securityspecifiers

CONSULT 2020

VIRTUAL TECHNICAL SECURITY SYMPOSIUM

OCTOBER 26-27

In Coordination With

SIA
SECURITY INDUSTRY ASSOCIATION

Diamond Sponsor

Altronix®

Gold Sponsors

ACRE
OPEN OPTIONS
RS Technologies
VANDERBILT
intel
LENEL:S2
SALIENT

PROGRAM

Bicsi
CONTINUING EDUCATION CREDIT PROVIDER

ASIS INTERNATIONAL
Preferred CPE Provider

Presented, operated and organized by SecuritySpecifiers, and supported by the Security Industry Association (SIA), the 2020 virtual mini-conference has been developed specifically for technical security design professionals. From cybersecurity to spec writing and design issues, the environment that security consultants and engineers face is constantly evolving. The design challenges are shared.

If you have an interest in security engineering and technology, you simply can't afford to miss this FREE technical learning symposium featuring six targeted education sessions presented by elite speakers.

The event has been approved by BICSI for 6 CEC's and for up to 6 CPE's from ASIS.

More Details and Registration Here

securityspecifiers

securityspecifiers

CONSULT 2020

VIRTUAL TECHNICAL SECURITY SYMPOSIUM

OCTOBER 26-27

MONDAY, October 26

sponsored by

milestone

1:00 – 2:00 PM EDT

How Effective Are Thermographic Cameras?

Moderator:

Benjamin Butchko, President & CEO, Butchko, Inc.

Panelists:

Lorna Chandler, CEO, Security by Design
Joe Fallon, Security Team Manager, Faith Group
Charles LeBlanc, Associate Principal and Project Executive, IMEG Security Group
Gary Strahan, CEO, Infrared Cameras Inc.

Consultants have had the challenge of helping clients with the challenges of quickly deploying or adapting thermographic technology (whether it works or not) into existing operations and managing performance expectations. Issues have included performance measurement, false and/or highly exaggerated manufacturer claims, effectiveness of temperature verification, compliance (privacy, HIPAA, CDC medical devices, etc.), integration with operations, additional queuing, and integration with architecture. These challenges have led to additional COVID-19 inspired considerations such as the entire pre-screening process and its application to all building entrants. What was once a screening process primarily limited to visitors has become, in many cases, a process applied to all facility entrants. If a person triggers as a potential threat, how do you handle it from a privacy, contract tracing, access, and customer service standpoint? Hear an informed panel discussion on the technology's effectiveness and deployment issues.

Learning Objectives:

1. Understand the technology underlying thermographic cameras.
2. List key evaluation parameters for thermographic performance.
3. Understand typical use cases in security screening.
4. Provide examples successful applications and tests.
5. Describe likely scenarios for thermographic camera deployment.
6. List privacy concerns with the deployment of this technology.

securityspecifiers

CONSULT 2020

VIRTUAL TECHNICAL SECURITY SYMPOSIUM

OCTOBER 26-27

MONDAY, October 26

2:15 – 3:15 PM EDT

What's the Best Way to Specify Integrated Systems?

sponsored by

SIEMENS

Ingenuity for life

Moderator:

Ray Coulombe, Managing Director, SecuritySpecifiers

Panelists:

Greg Ceton, Director of Strategic Initiatives and Special Projects, Construction Specifications Institute (CSI)

Jim Henry, Independent Consultant and Co-Host, The Risk Advisor Podcast

James Krile, Senior Technology Engineer, Heapy Engineering

Frank Pisciotta, Founder & President, Business Protection Specialists

CSI MasterFormat as it relates to security (Div 08 and Div 28) is largely structured around components – cameras, readers, etc. Increasingly, however, systems are specified as a unified or integrated collection of sub-systems. There is some newer provision for this in Div. 28 (see 28 05 45, Systems Integration and Unified Systems) and added flexibility within the MasterFormat framework. Is this adequate or should a rethinking of MasterFormat be considered. Hear from several consultants who are wrestling with this issue and from CSI with a broader construction industry perspective.

Learning Objectives:

1. Understand the role of Construction Specifications Institutes (CSI) MasterFormat.
2. Understand the flexibility provided by CSI in assigning classification numbers in specifications.
3. Understand the limitations and issues with compiling a specification based on a collection of component pieces and software.
4. Explain what is meant by a "Unified System".
5. Know where to find Systems Integration and Unified Systems in MasterFormat.
6. List the pros and cons of specifying a security system as a unified system versus its component pieces.

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM
OCTOBER 26-27

MONDAY, October 26

3:30 – 4:30 PM EDT

Plugging into Managed Services

sponsored by

brivo
simply better security

Moderator:

Dan Dunkel, Managing Director - Managed Security Services Practice, PSA Security Network

Panelists:

Bud Broomhead, CEO, Viakoo

Gary Hoffner, Vice President, PSLA

David Lathrop, Vice President, Unlimited Technologies

Steve van Till, President & CEO, Brivo

Remote Managed Services, including cloud-based video and access control and network monitoring, has become an important component of many systems integrators' offerings, particularly in the COVID-19 environment. Further, cloud-based services are a key element of both the security and IT landscapes, but have not been widely specified. Based on responsibilities within the Client organization, a subtle benefit may be isolating the product selection from the General Contractor yet introduce deeper issues of data security and policy development. Also, the field of capable bidders may be narrowed to those who have the expertise to effectively address the issues that arise under cloud managed services (such as configuring the security features for the cloud based servers)? Learn more about managed services and their associated benefits, issues, and importance in a post-pandemic environment.

Learning Objectives:

1. Understand the types of services that qualify as “managed”.
2. Describe how managed services are delivered remotely?
3. Explain potential security vulnerabilities and considerations in remote delivery of services.
4. Describe how the provision of managed services can provide enhanced system reliability.
5. List the pros and cons of remote managed systems vs. on-site maintenance.
6. Explain why the availability of remote managed services should be of interest to a design consultant during the system design phase and contracting phase of a project.
7. Explain the sufficiency of remote managed services during a lockdown event, such as the current pandemic.

securityspecifiers

CONSULT 2020

VIRTUAL TECHNICAL SECURITY SYMPOSIUM

OCTOBER 26-27

TUESDAY, October 27

1:00 – 2:00 PM EDT

It's Time to Specify OSDP

sponsored by

CYPRESS INTEGRATION SOLUTIONS

Moderator:

Rodney Thayer, Convergence Engineer, Smithee Solutions

Panelists:

Paul Ahern, President & CEO, Cypress Integration Solutions

Brian Coulombe, Principal and Director of Operations – DVS, Ross & Baruzzini

Joe Gittens, Director – Standards, Security Industry Association

John Nemerofsky, Chief Operating Officer, Sage Integration

Open Supervised Device Protocol (OSDP), advanced and maintained by SIA, is now an IEC standard. OSDP provides major improvements over Wiegand communications technology, through advanced security, device supervision and management, and interoperability, all under the umbrella of an open and standard protocol. Hear from a panel representing those involved in the development of the OSDP standard, manufacturers who have implemented it, and potential specifiers about field experiences, implementation issues and the way forward.

Learning Objectives:

1. Understand the basics of Open Supervised Device Protocol (OSDP).
2. List the advantages that OSDP provides over Wiegand technology.
3. Describe how OSDP enables device interoperability.
4. Explain how device supervision can be accomplished through OSDP.
5. Understand OSDP encryption means.
6. Describe field implementation issues that have accelerated or hindered the adoption of OSDP.

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM
OCTOBER 26-27

TUESDAY, October 27

2:15 – 3:15 PM EDT

Delivering Secure Identity

sponsored by

ALLEGION™

Moderator:

Sal D'Agostino, CEO, IDmachines

Panelists:

Consuelo Bangs, Sr. Program Manager, IDEMIA

Pierre Bourgeix, Chief Technology Officer & Founder, ESI Convergent

David York, Chief Information Security Officer, Allegion

Hugo Wendling, CEO, WaveLynx

Preserving the security of an identity has the objectives of (1) uniquely tying one's credentials to an individual to validate who they say they are, and (2) to maintain the security of those credentials to prevent someone else from stealing them to access information or services tied to the credential holder. No longer are user names and passwords considered adequate. This session will review current and proposed techniques to provide more highly secured credentials. These will include FIDO ("Fast Identity Online"), PIV ("Personal Identity Verification"), CIV ("Commercial Identity Verification") smart cards, and mobile credentials.

Learning Objectives:

1. Explain the importance of secure identity.
2. List common means of identity verification.
3. Assess the relative security of security identification methods.
4. Explain how mobile devices can deliver secure identity verification.
5. Understand proposed techniques for provisioning secure identity.

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM
OCTOBER 26-27

TUESDAY, October 27

3:30 – 4:30 PM EDT

The Impact of Privacy Laws on Access Control

sponsored by

tyco

Moderator:

Forrest Gist, Global Technology Lead – Security, Jacobs

Panelists

Kathleen Carroll, Managing Partner, Seven Seas Strategic Communications

Min Kyriannis, Managing Director, EMD|JMK

Rick Focke, Senior Product Manager, JCI/Tyco Security Products

Brenda Leong, Senior Counsel & Director of Artificial Intelligence and Ethics, Future of Privacy Forum

Protection of cardholders' personal data, photo, DOB, license number, work and vacation schedule, etc, contained in access control systems is often overlooked – and can easily be violated. Facial recognition has its own set of concerns. Those with appropriate privilege levels may theoretically abuse their privileges and view the access control transactions and personal information of cardholders for non-security-related purposes. Further, how is cardholder data entered, managed, stored, and secured? Video also plays a role in access control by providing verification and, in some cases, recognition. How is cardholder consent to the use of their data being obtained? Can privacy laws work to diminish security? With the prevalence of GDPR, CPPA, NY-Shield Act, and many others coming forward in the future, how would these privacy laws impact access control? Requirements are broad and wide and many fail to understand that these privacy laws also include any digital signature in these systems. How do you fuzz, encrypt and otherwise protect this data so it still falls under these requirements, yet maintain security?

Learning Objectives:

1. List common privacy laws and discuss what led to them.
2. Understand the impact of privacy laws on security system products and access control in particular.
3. List types of data that may be subject to privacy laws.
4. Understand the precautions security manufacturers and provides must reasonably take to protect the privacy of personal data contained within their systems.
5. Describe how privacy and security may have different or conflicting objectives.
6. List means of protecting data to keep it private.