<table>
<thead>
<tr>
<th>Time</th>
<th>Session Description</th>
<th>Speaker(s)</th>
</tr>
</thead>
</table>
| 9:00 – 9:15 am | Opening Remarks                            | Rob M Lee, @RobertMLee, SANS Senior Instructor  
Tim Conway, SANS Certified Instructor |
| 9:15 – 10:00 am | Keynote                                     | Q&A with CESER’s Sean Plankey  
Andrew A. Bochman, Senior Grid Strategist, National & Homeland Security  
Sean Plankey, Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy |
|              |                                             | The #2 man at the Federal government’s #1 grid protection organization has agreed to take questions from INL’s senior grid strategist, and the exchange promises to be lively. Here is some of what they’ll hash out: |
|              |                                             | • How Sean’s time at BP helped shape his ICS cyber perspective  
• Executive order 13920 on supply chain security for the bulk power system  
• The Cyberspace Solarium Commission’s recommendations  
• The expanding role of natural gas and distributed energy resources in electricity production and ramifications for grid security and resilience  
• DOE stepping in assist, participate in and guide DHS’ long-running ONG Cyber LOGIIC program  
• A rundown on CESER’s highest impact programs  
• A gaze into the crystal ball at likely future challenges and priorities |
| 10:00 – 10:35 am | Raiders of the lost RTUs, Meters, and Valves | Ron Brash, @ron_brash, Director of Cybersecurity Insights, Verve Industrial Protection |
While IoT/IIoT is everywhere in product catalogues today, Oil & Gas is the original Joe for connected embedded things to fulfill specific purposes such as providing telemetry remotely, or to monitor the health of a well or pipeline. And like many aspects of industrial systems, it was and still is the Wild West of security, updates (or lack of), and deployments where it makes little economic sense to upgrade enforces the fact that producers need to reduce any disruption or security risk for these devices – new or legacy.

With thousands of existing deployments, these devices are often forgotten, and whether for cyber-security or for merely inventory management due to divestment, an effective resource-friendly method is absolutely required to manage these types of systems.

This session walks through several areas (agnostically) with more than 35 years combined experience on:

- How are these devices are often deployed, and in what kinds of environments?
- Discovering technical vulnerabilities/weaknesses and horror-shows buried in these devices
- One approach to successfully enumerate, research, and support candidate devices
- A live demonstration of a hidden surprise with a device obtained from the grey-market
- And how to bring these devices into the fold for inventory/asset management with considerations for cyber-PHAZOPs & vulnerabilities

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:35 – 10:50 am</td>
<td>Break</td>
</tr>
</tbody>
</table>
| 10:50 – 11:25 am | Developing Effective Detection and Defense Strategies Against Activity Groups in Oil & Gas OT using the Diamond Model, Kill Chain, and ATT&CK  
Sergio Caltagirone  
Following best practice is always a good approach when establishing cyber defense policies. But best practices are general guidance and don’t fit every situation. Instead, we can get specific by using the Diamond Model, Kill Chain and ATT&CK frameworks to develop threat-specific detection and defense strategies based on your own threat profile. In this presentation you’ll learn how to build a better threat model, develop a measurably effective detection and defense strategy, and, usually skipped by many, evolve and measure your defenses as the threat environment changes. |
| 11:25 am – 12:00 pm | Preparing for M&A and Onboarding Newly Acquired "Immature" Organizations  
Brent Foster, Founder, Extensible Security |
A drop in oil prices means M&A. Now is the time to get ahead by updating your due diligence process and checklists to support your ICS security objectives. We will look at ways to efficiently get the right information and executive visibility of security issues up front to prevent future pain. Spoiler, the best answer isn't "Go get 3PAO to audit target against (insert framework here)" - few M&A efforts look the same from a ground level operational perspective. Plus, executives will be happy because of the potential impact to price. However, despite your target's best efforts, cost cutting measures negatively impacted ICS security. We will discuss how to utilize the executive buy-in, information gathered, and relationships built during the M&A process to quickly fix critical issues while prioritizing future efforts. The goal is for you to leave able to update your M&A processes, so when the deal is inked there's already explicit (or at least implicit) approval to fix critical issues asap, with other issues roughly tied to your current roadmap.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 – 1:00 pm</td>
<td>Lunch</td>
</tr>
</tbody>
</table>
| 1:00 – 1:35 pm | **Process Vulnerabilities for Refineries: When miliseconds matters**  
  Can Demirel, [@secandit](https://twitter.com/secandit), ICS Cyber Resilience Services Manager, Cyberwise  
  Yusuf Yılmaz Akdemir, Independent Researcher  
  The most of the time security assessments, penetration tests or red teaming activities at Oil &Gas plants focus on core processes and their vulnerabilities. What if attacker leverage supportive processes such as power or steam load shedding, decontamination, pipeline operations etc. During this talk we will walkthrough how to exploit and defend process vulnerabilities with real world scenarios. And also, we will discuss how to create use cases and basic simple defense mechanisms to enable OT-SOC. |
| 1:35 – 1:55 pm | **the “BLACK GOLD”: battle to defend the most treasured assets in world**  
  Anas Faruqui, [@anasf1885](https://twitter.com/anashf1885), OT Cybersecurity Engineer, Aramco  
  You’re a CIO, CISO or IT Security Manager - and you wake up in the middle of the night to a call from your Security Operations Center (SOC) analyst. And suddenly you find that your organization is in the headlines of national newspapers because their core business - operational technology (OT) (an energy/oil producing plant) - was breached.  
  It does not only stop there, but this cyber incident has caused huge environmental disaster and resulted in an explosion due to incorrect mixture of blend or kicked-off emergency shutdown procedure of an production facility.  
  But what if you can know stop all hacker/terrorist before it happens … The recent growth of IP based systems and push for Industrial Revolution 4.0 (IR 4.0) in OT/ICS/SCADA presents a massive opportunity for companies to use these datasets in many meaningful ways for security/network/OT centers. |
As more and more IT and OT integration happen, and we have created this world of hybrid environments infrastructures requiring businesses to address both technological and organizational to comply with government and industry best approach requirements.

This session will SPELL out the plan and show case you how the largest OT implementation of cyber security monitoring in the world happened, enabling us to be ready for any breach in OT.

### 1:55 – 2:30 pm

**Detecting Encrypted Radio Communications Using Universal Hacker Radio**

**Don Weber, @cutaway**, Information Security Consultant, Cutaway Security, LLC

Radio communications are used to establish communications without the need for wired connections. They also provide a degree of safety to personnel supporting dangerous processes. These benefits come with additional risk. Radio communications are externally accessible, meaning that they expose their networks to the public. This presentation will demonstrate how to capture radio communications of 900 MHz radios that are commonly deployed in operational technology (OT) environments. The tool Universal Radio Hacker (URH) will be used to quickly isolate the radio communications, transform those transmissions to data packets, and review the packets for encryption.

### 2:30 – 2:45 pm

**Break**

### 2:45 – 3:20 pm

**What’s cooking? Starting your own DIY Automation and ICS Security Projects**

**Mike Hoffman, @ICSSecurityGeek**, Principle ICS Security Engineer, Shell

Continuous learning and curiosity are both pre-requisites to a successful and rewarding profession in ICS Security. Getting hands-on time with ICS systems is a great way to hone skills and reinforce ideas and concepts gained from SANS courses and time in the field. This presentation will show how you can turn a CLICK PLC and C-more HMI from ICS612 into a safe and secure home coffee roaster -- a project that will help you learn Ladder Logic Programming, PID Control, and ICS protocols. Implemented correctly, you will reap not only the benefits of knowledge gained but also a favorable cup of joe.

### 3:20 – 3:55 pm

**Secure and Safe Operations in the Remote Work Era: COVID-19 and Beyond**

**Mark Carrigan**, Chief Operating Officer, PAS Global, LLC

The executive desire for a shift to remote work within the oil and natural gas industry has been underway for some time. While such a shift is likely to benefit
the broader organization with lower costs and greater safety, it is also not without risks to security and also safety. The COVID-19 pandemic has been a catalyst for increasing the shift to remote work, but it has also exposed weaknesses in processes and tools to support it.

In this session:
- Explore the benefits that remote work can bring to operators, automation engineers, and health & safety personnel
- Examine the tools and process changes required to enable effective, secure, and safe remote operations
- Hear specific recommendations to help guide decisions and investments that enable remote work, while addressing potential security and safety implications
- Review lessons learned on challenges to anticipate, pitfalls to avoid, and best practices for ensuring process safety as well as reducing potential cybersecurity risks

<table>
<thead>
<tr>
<th>3:55 – 4:30 pm</th>
<th>OT IR: Are You Prepared to Respond?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gabriel Agboruche</strong></td>
<td></td>
</tr>
<tr>
<td>There are a plethora of well-defined IT security incident response methodologies, tools and methods, but at times, OT incident response gets left out. When an organization gets breached, the incident affects the IT and OT sides of the organizations. Whether it’s commodity ransomware or a targeted OT payload running wild in control systems, the entirety of the organization should be ready to identify and respond. This presentation will address integral areas that will assist organizations with responding to cybersecurity incidents, it will cover frontline incident responses engagements, and the aim is to provide actionable guidance on improving and fortifying your OT incident response plans.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4:30 – 5:05 pm</th>
<th>A Game Theory Approach for Defending the ICS-SCADA Environment: Win the game using ICS MITRE.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rashed Rabie</strong>, Cyber Threat Hunter, Deloitte &amp; Touche LLP</td>
<td></td>
</tr>
<tr>
<td>This presentation will describe how to map the ICS threat landscape to MITRE ICS ATT&amp;CK. This approach correlates game theory modeling and the ICS ATT&amp;CK framework to identify the security solution to win the game against the adversary.</td>
<td></td>
</tr>
<tr>
<td>The game theory modeling can be summarized as follows: 1) Game – the game-players are in a Simultaneous Static Game; 2) Strategy – the defender's strategy is to determine an optimal security system solution to detect the attacker traffic, and the attacker's strategy is to find the optimal sophistication level to elude the defender's security measurements; 3) Payoff – the model projects the payoff for each player's strategy based on mapping the threats to ICS ATT&amp;CK. The goal will then be to solve the game and find the equilibrium point, which is the best strategy for both players. This equilibrium will occur when the players do not</td>
<td></td>
</tr>
</tbody>
</table>
have any profit deviation in using any other strategy.

In this game, mapping threats to ICS ATT&CK leads to identify the adversaries' sophistication levels. The sophistication then guides the defender for the most effective strategy. When the adversary chooses a low sophistication threat, the defender can use the ICS security measurements and controls, in addition to isolating OT and IT by using Data Diode technology. If the adversary chooses a medium sophistication threat, the defender can use continuous monitoring suction (e.g., Security Operating Center (SOC)) and hunting service for non-target dual-use prolific exploits. When the adversary chooses advanced threats, the defender can apply defense-in-depth solutions such as hardware-based fingerprints detecting using NoiSense techniques. This approach provides stakeholders with broad solutions to help secure the ICS environment.

5:05 – 5:15 pm  Day 1 wrap-up

Speaker Biographies

Anas Faruqui
Anas Faruqui is a Cyber Security Consultant specializing in Industrial Control System for Saudi Aramco, a leading Energy and Oil Company in the world based in Dhrahan, Saudi Arabia. He is also co-founded Zypher Company based in United States dedicated for consulting IT/OT services projects making a positive impact on the banking, financial and manufacture services industry. Over the last ten years Anas has helped various of organizations and companies across the world to help on numerous cyber security projects.

Andy Bochman
Andy Bochman is the Senior Cyber and Energy Strategist at Idaho National Lab. Andy provides strategic guidance on topics at the intersection of critical infrastructure security and resilience to senior U.S. and international government and industry leaders. His career began with the US Air Force, and before joining INL, was in several cybersecurity start-ups, was Global Energy & Utilities Security Lead at IBM, and a Senior Advisor at the Chertoff Group in Washington, DC. A member of the global advisory board for the Control Systems Cyber Security Association International (CS2AI). Andy is on the advisory committee to the SANS Institute and a cybersecurity subject matter expert listed with the U.S. State Department Speakers Bureau. In 2018 his publications include “The Missing Chief Security Officer” (CXO) and “Internet Insecurity: the Brutal Truth” (HBR), and “Supply Chain in the Software Era” (Atlantic Council).

Brent Foster
Brent Foster started his professional career at a law firm where his clients included privately held asset owners along the Gulf Coast. Later he went in-house at an asset owner in the chemical industry, and was responsible for their IT & OT security, legal, and tax. He founded Extensible Security to help secure ICS in small to mid-sized companies.
Can Demirel
Can Demirel has been working as a cyber security professional since 2011. Demirel took part in various security projects in diverse disciplines and sectors such as; finance, e-commerce, government, telco and energy. Recently Demirel has been working on national critical infrastructure security projects mostly focusing on energy. Demirel published/reported zero-day vulnerabilities on well-known products and is also listed on ICS-CERT advisories and participates NATO and EU FP7 energy security workshops. Demirel holds a bachelor’s degree in electrical and electronics engineering. Demirel also leads community activities in Turkey. Such as conference and student bootcamps. Details can be found at: kamp.eksguvenligi.org, ekskonferans.org

Don Weber
Don C. Weber has extensive experience in security management, physical and information technology penetration testing, web assessments, wireless assessments, architecture review, incident response and digital forensics, product research, code review, and security tool development. He is currently focusing on assisting organizations secure their business and Industrial Control System environments thru program reviews, security assessments, penetration testing, and training.

Gabriel Agboruche
Gabriel Agboruche (@ICS_Gabe on Twitter) is a Senior Consultant working in Mandiant’s Security Consulting Services practice, focusing on cybersecurity for industrial control systems and critical infrastructure. Previously working as an Electrical Engineer in the automotive sector, Gabriel transitioned to the security field shortly after the outbreak of the Stuxnet Worm where his commercial nuclear plant environment went through a drastic transformation thrusting him into the midst of the ICS Security field. He began to specialize in commercial Nuclear Plant cybersecurity working as a Security Control Assessor, Security Engineer and Associate Cyber Security Program Manager roles for Orano (formerly Areva) and Westinghouse Electric Company. He also served as a Lead Security Architect for an electrical grid products organization where he specialized in securing microgrid environments for US Federal control system environments. Gabriel currently holds the GSLC, GNFA and GICSP GIAC certifications and is a member if the MiC3 (Michigan Cyber Civilian Core), a group of trained civilian technical experts who individually volunteer to provide rapid response assistance to the State of Michigan in the event of critical cyber incidents.

Mark Carrigan
Mark Carrigan joined PAS in 2000. As Chief Operating Officer & Chief Revenue Officer, Mark leads the technology, operations, and sales 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
Michael Hoffman has over 20 years of experience covering ICS Security, Controls & Automation, and Instrumentation. He is currently a Principle ICS security Engineer and has over 10 GIAC certifications. Michael is enrolled in the STI MSISE Program and is working towards becoming a SANS instructor for ICS curriculum.
Rashed Rabie
Cybersecurity threat hunter and a Ph.D. researcher in electrical engineering and ICS. Published author with IEEE and awarded a Cisco Global Cybersecurity Scholarship. With more than 10 years of working experience in multiple industries, both IT and OT.

Ron Brash
Ron is an experienced speaker, advisor, researcher, and developer with over a decade of experience in industrial control system cyber security. In a previous life, he operated an embedded systems consultancy, was a risk advisor for aerospace, an embedded systems developer for Tofino, and specialized in state-of-the-art packet inspection for critical infrastructure.

Sean Plankey
Prior to joining the Department of Energy, Mr. Plankey served on the National Security Council as the Director for Maritime and Pacific Cybersecurity Policy, where he designed national security policy to address threats from cyberspace. He has also served as the Global Cyber Intelligence Advisor for BP, and as the Deputy Chief Information Officer for U.S. Navy Intelligence.

Mr. Plankey served 13 years as an officer in the U.S. Coast Guard, including a tour as the Offensive Weapons & Tactics Chief at US Cyber Command. During this time, he completed a deployment to Afghanistan, where he was the first U.S. Coast Guard Officer deployed to Afghanistan to conduct offensive cyber operations. He also held the role of Operations Officer and Law Enforcement Boarding Team Leader for two Coast Guard Cutters, one deployed on the Great Lakes and the other in the Bering Sea and Gulf of Alaska.

Mr. Plankey is a graduate of the U.S. Coast Guard Academy and of the University of Pennsylvania’s School of Engineering and Applied Sciences. He holds multiple professional cybersecurity and information technology certifications.

Sergio Caltagirone
Sergio Caltagirone is committed to tracking down hackers and safeguarding civilization. In 9 years with the US Government and 3 years at Microsoft, Sergio has hunted the most sophisticated targeted threats in the world, applying intelligence to protect billions of users while safeguarding civilization through the protection of critical infrastructure and industrial control systems. He co-created the Diamond Model of Intrusion Analysis, helping thousands of others bring more pain to adversaries by strengthening hunters and analysts. He also serves as the Technical Director of the Global Emancipation Network, a non-profit, non-governmental organization (NGO), leading a world-class, all-volunteer team dedicated to ending human trafficking and rescuing victims through data science and analytics, saving tens of millions of lives.