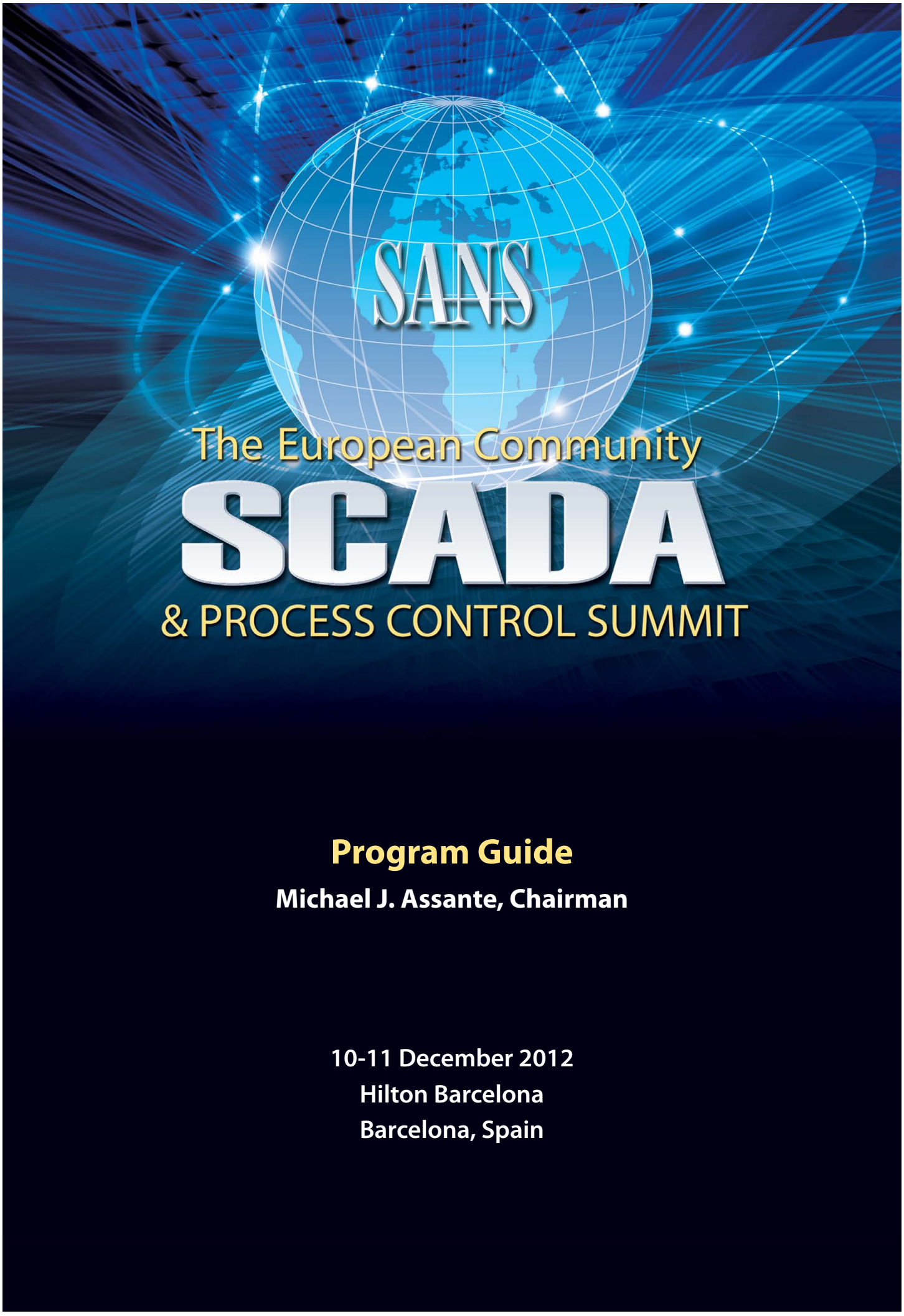


Program Guide

Michael J. Assante, Chairman

10-11 December 2012
Hilton Barcelona
Barcelona, Spain

Summit Agenda

All Summit Sessions will be held in Ramblas B (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euscada12**
An e-mail will be sent out within 5 business days once the presentations are posted.

Monday, 10 December

7:30am - 8:30am

Registration and Morning Coffee

8:30am - 9:00am

Welcome, Introduction & Awards Presentation
European SCADA Security Innovation Awards

Michael J. Assante, President & CEO, National Board of Information Security Examiners; SCADA Summit Chair

The European SCADA Security Innovation Awards recognize the most innovative SCADA projects being done in Europe and the leading innovators in the field. Areas of recognition include:

- Management support in the development of an industry leading security program
- Innovative ICS security implementations
- Community-enhancing research and testing

9:00am – 10:00am

Keynote
Step by Step: The Journey to Secure SCADA Systems

Miguel Chavero Escamilla, CMDS IT Manager, Iberdrola

Chinese philosopher Lao-Tzu said, "A journey of a thousand miles begins with a single step," and so is the case with securing control systems. Four years into their SCADA security initiative, Iberdrola, Spain's largest energy group, is well on their way, but still has a lot of ground to cover. Hear about Iberdrola's challenges, progress and goals.

10:00am - 10:30am

Networking Break & Vendor Expo

10:30am - 11:00am

Expert Briefing
Smart Grid & SCADA: ENISA's Findings

Dr. Konstantinos Moulinos, Expert in Network & Information Security - Resilience and CIIP, European Network and Information Security Agency - ENISA

There is a lack of harmonised security measures when it comes to smart grid across Europe. As a result, there are varying levels of measures of implementation sophistication. Furthermore, the current regulatory measures do not yet actually address or do not address in detail data security issues of the smart grids. ENISA has recognised the problem, and performed a study in order to provide a framework / measurement tool that could be used by RAs for allying the varying levels of security of operators with a minimum national framework and providing an indication of a minimum level of security in the Member States. Dr. Moulinos will share the results of the study.

Summit Agenda

All Summit Sessions will be held in Ramblas B (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euscada12**
An e-mail will be sent out within 5 business days once the presentations are posted.

Monday, 10 December

11:00am - 11:45am

Panel

The Pitch: Selling Cyber Security to Upper Management

Panelists:

- *Michael J. Assante, President & CEO, National Board of Information Security Examiners; SCADA Summit Chair*
- *Markus Braendle, Group Head of Cyber Security, ABB Inc.*
- *Robert McComber, Sr. Program Manager (Security), Telvent*
- *Tyler Williams, Industrial Cyber Security Solutions Manager, Global Oil and Gas Company*

Executive management doesn't need to be convinced to lock the doors of the building at night or to require access cards for the corporate parking garage. The need to implement physical security is obvious. But while your cyber assets are at far greater risk than your physical infrastructure, it can be hard to make the case for cyber security. Learn how to talk about cyber security so that management understands – and signs the checks so you can get what you need.

11:45am - 12:30pm

Case Study

Dream Team: Building the Perfect SCADA Team

- *Auke Huistra, Project Manager - National Roadmap to Secure Process Control Systems CPNI.NL; ERNCIP ICS & Smart Grids Work Stream Lead Workforce Development*
- *Tyler Williams, Industrial Cyber Security Solutions Manager, Global Oil and Gas Company*

Protecting our SCADA systems is not a one-person job. It takes a team. So how do you build the perfect team? Who should be part of the team? What experience and training do they need? How do you keep their skills current? How do you define the roles and functions of each team member? Hear from leaders who've built SCADA teams about what works – and what doesn't.

12:30pm - 1:15pm

Case Study

Leveraging Corporate Risk Porfolios to Quantify the Need for Security Team Expansion

Robert McComber, Sr. Program Manager (Security), Telvent

Today's security leaders face an increasingly complex challenge with regard to expanding their teams to meet what they believe to be an apparent threat. As executives try to balance increasing shareholder pressure for fiscal restraint with a desire to keep the enterprise safe through security investment, new approaches are required not only to 'sell' security upstream to corporate leadership, but also to determine internally where to invest more limited budgets. This talk will focus on the application of corporate risk analysis tools and models to security challenges in a manner that not only provides strong justification, but also reduces overlap with other groups and focuses on core threats, rather than expending resources on outlier risks.

1:15pm - 2:45pm

Lunch

Summit Agenda

All Summit Sessions will be held in Ramblas B (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euscada12**
An e-mail will be sent out within 5 business days once the presentations are posted.

Monday, 10 December

2:45pm - 3:45pm

Expert Briefing

SCADA 2017: The Future of SCADA Security

Jonathan Pollet, CAP, CISSP, PCIP, Founder/Principal Consultant, Red Tiger Security

New threats to cyber security are constantly emerging and rapidly evolving. One of the best ways to prepare for threats you can't even predict if to build an agile organization with flexible response strategies. This session will delve into the current threat landscape, scan the horizon for emerging threats that are likely to emerge in the next few years, and look at how your team can be ready to respond to the threats no one can yet predict.

3:45pm - 4:15pm

Networking Break & Vendor Expo

4:15pm - 5:00pm

Talk

Implementing SCADA Security in the Real World

Franky Thrasher CISSP,CSSA , Information Security Manager - Generation, Electrabel/GDF Suez

Talking about SCADA security is important; getting in done in the real world is much more difficult. First, you must convince management that SCADA security is a priority worthy of investment of resources. Secondly, you must truly understand the landscape, including the gap between compliance and true security. Third, you must know what pitfalls to watch out for and be aware of common misconceptions that can derail your SCADA security efforts. This session will cover all this, including real-world examples and lessons learned from the power generation sector.

Please remember to complete your speaker evaluation for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

5:00pm -6:00pm

Networking Reception

Located in the Lobby Vibe Bar

Presented by Industrial Defender

Summit Agenda

All Summit Sessions will be held in Ramblas B (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euscada12**
An e-mail will be sent out within 5 business days once the presentations are posted.

Tuesday, 11 December

8:00am - 8:45am

Registration & Coffee

8:45am - 9:45am

Keynote

Virtually Protected: Virtualization and ICS

Brian Endres, MCSE, MCP+I, PFA, VTSP, Principal Network Analyst, Invensys Operations Management

Virtualization can lead to SCADA systems that are more resilient and can reduce recovery time from software crashes, but it's not a cure-all. What are the pros and cons of virtualization in an ICS environment?

9:45am - 10:15am

Networking Break & Vendor Expo

10:15am - 11:15am

Case Study

Preparing ICS Defenders: What Skills Really Matter

Michael J. Assante, President & CEO, National Board of Information Security Examiners; SCADA Summit Chair

The most important element of cybersecurity is the human element. Just as in any contest, success lies in identifying talent and continually developing and conditioning teams of professionals to be competitive. The identification and development of competence is no easy task, especially in the field of cybersecurity. In this session, you will learn what a group of experts believe are the technical tasks and skills required for successful ICS cyber defense. We will discuss critical tasks that differentiate performance at various competency levels.

11:15am - 12:00pm

Case Study

Blueprint for Security: The 20 Critical Controls for the ICS Community

Speaker from Centre for the Protection of National Infrastructure (CPNI)

Much research and work has gone into the development of the 20 Critical Controls. Applying that framework to control systems can provide a blueprint that's efficient and effective. Learn how to use the 20 Critical Controls as the basis for your own plan.

12:00pm - 1:15pm

Panel

Supply Side: Perspective on Progress and Challenges

Panelists:

- *Markus Braendle, Group Head of Cyber Security, ABB Inc.*
- *Paul Forney, CSSLP , Chief Technologist, Invensys Operations Management*
- *Amir Grovais, Director, Waterfall Security Solutions LTD.*
- *Robert McComber, Sr. Program Manager (Security), Telvent*

In this session, representatives from the leading control systems suppliers will share their perspective on the progress that has been made and the challenges still to be tackled. Learn what's new and what's next

In testing, security baseline, life-cycle support, vulnerability management, patch validation, and more.

Summit Agenda

All Summit Sessions will be held in Ramblas B (unless noted).

All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euscada12**
An e-mail will be sent out within 5 business days once the presentations are posted.

Tuesday, 11 December

1:15pm - 2:30pm

Lunch

2:30pm - 3:30pm

Expert Briefing
The SCADA Battlefield: Fighting the Enemy Within

Jess Garcia, Certified Instructor, SANS Institute

In the last few years SCADA networks have come into the limelight. Stuxnet, Flame, and other recent attacks against SCADA-related organizations have been a wake-up call. You are doing your best to protect your SCADA networks, but...

What will you do if the attackers break your defenses? What if they are already inside your network? How will you detect them? How can you know what they've done? How can you stop them before it's too late?

In this talk Jess Garcia will share his long international experience in SCADA Network Monitoring and Incident Response, illustrating what are the most common mistakes that allow attackers to reach critical networks, what are the best strategies to detect them and stop them once they are inside, and what can be done today to be ready for the worst.

3:30pm - 4:00pm

Networking Break & Vendor Expo

4:00pm - 5:00pm

Closing Keynote
ICS Security: Time to React

Ruben Santamarta, Security Researcher, IOActive

Industrial control systems are no longer living the quiet existence they used to. Every day, we see how the technological pillars that support our modern society are being scrutinized by different actors with different purposes: researchers looking for vulnerabilities, nation-states trying to collect information or disrupt foreign facilities. SCADA systems, PLCs, SmartMeters and other industrial devices are the new crown jewels everyone is eager to protect...and attack.

This presentation discusses the new scenario this sector is facing by analyzing real-world cases where vulnerabilities, backdoors, cyberwar and espionage come into play. However, we will also highlight positive momentum that's building, with security professionals becoming more involved in and committed to the difficult but crucial task of securing industrial control systems.

Thank you for attending the European SCADA & Process Control Summit.
Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

INDUSTRIAL DEFENDER®

Security. Compliance. Change Management

Tackle Your Industrial Control System Challenges in One Solution

Reduce exposure to cyber risk, ease compliance challenges, and more effectively manage change in your SCADA environment.

With our single, unified platform Industrial Defender's Automation Systems Manager (ASM) integrates asset management, event management, configuration change management, policy management, end point security, and reporting into one powerful vendor & platform agnostic solution.

Scan the barcode to **watch a demo** of ASM or visit
http://www.industrialdefender.com/asm_products/

© 2012 Industrial Defender, Inc.

SANS Survey

Security Practices of SCADA System Operators

SANS Institute is asking those who work for SCADA and other control systems operators to take a 10-minute survey to reveal the level of awareness system operators have around cyber risk, their attempts to manage that risk, and how their efforts are working out so far.

The survey is open until December 18. Results will be released during a webcast held on February 20, 2013.

Not only will respondents help shape industry practices, they will be entered into our iPad drawing!

splunk>

INDUSTRIAL DEFENDER®

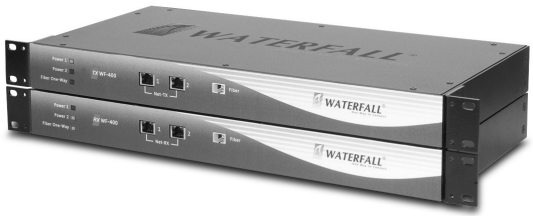
Power and productivity for a better world™

ABB

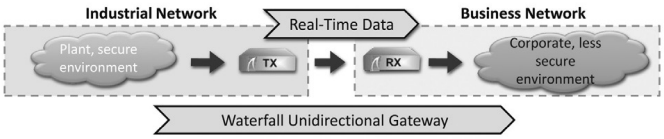
Follow this survey link or scan the QR code to begin: https://www.surveymonkey.com/s/2013_SANS_SCADA_Survey

WATERFALL®
One Way to Connect

Industrial Cyber Security Keeping your Critical Network Safe



- *Absolute protection from external network attacks*
- *Secure your SCADA and DCS networks*
- *Unidirectional Gateways are better than traditional IT security (FW, AV, etc.)*
- *Assists in achieving regulatory compliance*
- *Hundreds of sites deployed in any industrial, critical or operational environment types*



Waterfall® Security Solutions Ltd. is the leading provider of Unidirectional Security Gateways for Process Control Systems, SCADA systems, Remote Monitoring and Segregated Networks, enabling secure and real-time data transfer, from critical (e.g.: SCADA, production, industrial, etc…) networks to external/business networks.

Waterfall's customer base includes Power Generation plants, Oil & Gas upstream/downstream companies, Water and Wastewater facilities, Chemical, Transportation and other utilities and industrial facilities.

Waterfall's Unidirectional Security Gateways include inherent integration with leading industrial applications such as OSIsoft PI™, GE Proficy™ iHistorian, Siemens WinTS, McAfee SIEM as well as leading industrial protocols such as OPC, Modbus, DNP3, and many other SCADA and industrial applications and protocols.

Waterfall's security solutions assist in achieving compliance to NERC-CIP, NRC, NIST, CFATS and other regulations as well as cyber-security best practices.

Contact us for more information: info@waterfall-security.com
www.waterfall-security.com

IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Proven Pioneers in ICS & Smart Grid Security

Expert Services:

Smart Grid Security Research & Assessments
SCADA & ICS Security Assessments
CIPS Compliance Technical Support

www.IOActive.co.uk **info@IOActive.co.ok** **@IOActive**

UPCOMING SUMMITS AND COURSE TRAINING

Virtualization and Cloud Computing Summit 2013

Anaheim, CA | January 7-14, 2013

Mobile Device Security Summit 2013

Anaheim, CA | January 7-14, 2013

North American SCADA and Process Control Summit 2013

Lake Buena Vista, FL | February 6-15, 2013

AppSec Summit 2013

Austin, TX | April 22-27, 2013

IPv6 Summit 2013

Washington, DC | June 14-16, 2013

Digital Forensics & Incident Response Summit 2013

Austin, TX | July 9-16, 2013

Critical Controls Summit 2013

Washington, DC | August 12-18, 2013

Counter Hack Summit 2013

Washington, DC | November 7-14, 2013

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at summit@sans.org

Visit www.sans.org/summit for detailed summit agendas as they become available.