<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-9:15 am</td>
<td>Welcome &amp; Introductions</td>
</tr>
</tbody>
</table>
| 9:15-10:00 am | **Keynote**  
**Blurring the Lines between IT and OT: Building a Better Defense through Partnership**  
Traditionally, information technology (IT) and operational technology (OT) have had fairly separate roles, dividing the security conversation into confidentiality, integrity, and availability versus safety and reliability. The continuing digitization of all aspects of the oil and gas industry has created an interdependence that many IT and OT professionals still fail to recognize, and the divisive ‘IT versus OT’ conversation has grown stale. Steve Neiers, Chief Information Security Officer for Chevron, discusses the critical need for building partnerships between IT and OT and finding the common ground to more secure and productive operations.  
*Steve Neiers, GM, Information Risk Strategy & Management, Chevron* |
| 10:00-10:20 am| Networking Break                                                                                 |
| 10:20-11:05 am| **Using Augmented Reality to Streamline Design, Construction and Operations of a Major O&G Facility**  
BP has long-established policies and procedures for digital security management and assurance. Like many similar companies, it has been a challenge to align existing facilities and their associated practices to meet these requirements and keep up with the ever-changing security landscape. This presentation highlights some of the challenges and opportunities for BP in the development of a major new facility, in particular:  
• The challenges of securing the IT/OT environment: working with multiple vendors, with existing and new technology.  
• Balancing ease of use and accessibility: Remote access demands in a multi-vendor environment.  
• New technology adoption: Applying LTE, Augmented Reality and other technology to streamline project and operations activities.  
*Steve Mustard (@steve_mustard), Digital Security & Risk Consultant  
Ken Nguyen, Mad Dog 2 IT&S Program Manager, BP* |
| 11:05-11:50 am| **A Look Inside a Real-world O&G Industrial SOC**  
While some may dream of what an Industrial Security Operations Center (SOC) might look like, others Do. Building a fully-functional Industrial SOC for Oil & Gas process control systems from the ground up requires a combination of vision, talent and perseverance. For those who succeed, the paybacks can be high and |
deliver positive effects on key business imperatives to include safety, availability, productivity and profitability.

In this session, hear directly from an O&G asset owner how they overcame technical and organizational hurdles while building their Industrial SOC to gain greater insight into the security posture of their ICS/SCADA systems. What technologies are at work in their security stack? What dashboard views and intelligence do OT SOC analysts have of their process control networks? What KPI’s are tracked? How does the team facilitate asset life-cycle management, incident response, forensics, while also reducing risks to the company’s OT systems?

Beyond just theory and discussion, real practical knowledge, lessons-learned and actual experience gained through their investments will be shared—and also learn why Idaho National Labs (INL) took particular note of this industrial SOC as a model that others might follow.

Daniel R. Crandell GICSP, CISM, CISSP, PMP, Manager of Cyber Security for Critical Infrastructure, Enterprise Products LP

**Lunch Panel**

**Challenges and Successes in Developing the OT Cyber Workforce**

This panel session will examine approaches from industry and government alike to deal with the acute shortage of cyber workers. The enterprise IT sector has known for some time that they don’t have enough skilled people, and when you overlay that with the additional engineering skills required to be a knowledgeable OT cybersecurity worker the problem is magnified many times. The Oil & Gas industry is not immune, and the challenge to find and develop qualified personnel who can manage security risks and safeguard operations are imperatives. Organizations such as Automation Federation, SANS, ISA and others are working with industry and government departments such as NIST to improve the way we build workforce skills, including education and apprenticeship programs.

**Moderator:** Marty Edwards (@ics_marty), Managing Director, Automation Federation

**Panelists:**

Wm. Arthur Conklin (@ArtConklin), PhD, College of Technology, University of Houston

Additional panelists to be announced

**1:15-2:00 pm**

**Talk to be announced**

**2:00-2:45 pm**

**Critical Lessons from TRITON: Protecting Safety Instrumented Systems from Advanced Malware**

In December news of the TRITON attack on the safety system of a critical infrastructure facility sent shockwaves through industrial operators and security practitioners worldwide. TRITON is one of a limited, but quickly growing number of publicly identified malicious software families targeted at industrial control
systems (ICS) and the first known ICS attack to infiltrate a Safety Instrumented Systems (SIS). In this session, Nozomi Networks will share findings and critical lessons learned from the industry’s most extensive analysis of TRITON to date, including: Why we believe the shutdown was an unintended outcome that occurred while the attacker was developing the ability to cause physical damage. What oil and gas operators and security experts should know about a much larger attack plan the hackers likely intended; and Steps you can take now to protect against these types of attacks. To reach these findings, Nozomi Networks Labs conducted extensive analysis of TRITON’s behavior in a live environment with the same model of Triconex controllers and firmware used in the attack. During our study, we discovered how TRITON’s capabilities are based not only on reverse-engineering the TSAA proprietary protocol (the Triconex master/slave protocol for Ethernet networks), but also on extensive research of the device. In the presentation we’ll share how using a combination of static and dynamic analysis, we fully profiled the malware behavior, studying the impacts of several attack scenarios. Using these methods, we were able to develop a tool for detecting an infected controller. Code for this tool will be available on GitHub. TRITON’s sophistication, and its targeting of a SIS, cannot be ignored. It highlights the need for appropriate cybersecurity solutions and greater visibility into the entire industrial process.

Andrea Carcano (@andreacarcano), Co-Founder and Chief Product Officer, Nozomi Networks

2:45-3:05 pm Networking Break

3:05-3:50 pm

**Tactics and Techniques for Threat Hunting in Oil Refineries**
Threat hunting provides an excellent opportunity to boost the current level of defense from both the threat prevention and detection perspective. This talk will highlight lessons learned from threat hunting in Oil Refineries. We will first share the approach we have found to be the most successful based on the architecture of refinery networks. We will then cover open-source tools and techniques we have found to be particularly successful. Along the way, we will share stories from our threat hunts in refinery environments. Attendees will take away tactics and techniques immediately useful for hunting in refinery environments both in production and during a turnaround. This talk covers threat hunting approaches that can be applied to both passive network traffic and collected host logs. We hope attendees also learn about sources of information within process control networks that they had not considered before.

Dan Gunter (@dan_gunter), Principal Threat Analyst, Dragos

3:50-4:35 pm

**Detecting Counterfeit Software in Oil and Gas Control Systems**
Oil and gas companies depend on their vendors to supply valid software and firmware for control system implementation and upgrades. If this chain of trust is compromised, then malicious software can be introduced that alters core system functionality, potentially impacting critical operations and human safety. Unfortunately, there are currently few safeguards in place to protect IIoT and ICS devices against introduction of counterfeit firmware and software.
This is not a hypothetical risk. In 2014, the Dragonfly attack targeted critical infrastructures in North America and Europe by inserting malware into legitimate software bundles available for download on three ICS vendor’s websites. As a result, any asset owner that installed these modified software bundles had their critical systems infected. These attacks highlighted the fact that industry currently needs a robust and universal solution for safeguarding against the counterfeit of firmware/software upgrades.

This talk reports on the results of a US Department of Homeland Security (DHS) funded research project to investigate the viability of using trust anchor technologies for onsite validation of ICS upgrade packages used in the oil and gas sector. The project investigated methods of generating digital fingerprints of both legitimate and suspect firmware via automated agents and then assigning reputational scores to the artefacts. An API and web tool allows end users to incorporate a validation process into their daily operations, ensuring the legitimacy of updated firmware/software, without impeding critical operations.

Eric Byres (@ICS_Secure), P.Eng, ISA Fellow, ICS Secure

4:35-5:20 pm

How’s Our Industrial Cybersecurity? Go Ask the OT Guys

A prominent offshore drilling operation was required to make ICS security changes within their operations and production technology group by a key customer’s demanding ICS security requirements. The journey resulted in a funded project to create a security operations center (SOC) run by the OT team to monitor and manage industrial security across their rigs and fleet of ships that remain continuously at sea. Four years later, the OT team manages their remote access, application and equipment vendors, OT network and assets through their SOC and are in the enviable position of having funding and equipment to keep their operations secure 7x24x365. This case study has applicability to other industries as well. Attendees will gain insight on corporate drivers for improving industrial cybersecurity, how to set and manage OT priorities and still work with stakeholders, what training, funding and assistance may be needed, and how to manage their vendors for operational success. Appropriate for field technicians to management and any range of cybersecurity knowledge.

Katherine Brocklehurst (@kat_brock), Senior Director, Claroty

5:20-7:00 pm

Networking Reception

SANS strives to present the most relevant, timely, and valuable content. As a result, this agenda is subject to change.

Please check back frequently for changes and updates.
Speaker Biographies

Katherine Brocklehurst (@kat_brock), Senior Director, Claroty
Katherine Brocklehurst has been doing cybersecurity since the mid-1990s, working in all OSI layers from packet sniffing and testing early TCP/IP and XNS protocols through web application firewall technology. https://www.linkedin.com/in/katherine-brocklehurst-915a47/ In 2013 she began working with industrial cybersecurity issues at electric utilities in the US and various requirements such as NERC CIP, IEC-62443 and NIST requirements. Through acquisition, she also worked with Belden's Tofino Security appliances.

Andrea Carcano (@andreacarcano), Co-Founder and Chief Product Officer, Nozomi Networks
Nozomi Networks Co-founder and CPO Andrea Carcano is an industrial network security expert. Carcano worked on the European Commission Power Plant Security Program, was a Senior Security Engineer for global oil and gas supermajor Eni, and (through his work at Nozomi) is building a new generation of ICS Security products.

Daniel R. Crandell GICSP, CISM, CISSP, PMP, Manager of Cyber Security for Critical Infrastructure, Enterprise Products LP
Daniel R. Crandell is currently a Manager of cyber security for critical infrastructure within Enterprise Products in Houston, Texas. He is responsible for the security of all operation assets within the company. Some but not all of these assets include the security of over 67 major gas and storage facilities and 65,000 mile of pipeline with Windows and Linux systems, as well as architect and installer of Cisco appliances within its gas and storage facilities. Daniel holds a BS in industrial technologies-computer science from Sam Houston State University and an MS in information systems security from the University of Houston. He is a certified Project Management Professional (PMP), Certified Information Systems Security Professional (CISSP), Cisco Certified Network Professional (CCNP), Cisco Intrusion Detection/Prevention Specialist, and Cisco Certified Firewall Specialist, Certified Information Security Manager (CISM), Global Industrial Control Security Professional (GICSP).

Marty Edwards (@ics_marty), Managing Director, Automation Federation
Marty Edwards, a globally recognized industrial control systems cybersecurity expert and speaker, serves as Managing Director of the Automation Federation. Prior to joining the Automation Federation in mid-2017, Edwards—a 25-year industry veteran—was the longest-serving Director of the US Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Edwards holds a diploma of technology in Process Control and Industrial Automation (magna cum laude) from the British Columbia Institute of Technology (BCIT), and in 2015 received the institute’s Distinguished Alumni Award. In 2016, Edwards was recognized by FCW in its “Federal 100 Awards” as being one of the top IT professionals in the US federal government.

Dan Gunter (@dan_gunter), Principal Threat Analyst, Dragos
Dan Gunter is a Principal Threat Analyst at the industrial cyber security company Dragos, Inc. where he discovers, analyzes and neutralizes threats inside of ICS/SCADA networks. In this capacity, he performs threat hunting, incident response, and malware analysis mission for the industrial community.

Steve Mustard, Digital Security & Risk Consultant
Steve Mustard is an industrial automation consultant with extensive technical and management
experience across multiple sectors. He is a licensed Professional Engineer (PE), ISA Certified Automation Professional® (CAP®), UK registered Chartered Engineer (CEng), European registered Engineer (Eur Ing) and GIAC Global Industrial Cyber Security Professional (GICSP).

A widely recognized expert in industrial cybersecurity and an ISA99 Security Standards Committee member, Mustard played an essential role in the development of the world’s only consensus-based series of industrial cybersecurity standards - ISA/IEC 62443. He also actively participates in cybersecurity working groups formed by the Automation Federation, ISA’s umbrella organization.

Backed by nearly 30 years of software development experience, Mustard specializes in: the development and management of real-time embedded equipment and automation systems; and the integration of real-time processing, decision-support and other disparate systems to improve business processes. He serves as president of National Automation, Inc.

Mustard’s previous and current client list includes: the UK Ministry of Defence; NATO; major utilities, such as Anglian Water Services and Sydney Water Corporation; major oil and gas companies, such as BP, BG Group and Shell; Fortune 500 companies, such as Quintiles Laboratories; and other leading organizations.

**Steve Neiers, General Manager, Information Risk Strategy & Management, Chevron**

Steve Neiers is general manager, Information Risk Strategy & Management (IRSM) for Chevron Corporation’s Information Technology Company. He is responsible for Chevron’s information risk and cybersecurity strategy, implementation and operations. IRSM is headquartered in Houston, TX with locations in San Ramon, Singapore, Manila, Buenos Aires and London.

Steve acquired a Bachelor of Science and a Master’s degree in Geophysics from Saint Louis University. He joined Chevron in 1987, starting with a variety of technical geophysical roles and then moving into leadership positions including managing Chevron’s global network, managing Chevron’s end user computing infrastructure and most recently, assuming the role of CISO for Chevron.

He is a founding board member of the Oil and Natural Gas Information Sharing and Analysis Committee and an active participant with the CEB Information Risk Leadership Council and Information Risk Management Research Board. Steve is also co-chair of the Houston CISO Executive Summit and a member of the Engineering Advisory Board for Houston Baptist University.