming a SANS instructor for the ICS curriculum.

Mikhail Y. Falkovich
Mikhail Falkovich is the Director of Information Security for Consolidated Edison Company of New York, Inc., one of the nation's largest investor-owned energy companies, providing electric, gas and steam service for New York City and Westchester County, New York.

Mikhail is a utility industry professional with expertise in information technology, reliability, and cybersecurity efforts. Mikhail has designed secure network infrastructures for control centers and corporate environments and supports the development of Critical Infrastructure Protection (CIP) standards for the utility industry.

Mikhail previously chaired the regional ReliabilityFirst Critical Infrastructure Protection Committee and the New York State Utility Security Working Group. He currently leads several collaborative efforts between the government and utility sector partners to achieve industry wide security benefits.

He is a graduate of Cornell University where he received a bachelor's and a master's degree in Electrical Engineering and built a world champion team of soccer playing robots.

Oscar J. Delgado
Process Engineer with over 13 years of experience in Industrial Plant design. Responsible for the design, analysis, and troubleshooting of equipment, piping, and instruments in critical industries (Oil & Gas, Mining Water & Wastewater treatment plants). Programmer and Pentester by hobby.

Dr. Paul Stockton

As Assistant Secretary of Defense for Homeland Defense from 2009-2013, Dr. Stockton led the development of *DOD's Strategy for Mission Assurance*, which highlighted the foundational importance of the electric system for US security and launched new Defense partnerships with industry and DOE. After leaving office, Dr. Stockton wrote a pioneering NARUC analysis differentiating grid reliability from resilience. He subsequently published a series of studies to help strengthen BPS cyber resilience, including *Resilience for Grid Security Emergencies: Opportunities for Industry-Government Collaboration*. Most recently, his works include *Strengthening the Cyber Resilience of the North American Energy Systems* (the Wilson Center, September 2020) and *Securing the Grid from Supply-Chain Based Attacks* (Idaho National Laboratory, September 2020). Dr. Stockton chairs DOE's advisory subcommittee on Grid Resilience for National Security. He is also a member of DHS' Homeland Security Advisory Council and of NARUC's Emergency Preparedness, Recovery, and Resilience Task Force.

While serving as Assistant Secretary, Dr. Stockton led Defense support for DOE and power companies affected by Superstorm Sandy, including the first-ever use of DOD cargo aircraft to transport restoration assets. Building on that operational experience in *Superstorm Sandy: Implications for Developing a Post-Cyberattack Power Restoration System*, Dr. Stockton supported the ESCC's development of the cyber mutual assistance system and other initiatives to enable power restoration "under fire." He is currently helping the Defense Advanced Research Projects Agency develop new options to meet requests for assistance from BPS entities, including National Guard and US Cyber Command support for blackstart restoration in wide-area outages. He has also helped industry leaders and their government partners build preparedness for emergency operations in the GridEx IV and V Executive Tabletops, serving as the facilitator and helping design the exercises.

Dr. Stockton has frequently testified before US congressional committees and closely collaborates with Members and staff on resilience issues. He has also testified at FERC reliability technical conferences and other meetings, and provided regulatory filings on grid reliability and resilience pricing. Dr. Stockton has served on seven NARUC conference panels on improving metrics and regulatory frameworks. In addition, he has made presentations to the Harvard Electricity Policy Group and other organizations on redesigning wholesale markets to further incentivize resilience investments.

Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. The Department of Homeland Security also awarded Dr. Stockton its Distinguished Public Service Medal. Prior to joining DOD, Dr. Stockton served as a Senior Research Scholar at Stanford's Center for International Security and Cooperation, Associate Provost of the Naval Postgraduate School in Monterey, CA, and as Legislative Assistant for defense and foreign policy for Senator Danial Patrick Moynihan.

Peter Jackson
Peter leads the SGS ECL team of ICS Cyber Security Engineers & Consultants supporting the industrial sector in New Zealand. His background includes control and safety systems experience as a TÜV certified Functional Safety Engineer. Peter teaches the SANS ICS515 Active Defense & Incident Response Course (GRID certification).

Dr. Reem F. Al-Shammari
Dr. Reem is the Information Security Team Leader "i.e. CISO" at Kuwait Oil Company and led significant changes to the maturity of cybersecurity in Energy sector which is closely linked to Kuwait's National CyberSecurity posture.
She is a passionate leader whose valuable contribution to cybersecurity is recognized at national, regional and international levels. She is one of the Co-founders and Board member of Women in CyberSecurity MiddleEast (WiCSME), which has approximately 900 members across the region. Having a number of Academic and Professional degrees such as Engineering, MBA, PhD and Harvard's Business School Executives Program helps her bring a balance of technical and management skills to her current Leadership role as a CISO.
She represents her country in a number of regional and global program and forums, and is recognized as an "Innovator" and "Wild Card" who continues to 'push the envelope' to get to the most optimum outcome on an initiative or a project. In addition to a number of other accolades, Dr. Reem has been ranked #1 at IFSEC Global Top Influencers in Security & Fire 2019 and also awarded the "The Arab CISO of the Year 2019".
She's a very active contributor to Cyber Security Community promoting collaboration via sharing of knowledge "#StrongerTogether", organizing various CyberSecurity related workshops/events and meetups, as well as participating as Judge in various Prestigious Awards as well as a Keynote and speaker in various national, regional, and international forums. She had contributed heavily in Academia including PhD research & MIT Review Article interview. She is also a member in the World Economic Forum's Program "Cyber Resilience in Oil & Gas". She recently did her TEDx Talk on Nov.,2020 under title "Let your passion lead the way" which is now available on TEDx channels.
She is a true inspiration to a number of young Women to strive for more. As she strongly believes that when any Woman rise, we ALL as women rise along with her.

Robert M. Lee
Robert is the CEO and co-founder of Dragos, an ICS/OT cybersecurity technology and services company. He is also a Senior SANS Instructor and Course Author of ICS515 and FOR578.

Ron Brash
Ron Brash is a Director of Cyber Security Insights at Verve Industrial Protection, a critical infrastructure-focused organization that specializes in cyber security products, asset inventorying, vulnerability management, and process integrations/upgrades. Previously, Ron was a manager and SME at a Canadian Cyber Risk Advisory practice based out of Montreal, Quebec. He provided technical knowledge in the aviation security domain, selected ICS/SCADA topics, and advised on a number of technical areas ranging from reverse engineering firmware, risk assessments, security architecture reviews, vendor-integrations, and controls review. Additionally, Ron has an extensive history with oil & gas, was CTO of a technology consultancy providing secure development and security services for industrial devices, co-author at Packt publishing, vulnerability researcher, and was an embedded developer at Tofino Security (A division of Belden) where he worked on several products that are widely deployed today.

Salimah Liyakkathali
Salimah is a Cyber Security Technology Engineer based in academia.
She focuses on the research of critical infrastructure security of Industrial Control Systems (ICS) from an offensive perspective that includes performing cyber-physical attacks, creating attack vectors and validating against defence mechanisms using world-class actual physical testbeds in iTrust such as Secure Water and Treatment (SWaT) plant. She was also involved in international cyber exercises such as NATO CCDCOE crossword 2020 and Critical infrastructure Security Show 2019, 2020

Sarah Freeman
Sarah Freeman is an Industrial Control Systems (ICS) cyber security analyst at Idaho National Laboratory (INL), where she provides U.S. government partners and private sector entities with actionable cyber threat intelligence, developing innovative security solutions for the critical infrastructure within the U.S. She pursues innovative threat analysis and cyber defense approaches.

Saravanakumar Gunaseelan

Saravanakumar has over 10 years of experience in translating security risks into business risks to influence change towards achieving organizational objectives; he holds diversified exposure across multiple domains including Transportation, Energy, Technology & Finance. He has helped organization on several crucial industrial cybersecurity engagements related to cybersecurity governance, architecture and security operations.

Seth Enoka
Seth has over a decade of experience in IT and cybersecurity, having worked on large and complex security incidents and investigations. He has helped large multinational organizations, government agencies, law enforcement, and local businesses to detect, investigate, and remediate cyber incidents and eradicate adversaries from their networks. He is a leader in performing DFIR at scale with geographically diverse teams and systems, as well as building accredited labs and teams to hunt advanced adversaries and activity groups.

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 cybersecurity 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.

Thomas L. Kuczynski
Thomas Kuczynski is the Vice President of Information Technology for the District of Columbia Water and Sewer Authority (DC Water) and the interim President of Blue Drop. Tom joined DC Water in August 2013 and heads up an IT team of 60 individuals and a $20 million budget to develop applications that support customer services and operations, and provide technical support to help employees do their jobs. As Interim President of Blue Drop, Tom leads the team responsible for generating non-ratepayer revenue from various products and services including Bloom, intellectual property and other non-traditional sources at DC Water.

Tom has more than 40 years of experience in utility management and operations including nearly 30 years at Philadelphia Gas Works (PGW) in two separate terms of employment. He was most recently Senior Vice President, Strategic and Information Services for PGW managing Strategic Planning, Enterprise Performance Management, Information Services and Internal Auditing. In his first employment at PGW, he led development efforts for the company's customer information system, credit and collections, automated meter reading and distribution leak tracking.

He has also worked for Pacific Gas & Electric's National Energy Group as Director of Technology Strategic Planning and Architecture, and for Delmarva Power in Wilmington, Delaware where he provided IT Strategic Planning Services to the Energy Supply Group.

Tom is a graduate of La Salle College of Philadelphia and the Executive MBA program at University of Maryland University College.

Uduak Daniels
Uduak Daniels has over 20 years of experience, 15 working in Cybersecurity. He is currently an ICS Cybersecurity Specialist with Saudi Aramco. His professional exposure has cut across multiple industries in North America and MEA. Uduak has participated in a wide variety of information and operational technology cybersecurity assessments, consultancy, design and deployments. In addition, he has led first responder and offensive security engagements. Uduak is a current member of the International Society of Automation (ISA), vice-chair of the Saudi Aramco ICS Cybersecurity Standards Committee, and a technical member representative for SA at ISCI ISASecure. He has a B.S. degree in Computer Science and is a Certified Information Systems Security Professional (CISSP), and a Certified Information Security Manager (CISM).