



**Process Control Systems
Industry Conference**

2008 INDUSTRY CONFERENCE

“Tactical & Strategic Solutions for the Control Systems Community”

SPEAKER BIOGRAPHIES

*HILTON LA JOLLA TORREY PINES
LA JOLLA, CALIFORNIA*

AUGUST 26 – 28



Keynote Biography

Phyllis A. Schneck, PhD

Vice President of Research Integration, Secure Computing Corporation

Chairman Emeritus, Board of Directors, InfraGuard National Members Alliance

Dr. Phyllis Schneck is Vice President of Research Integration for Secure Computing Corporation. In this role, she is responsible for the design and applications of Secure Computing's Internet reputation intelligence, strategic thought leadership around technology and policy in the security and infrastructure protection space, and management of the company's intellectual property portfolio.

For more than 13 years, Dr. Schneck has had a distinguished presence in the security and infrastructure protection community, serving for 8 years as chairman of the National Board of Directors of the FBI's InfraGuard program and founding president of InfraGuard Atlanta, growing the InfraGuard program from 2,000 to over 26,000 members nationwide. In this role, she was primarily responsible for the strategic growth and vision of the private sector side of the InfraGuard Program and for growing the relationship between InfraGuard and the US Department of Homeland Security (DHS) through several Directorates. As examples, Dr. Schneck was chiefly responsible for the first Memorandum of Understanding between DHS and InfraGuard and for engaging DHS officials with all local InfraGuard Chapters nationwide. She was also responsible for creating the first overall strategic plan in 2002 and worked with the team to augment the plan for engaging the private sector in integrated infrastructure protection information, and dissemination and participation in the creation of National Policy, such as the National Infrastructure Protection Plan. Dr. Schneck is currently co-Chairing a working group for the CSIS Commission to Advise the 44th President on Cyber Security.

Named one of Information Security Magazine's *Top 25 Women Leaders in Information Security*, Dr. Schneck briefed the Japanese Government on information sharing and infrastructure protection and was the moderator of the White House Town Hall Meeting in Atlanta for the National Strategy to Secure Cyberspace in June 2002. She holds three patents in high-performance and adaptive information security and has six research publications in the areas of information security, real-time systems, telecom, and software engineering.

Before joining Secure Computing, Dr. Schneck was vice president of Enterprise Services for eCommSecurity. Prior to that, she served as vice president of Corporate Strategy for SecureWorks, Inc., and was founder and chief executive officer of Avalon Communications, a provider of real-time security technology that was acquired by SecureWorks, Inc. Dr. Schneck also held various information science technical positions with CygnaCom Solutions, The MITRE Corporation, Computer Sciences Corporation, IBM Systems Integration Division, NASA Goddard Space Flight Center, and the University of Maryland's Department of Meteorology.

Dr. Schneck received her PhD in Computer Science from Georgia Tech. She maintains a seat on the Advisory Board of the Johns Hopkins University Department of Computer Science, served on the Steering Committee for the Sam Nunn Information Security Forum as well as a term on the Georgia Tech Advisory Board, and co-founded the Georgia Tech Information Security Center and the Georgia Electronic Commerce Association's Working Group on Information Security.

Speaker Biographies

Ted Angevaare, Global DACA Manager, Shell Global Solutions International BV, Global DACA Team, Rijswijk, GSES

As Shell's Global Manager of Process Control Security and Architecture, Ted brings more than 27 years of Process Control and Automation experience to Shell. Ted has worked in all aspects of the Process Control and Automation world, with postings in Syria, Brunei, Tunisia, Morocco, Argentina, the Netherlands, and other countries where Shell is active. His experience varies from Operations & Maintenance through Engineering & Project Management to Standardization and Leadership. He has been active in Process Control Security and Architecture over the past six years and is the godfather of Shell's DACA for which he has created Shell's first standard on Process Control Security. Ted holds a degree in 'Measurement & Control' and 'Electronics' and is currently leading a team of 14 experts involved in Process Control Security and Architecture for all business groups of Shell. Ted is vice-chairman of LOGIIC, a consortium of oil companies and API, sponsored by DHS, and he is also chairman of the Process Control Security working group of the WIB, an international group of Instrument Engineers.

Clint Baker, Sergeant, Integrated Technological Crime Unit, Royal Canadian Mounted Police

Clint Baker is a Sergeant working in the Integrated Technological Crime Unit and has been a member of the RCMP for 13 years. Mr. Baker has extensive experience in network security related investigations and related technology. He has worked with the Tech Crime field since 2001 and has a Bachelor's degree in Physics from the University of Alberta.

Clint Bodungen, Founder/Principal Analyst, Critical Infrastructure Defense Group

Mr. Bodungen has over 13 years of experience in both physical and systems security, most of which has been dedicated to industrial systems, process control, and SCADA. He began his professional career as a Computer Systems Security Officer and Operational Security Manager in the United States Air Force, where he participated in both physical and cyber red team (covert) Operations. Following the Air Force, he was employed by a major security software vendor to test Network Intrusion Detection Systems (IDS), including authoring several custom IDS evasion and penetration testing tools. Over the past decade, Mr. Bodungen has built corporate security departments from the ground up, led numerous security assessments and penetration testing teams, and has played a key role in securing some of the nation's top organizations within the heart of our nation's critical infrastructure industries. These industries include the DoD, DoE, top Oil & Gas companies, financial institutions, utility companies, and major telecommunications companies. Mr. Bodungen was the Co-Founder of the Critical Infrastructure Institute and the founder/principal analyst of CIDG., Corp. (Critical Infrastructure Defense Group), where he continues to perform PCN/SCADA security assessments, red team testing, and regulatory compliance consulting.

Wayne F. Boyer, PhD, Advisory Engineer/Scientist, Idaho National Laboratory

Dr. Wayne Boyer received a BS degree in Electrical Engineering at Brigham Young University and an MS degree in Electrical Engineering at Stevens Institute of Technology. He earned a PhD in Computer Science from the University of Idaho. He has worked as a systems engineer and software engineer on Ballistic Missile Defense systems and various communications systems for AT&T Bell Laboratories in New Jersey and in Denver, Colorado. Wayne was also a technical supervisor for several years at AT&T Bell Laboratories where he was the leader of teams that developed and tested business communications products such as Private Branch Exchange switching systems and Voice Mail systems. Since joining the INL, Wayne has been an Advisory Engineer/Scientist and has acted as a control system engineer, systems analyst, software engineer, and researcher on various projects including robotics research, high level waste processing, distributed computing, and control system cyber security. Wayne is an affiliate faculty in the Computer Science department at the University of Idaho in Idaho Falls. He has taught undergraduate courses in Computer Science including Software Engineering, System Software, and Algorithms. He is teaching a graduate course in Fault Tolerant Systems. He has published several papers on computer security and efficient scheduling algorithms for distributed computing systems.

Dr. Markus Braendle, Principal Scientist, ABB Corporate Research

Dr. Braendle works as a Principal Scientist for Corporate Research of ABB, a major global supplier of industrial and utility automation products and solutions. He is responsible for coordinating security related activities within ABB Corporate Research world-wide. He also leads the Security Council of the Power Systems division. Dr. Braendle is an active member of different standardization efforts (e.g. ISA S99, IEC TC57 WG15, Cigre B5.38), various IEEE-related security working groups and task forces, and is involved in security discussions with government and regulatory organizations (e.g. NERC). Dr. Braendle has a MS and a PhD in Computer Science from ETH Zurich (Switzerland).





Eric Byres, Chief Technology Officer, Byres Security Inc. & Senior Partner, Byres Research

Recognized as one of the world's leading experts in the field of Critical Infrastructure Security, Eric Byres has been responsible for numerous standards, best practices, and innovations for data communications/controls systems security in industrial environments.

Eric's work in Industrial Cyber Security spans both the academic and industry domains. As the founder of the BCIT Critical Infrastructure Security Centre, he shaped it into one of North America's leading academic facilities in the field of SCADA cyber-security, culminating in a *SANS Institute Security Leadership Award* in 2006. At the same time, Eric has provided security guidance to government security agencies and major energy companies on cyber protection for critical infrastructures. Eric is also the chair of the ISA SP99 Security Technologies Working Group and is the Canadian representative for IEC TC65/WG10, a standards effort focusing on an international framework for the protection of process facilities from cyber attack.

Eric's achievements include testifying to the US Congress on the *Security of Industrial Control Systems in National Critical Infrastructures* as well as receiving awards from international organizations. These include the *IEEE Outstanding Industry Applications Article* prize in September 2000, the 2004 *Donald P. Eckman Education Award*, and the 2005 *Keith Otto Award* presented by the Instrumentation, Systems, and Automation Society (ISA).

Candace Chan-Sands, Program Manager, EMA, Inc.

Candace Chan-Sands is a Program Manager with EMA, Inc., a technology consulting firm headquartered in St. Paul, Minnesota. Candace has over 28 years experience in public and private sector program and project management with clients at the state, national, and international levels. Her areas of expertise include system security, business process design and re-engineering; information systems planning, design and implementation; information flow and work practice re-design; and requirement analyses. She is a certified Project Management Professional with the Project Management Institute and holds a BS in Nuclear Engineering and an MBA in Technology Management. Candace is a licensed instructor in the EPA/Sandia National Laboratories' Risk Assessment for Water™ training program and has conducted training for numerous water and wastewater utilities across the United States.

Prior to joining EMA, Candace spent over 10 years with the United Nations' International Atomic Energy Agency (IAEA) as a Scientific and Technology Officer/Project Manager. While with the UN, she was part of a six member team at the IAEA charged with oversight of all information technology/information systems-related activities. She developed long-term information technology strategies, established standards and policies, and managed the information technology/information systems budgets.

Since joining EMA, Candace has served as program manager for several major technology projects including Control System standards development and procurement guidance for a major city; implementing several Enterprise Maintenance Management and Inventory Management systems; development of a large revenue/billing system, strategic information technology planning, as well as Enterprise Architecture blueprints; and, definition, development, conversion, and implementation of Geographical Information Systems.

Currently, she serves as Principal Investigator/Project Manager on the Water Environment Research Foundation's project, "Security Measures for Computerized and Automated Systems." This project's research will provide utilities with tools and guidance on how to secure and protect automated systems, including examining available technology to sense and correct security breaches. The project team includes over 20 utilities from across the US, 10 Water Environment Federation Project Steering Committee members, the American Water Works Association Research Foundation, and 3 subconsultant firms. This project is collaborating with the US Department of Homeland Security, Control System Security Program, on its development of the Control System Cyber Security Self Assessment Tool.

Penny Chen, Principal Systems Architect, Yokogawa IA Global Marketing Center (USMK)

Penny Chen is a Principal Systems Architect at Yokogawa IA Global Strategic Technology Marketing Center in US. She is responsible for technology standardization and marketing focusing on wireless, network, and security. Over past 10 years, Penny worked as Sr. Architect and Technical Marketing Manager at Intel and Alcatel-Lucent; focused on wireless networking technologies and security solutions for a variety of wireless technologies including Bluetooth, WiFi, and 2G/2.5G/3G Cellular wireless. Penny is actively involved in ISA100, ISA100.11a standard group, ISA99, ISA Security Compliance Institute (ISCI), and Wireless Compliance Institute (WCI). She is currently Co-Chair of the ISA100.15 Backhaul Backbone Networks Working Group. Penny received a PhD in Electrical Engineering from Northwestern University.

Clayton Coleman, Senior Consultant, Invensys Process Systems Global Consulting

Clayton Coleman, Senior Consultant, IPS Global Consulting, has been working in the process controls industry for 10 years, primarily focused on the integration of Industrial Security and Information Technology. His past experiences have included managing global firewall infrastructures, assessing critical infrastructure facilities, and project management for network and security implementation

(continued next page)

(continued from previous page)

projects. Clayton has presented to numerous industrial groups on the topic of Cyber Security at venues in several countries. He is a CISSP and holds certifications from SANS, Microsoft, and Cisco. Clayton is a native Texan and enjoys fishing, kayaking, and ham radio. He resides in Rusk, Texas, home of the Texas State Railroad, with his wife and two daughters.

Eric C. Cosman, Engineering IT Consultant, The Dow Chemical Company

Eric C. Cosman is an Engineering Solutions IT Consultant with The Dow Chemical Company in Midland, Michigan. His responsibilities include system architecture definition and design, technology management, and integration planning for manufacturing systems globally. He has held positions in Process Engineering, Process Systems Software Development, Telecommunications, IT Operations, Automation Architecture, and Consulting. He has presented and published papers on various topics related to the management and development of information systems for process manufacturing.

Eric represents Dow on various standards committees, industry focus groups, and advisory panels. He has been a contributor to the work of the ISA95 committee and currently serves as the co-chairman of the ISA99 committee on industrial automation systems security. He also sponsors a Chemical Sector Cyber Security Program team focused on manufacturing systems cyber security and was one of the authors of the Chemical Sector Cyber Security strategy for the US, originally published in 2002 and updated in 2006.

Paul Didier, Industrial Solutions Architect, Cisco

Paul Didier is an Industry Solutions Architect for Manufacturing for Cisco. He is responsible for developing solutions for the Manufacturing vertical including those for Automation and Control systems. Paul is a member of the ODVA's Technical Review Board and has over 20 years of industry experience.

David Edwards, CIO, Metropolitan Water District of Southern California

Dave heads the Information Technology organization for the Metropolitan Water District of Southern California. As such he is responsible for overseeing the traditional IT functions as well as support for the Supervisory Control and Data Acquisition (SCADA) system. He serves as the water and wastewater representative on the Governing Board of the US Department of Homeland Security's Process Control Systems Forum. On behalf of the Water Sector Coordinating Council (WSCC) in Washington, DC, Dave is co-chairing the national effort to secure water sector industrial control systems.

Previously, Dave was Director of Information Technology Services for the Los Angeles County Metropolitan Transportation Authority (MTA). He currently chairs the Business Process Committee for the California State Water Contractors and serves as vice chair of the AWWA Cal Nevada Information Management Committee.

Dave holds a Bachelor's degree in Mathematics from Alberston College of Idaho and a Master of Business Administration from the University of Redlands.

Patrick Ellis, IT Director/CISO, Broward County Water and Wastewater Services

Patrick Ellis is the Director of Information Technology for the Broward County Water and Wastewater Services organization. He is responsible for the acquisition, provisioning, and maintenance of all technology-related systems and services for the Water and Wastewater utility. He and his team support over 70 servers that provision video, voice, and data services to over 700 workstations across 4 separate treatment facilities and 2 disparate networks. His role also includes that of Chief Information Security Officer for the utility. As such, he is responsible for establishing the security policy, ensuring the use of technology to improve the overall security posture of the utility, and spearheading the campaign to address issues related to the convergence of physical and cyber security systems. Mr. Ellis holds the following professional certifications: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Microsoft Certified Professional, Project Management Professional (PMP), Lean Six Sigma Yellow Belt, Certified Information Technology Infrastructure Library (ITIL), SANS Critical Infrastructure Protection (CIP) Certified. Mr. Ellis earned a Bachelor's degree in Information Technology from Barry University and a Master's degree in Management Information Systems from Florida International University.

Robert Evans, Engineer, Idaho National Laboratory

Bob Evans works as an Engineer at the Idaho National Laboratory with over 35 years experience in instrumentation, measurements, data validation, and control system cyber security. He has a BS and MS in Physics and a PhD in Engineering and Applied Science. Mr. Evans has been active in the control system cyber security arena for over 3 years and is member of ISA SP99 committee serving on Working Groups 1, 2, 4, and 5, the C1 Working Group of the Institute of Electrical and Electronics Engineers Power Engineering Society Substations Committee, the American Public Transportation Association's Control and Communications Security Working Group, and the US Department of Homeland Security Control System Security Program-supported Standards Awareness Team.





Mark Fabro, President & Chief Security Scientist, Lofty Perch

As President and Chief Security Scientist, Mark Fabro brings almost 20 years of information security business and thought leadership to Lofty Perch. As a recognized expert in developing cyber security strategies to empower business, he specializes in the development of strategic sector-specific cyber solutions for industrial and critical national assets. Known best for his role in defining cyber attack methods and threat vectors for critical infrastructure (CI) and key resource (KR) systems, he has worked on keystone security projects that include the White House National Strategy to Secure Cyberspace, the DHS Control System Security Program Recommended Practice committee, the National Response Plan, and the post-Katrina Industrial Control Systems Secure Rehabilitation Program. Mr. Fabro has authored numerous practices for the DHS Control Systems Security Program and various intelligence agencies around the world. Previously, he has been part of the senior leadership teams at many leading security firms including Guardent/Verisign, American Management Systems, Secure Computing Corporation, and BearingPoint's elite Security and Identity Management Practice.

In 2004, Consulting Magazine recognized him as one of the "25 Most Influential Consultants in the World" for his work in critical infrastructure protection and cyber security education.

Gary Finco, Control System Cyber Security Researcher, Idaho National Laboratory

Mr. Finco is the deputy project manager for the National SCADA TestBed Program (NSTB) established by the US Department of Energy (DOE-OE) and a SCADA Security Researcher for the NCSA Control System Security Program (CSSP), a US Department of Homeland Security (DHS) effort. Additionally, he is one of the authors of the *Cyber Security Procurement Language for Control System* document.

Mr. Finco has over 30 years experience in real-time data acquisition (22 of those with SCADA and EMS systems) at Texas Instruments, Abbott Laboratories, DataLab Inc., and ABB Inc. before joining INL in February 2005.

While at ABB he was the project manager for the first SCADA/EMS system to be assessed for cyber security vulnerabilities under the DoE's NSTB project. He also provided on-site system support for ABB at PEPCO in Washington, DC; Iberdrola in Bilbao and Madrid, Spain; DEWA in Dubai, UAE and ADCO in Abu Dhabi, UAE.

Stephen Gill, Chief Scientist, Team Cymru

Stephen Gill is Chief Scientist, Research Fellow, and co-founder of Team Cymru. Stephen has worked as a senior network engineer, security architect, and technical analyst at various companies including IBM, Dantis, GTP, Vanco, and Cisco Systems. He thrives on innovation, talking tech, and researching the 'who' and 'why'. He equally enjoys worldwide outreach with partners towards solving the technical and social challenges of malicious Internet activity. He is honored to lead the technical charge for such a forward thinking group of security researchers.

Clifford Glantz, Senior Staff Scientist, Pacific Northwest National Laboratory

Cliff Glantz is a Senior Staff Scientist and project manager with Pacific Northwest National Laboratory (PNNL). Cliff's primary areas of research are critical infrastructure protection and emergency management. Cliff is the manager of PNNL's cyber security project work for the Nuclear Regulatory Commission (NRC). Cliff has also played a key role in critical infrastructure research projects for the US Department of Energy, US Department of Homeland Security, and Institute for Information Infrastructure Protection (I3P). He is a member of the PCSF's SCADA Cyber Self-Assessment Working Group (SCySAG) and Control System Technical Security Metrics Interest Group.

Mark Hadley, Cyber Security Research Scientist, Pacific Northwest National Laboratory

Mark Hadley has been a research scientist at Pacific Northwest National Laboratory since 2001, and his current research focus is critical infrastructure protection. Mark is currently the project manager or principal investigator for a variety of projects for both government and private sector clients. Sample projects include the transfer of control system authentication technology to industry, evaluating the impact of encryption and authentication technologies upon serial communication, and assessing the applicability of traditional "IT" technology for use in the electric sector. Mark has a BS in Computer Science and Mathematics from the University of Puget Sound.

Steve Hargis, Director of Secure Networks™, Enterasys Networks, Inc.

Steve Hargis is the Director of Secure Networks™ Solutions at Enterasys Networks. Mr. Hargis has an extensive background in technology that spans over 19 years in both the public and private sectors. Currently, Mr. Hargis provides strategic technology direction for Enterasys' Secure Networks™ products and solutions. He also runs a Customer Advocacy and Strategy organization at Enterasys which provides critical customer input into technology development. Prior to joining Enterasys, Mr. Hargis was a chief network architect

(continued next page)

(continued from previous page)

for several government agencies and was principally involved in developing initial data communication systems for expansive public entities. Mr. Hargis has been instrumental in evolving leading technologies in the areas of network security, policy networking, and dynamic threat management. Mr. Hargis guest lectures on Advanced Network Technologies at the University of Houston and is an experienced industry presenter.

David Highfill, Utility Security Practice Lead, EnerNex Corporation

Mr. Highfill is a Software Engineer and the information security architecture expert for EnerNex Corporation. He is one of the system architects for the PowerWAN – TVA's new wide-area IP-communications network – and has been heavily involved in the integration of the Bradley County 500kV Substation. He is the primary author of the overall security policy for the PowerWAN as well as many other reference documents and specifications for both the PowerWAN and Bradley Substation projects.

He also serves as the information security expert for EnerNex in support of Southern California Edison's Advanced Metering Infrastructure Project. He has developed the information security framework that will be used to manage risk, write policy, and produce specifications for SCE and has adapted this framework for broader reference by the UtilityAMI forum.

Mr. Highfill is a Certified Information Systems Security Professional (CISSP) and holds Bachelor's and Master's degrees in Engineering Technology from East Tennessee State University.

Jason Holcomb, Security Consulting and Researcher, Digital Bond, Inc.

Before joining Digital Bond, Mr. Holcomb spent 10 years at a multidiscipline asset owner where he lead IT security efforts in a variety of control systems. This experience drives his passion to deliver useful assessment tools and methodologies to the control system community. He is a key contributor to Digital Bond's research and consulting work and is currently serving as the technical lead for the Bandolier project. Mr. Holcomb holds a BS in Computer Science, an MA in Computer Resources and Information Management, and several professional certifications including the designation of Certified Ethical Hacker.

Darren Hollifield, Manager, Water Treatment & Control Systems, JEA

Darren Hollifield is the Water Treatment Operations and Maintenance Manger at JEA. Darren is responsible for the 35 water treatment facilities and 140 Floridan aquifer wells that serve Duval, St. Johns, Clay, and Nassau counties. Darren is also responsible for managing the System Controls group which operates and maintains the SCADA systems for 15 wastewater plants, 35 water plants, and 1200 lift stations. Darren has 26 years of experience in the water and wastewater industry. Darren has a degree in Public Administration from the University of North Florida.

Robert Huber, Senior Cyber Security Researcher, Idaho National Laboratory

Robert is currently a Cyber Security Researcher in the Critical Infrastructure Protection/Resilience Division at Idaho National Laboratory (INL) tasked with analysis of the latest cyber threats and defensive technologies for control systems. Robert's research includes situational awareness, threat analysis and network security architecture.

Robert joined INL from JP Morgan Chase where he was a vice president and the chief security architect for the security event management team. Robert was the technical lead and manager for the intrusion detection, vulnerability assessment, and firewall log monitoring programs.

In addition to his civilian experience, Robert is a member of the Air National Guard serving in a network warfare squadron as a defensive element leader for digital media forensics, network intrusion, and malicious code analysis. Robert holds a BS in Computer Science as well as the CISSP, Sans GSEC, GCFW, and Certified Ethical Hacker certifications.

Scot Huntsberry, Supervisory Special Agent, Cyber Division/Computer Intrusion, Federal Bureau of Investigation

Scot Huntsberry is a Supervisory Special Agent of the Federal Bureau of Investigation. Having spent six years investigating cyber crime in the field, Scot is currently assigned to FBI Headquarters' Cyber Division.

Brian Isle, Chief of Operations, Adventium Labs

Mr. Isle is the Chief of Operations and a member of the technical staff at Adventium Labs. His current technical focus is in assessment of critical infrastructure safety and security. Mr. Isle is currently supporting a US Defense Department program developing approaches for automating aspects of vulnerability assessment for force protection at military bases and a US Department of Homeland Security program to apply advanced cyber protection technology to control systems for critical infrastructure. Mr. Isle is the chair person for the Process Control Systems Forum special interest group on cyber security for manufacturing and process control systems. Mr. Isle provides consulting services to Adventium's commercial clients to provide technical program reviews, advice on effective engineering operations, integration of new technology, and creating go-to-market strategies





Richard Jackson, Chief Information Protection Officer and General Manager of Global Information Risk Management, Chevron Corporation

Richard Jackson is the Chief Information Protection Officer and General Manager of Global Information Risk Management for Chevron Corporation and is responsible for the identification and management of risks relative to Chevron's business information and information technology assets. In this capacity, Mr. Jackson is responsible for the security of Chevron's worldwide computing infrastructure and information assets. Other areas of responsibility include data privacy, records management, information technology intellectual property rights, process controls network security, and information technology export compliance. He also serves as Corporate Champion and provides information risk management and security consultation services to Chevron's operating companies worldwide.

Prior to his current position, Mr. Jackson held numerous management positions in Chevron's Marketing organization including Manager – McDonald's Alliance, Manager – Global Aviation Fuel Sales, Manager – Lubricants National Account Sales, and Plant Manager – Lubricants Manufacturing and Distribution Center.

Mr. Jackson formerly served as Chairperson of the American Petroleum Institute's Information Technology Security Forum and Executive Director of the FBI's San Francisco Bay Area InfraGard Chapter.

Mr. Jackson earned a Bachelor's degree in mechanical engineering from Howard University and a Master's degree in business administration from Pepperdine University.

Jeff Kalibjian, HP Distinguished Technologist, HP Atalla Security Products, Hewlett Packard Corporation

Mr. Kalibjian is currently a senior security architect in Hewlett Packard's Atalla Security Products. Atalla Security Products has been a leader in hardware-based security for over 30 years. He is lead architect for HP's new energy compliance product: the Trusted Compliance Solution for Energy. He has been on the senior management teams of two security start-ups and has had his own security consulting company. Prior to working in the public sector, Mr. Kalibjian spent 12 years at the Lawrence Livermore National Laboratory, where he was involved in pioneering work in such fields as missile defense, automated design and manufacture, and electronic commerce. He has a BS in electrical engineering and computer science from UC Berkeley and is chairman of the IEEE East Bay Computer Society.

David Kleidermacher, Chief Technology Officer, Green Hills Software, Inc.

David Kleidermacher is Chief Technology Officer at Green Hills Software where he has been designing operating systems, virtualization, and security solutions for the past 17 years. David is responsible for the company's product planning, development, deployment, and technical support. David holds a Bachelor of Science in computer science from Cornell University and is frequent writer and speaker on technology subjects.

Serhii Konovalov, Industrial Solutions Architect, Cisco

Serhii is an Industrial Solutions Architect for OIL&GAS and Power Utility verticals at Cisco. Over the last four years, Serhii has been working closely with major Energy vertical companies on design of industrial automation and control network infrastructures and implementation of security policies. Serhii has MS in Computer Science from National Technical University of Ukraine, and completed CCIE and CISSP certifications. He is the author of three books and eight scientific publications.

Dr. Nate Kube, Co-founder and Chief Technology Officer, Wurldtech™ Security Technologies

Dr. Nate Kube is Co-founder and CTO of Wurldtech™ Security Technologies, Inc. where he oversees the development of advanced security technologies for the SCADA and process control domains. He is an expert in formal test methods, embedded systems testing, functional and declarative languages, and fault-tolerant computing. Dr. Kube has co-authored a number of best practices for the Industrial Automation Security sector, is a voting member of ISA SP99, and his research efforts have been heavily funded by Canadian, American, and International Government agencies. Dr. Kube holds a BSc in Mathematics and PhD in Computer Science.

Teja Kuruganti, R&D Staff Member, Modeling and Simulation Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory

Teja Kuruganti is a R&D Staff Member of the Modeling and Simulation Group in the Computational Sciences and Engineering Division at Oak Ridge National Laboratory. His research interests include wireless sensor networks for harsh environments, modeling and simulation of wireless propagation in harsh environments, modeling control systems that operate over communication networks, and collaborative signal and information processing in sensor networks. He received his MS degree in Electrical Engineering from University of Tennessee, Knoxville working on developing novel computing paradigms for information processing in distributed sensor networks. He is currently pursuing a PhD from University of Tennessee, Knoxville.

Ronald Lambert, Lead Consultant, Integration Services, LiveData

Ronald Lambert is the Lead Consultant, Integration Services with LiveData, Inc. Ron has over 12 years of experience integrating disparate real time and near real time utility systems. In his role at LiveData, Ron uses the LiveData RTI Server to unobtrusively establish real time bi-directional data flows between intelligent devices, SCADA/EMS/DCS, and other critical IT & Business systems.

Before joining LiveData in 2006 Ronald was a Lead Systems and Application Integrator with Oracle Utilities (formerly SPL World Group). Ron holds a BS in Electrical Engineering Control Systems from Michigan Technological University.

Ulf Lindqvist, Program Director, SRI International

Dr. Ulf Lindqvist manages R&D projects in enterprise and infrastructure security and leads SRI's Cyber Security R&D Center for the US Department of Homeland Security. Dr. Lindqvist's expertise includes development of efficient and generic methods for analysis, modeling, categorization, and automatic real-time detection and correlation of computer misuse. He has more than a dozen publications in the computer security area, many of which are bridging the gap between theoretical and applied research, and he holds one patent. Dr. Lindqvist is a member of the Executive Committee of the Institute for Information Infrastructure Protection (I3P), a consortium of leading national cyber security institutions, including academic research centers, government laboratories, and non-profit organizations. He holds a PhD in computer engineering and an MS in computer science and engineering, both from Chalmers University of Technology in Sweden.

Art Manion, Internet Security Analyst, CERT Coordination Center

Mr. Manion leads the Vulnerability Analysis Team at the CERT Coordination Center (CERT/CC) at Carnegie Mellon University. In this role, he supervises technical analysis, interactions with stakeholders, and coordination and disclosure of vulnerability information. Mr. Manion has written advisories, alerts, and vulnerability notes for CERT/CC and US-CERT. He also researches new ways to manage vulnerability information, decision making, economic factors of vulnerability disclosure, and ways to improve software quality and security. Prior to working at the CERT/CC, Mr. Manion was the director of network infrastructure at Juniata College. He received a BS degree from Penn State University in quantitative business analysis.

Chris Martin, Senior Director Product Management, Industrial Defender, Inc.

Chris Martin, Senior Director Product Management, is responsible for leading the strategies for all of Industrial Defender's product and services portfolio. Chris has almost 20 years experience in the high technology space, including 15 years experience in the industrial automation industry, working for leading control systems vendors such as GE Fanuc, Intellution, Schneider Electric and Honeywell. Chris has a diverse background in product management, product marketing, corporate marketing, business development and engineering.

Chris holds an MBA in Marketing from Temple University in Philadelphia and earned a BS in electrical engineering from the University of Massachusetts at Amherst.

Thomas Maufer, Director, Technical Marketing, Mu Dynamics, Inc.

Thomas Maufer is Director of Technical Marketing for Mu Dynamics, Inc. He has held various marketing and engineering/architect roles at NVIDIA and 3Com for networking products ranging from NICs up to routers. He also managed LAN and MAN connectivity for NASA's Goddard Space Flight Center, has written 3 books and has been awarded 15 patents in the field of computer networking.

Sean McBride, Cyber Security Researcher, Idaho National Laboratory

Sean McBride is a Cyber Security Analyst at the Idaho National Laboratory (INL). Sean's research includes situational awareness, threat analysis, and vulnerability characterization. Prior to his position at the INL, Sean received a Master of Business Administration degree from Idaho State University where he studied under the National Science Foundation Cyber Corps program. Sean is also a Certified Information Systems Security Professional.

Robert McComber, Product Security Specialist, Telvent

With six years at Telvent, three in his present capacity, Robert is responsible for developing enhanced product security models across Telvent's different product groups. Working with a strong team of security and development professionals, Rob ensures that products are securely architected and are deployed to minimize risk to Telvent's customers and to provide the highest level of regulatory and best practice compliance possible. Robert is also responsible for a number of internal security projects and manages Telvent's external security relationships.

Robert holds certifications from Microsoft and the SANS Institute and has presented at numerous events across different industries and in multiple countries. He holds a Bachelor of Arts in Political Science from the University of Calgary and currently sits on the governing board of the Control System Cyber Security Vendor Forum.





Kevin McGrath, Scientist, ABB, Ltd.

Kevin McGrath is a scientist at ABB Corporate Research, where he leads research and development activities to automate its on-going security and robustness testing. Prior to joining ABB, Kevin received a scholarship to pursue a research Master's degree at the University of Limerick (Ireland), where he researched tamper proof communication protocols and forensic analysis of anomalous wireless traffic.

Jeff Morgan, Process Control Systems Analyst, Cyber Division, Federal Bureau of Investigation

Jeff Morgan is a Process Control Systems Analyst in the FBI's Cyber Division. He holds a degree in Information Management from the Marriott School of Business at Brigham Young University and has 22 years experience in information and telecommunication systems design, installation, maintenance, and management in the Healthcare and Transportation industries.

Kevin M. Nixon, Senior Director, Americas, Integralis

Kevin Nixon has over 25 years experience in MIS design and development, Information Security, Business Continuity & Disaster Recovery, and US and European Regulatory Compliance. He joined Integralis in 2008 as a Senior Director and provides coverage for a wide area of responsibilities. Internally, Kevin leads initiatives in Consulting & Professional Service arena, provides staff education on Governance, Risk, & Compliance (GRC) specific to public policy, legislative and regulatory which influence Integralis' product offerings domestically and internationally. In addition to his primary role in Integralis' Consulting & Professional Services Team, Kevin also leads internal projects related to Governance, Audit, Policies & Procedures, and Continuity.

Kevin is a Master Security Architect (MSA), a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and attended the SMU Cox School of Business.

David Norton, Policy Consultant – CIP, Entergy Transmission

Mr. Norton currently holds the Electric Sector seat on the Process Control Systems Forum Board of Governors. He is a Certified Information Systems Security Professional (CISSP) with 30+ years experience in technical leadership positions in information technology, manufacturing automation, electric sector EMS/SCADA, and real-time military and intelligence environments. He was one of the drafters of the CIP Cyber Security Standards, and in compliment has played a leadership role on the SERC Cyber Security Compliance Review Subcommittee engaged in compliance measurement of the CIP Standards he helped develop. Within Entergy, he is leading implementation of a next generation high-speed digital communications networking architecture of his design to support substation automation (e.g., IEC 61850) and a move to new EMS/SCADA platforms. This experience has brought an end-user perspective to the Sandia OPSAID project aimed at creating a reference implementation of next generation TCP/IP protocols and related security improvements for PCS/DCS environs. Finally, Mr. Norton has actively worked with authorities at the local level to identify lessons learned and needed improvements to first-responder command and control systems in the wake of Hurricanes Katrina and Rita.

Chris Paul, Founder/Counsel, Joyce & Paul, PLLC

Mr. Paul focuses his practice on transactional and regulatory matters, including related litigation. He provides counseling to refining, manufacturing, and transportation operations on subjects including liabilities and exposures, regulatory and compliance programs, risk management, and development of training and management systems. He has extensive experience with pipeline issues, including transactions, integrity programs, SCADA auditing, contracting, and emergency response and litigation. Chris is admitted to practice in Oklahoma, Pennsylvania, Arkansas and Kansas, the US Supreme

Court, and various US District Courts. He is also an instructor on Oklahoma State University's Environmental Management Program. Prior to his present practice as an attorney and counselor, Chris worked in-house with Sun Company and as the environmental manager of its Tulsa Refinery. Prior to his commercial endeavors, Chris was a United States Army JACG lawyer with the Seventh ID(L) and a Special Assistant United States Attorney.

Daniel Peck, Offensive Security Researcher, Digital Bond, Inc.

Mr. Peck is a key participant in Digital Bond's control system research projects where he attacks applications, devices and systems to simulate a sophisticated attacker's actions. Prior to joining Digital Bond, he was a security researcher for SecureWorks where he analyzed attacks, vulnerabilities, and malware as well as developing protection and detection mechanisms for their managed service clients. He has a BS in Computer Science from the Georgia Institute of Technology.

Raphael Pereira, Security Officer, Chemtech – A Siemens Company

Mr. Pereira is currently head of information security for Chemtech – A Siemens Company, Rio de Janeiro, Brazil. His responsibilities include the internal Security Office, protecting internal information assets, and reports to the organization board. Additionally, he is the manager of internal implementation of Information Security Management System compliance for ISO:IEC 27001:2005.

Leandro Pflieger de Aguiar, Computer Security Analyst/Network Specialist, Chemtech – A Siemens Company

Leandro graduated with a degree in Information Systems from the Federal University of Santa Catarina (UFSC), Brazil and an Industrial Electronics degree from the Federal Center for Technological Education of Santa Catarina (CEFET-SC), with specialization in Microprocessed Systems. Currently he is pursuing a Master's degree from the Federal University of Minas Gerais (UFMG) while working for Chemtech as a Computer and Network Security Specialist developing projects in the industrial area. During his time at Chemtech, Leandro has already worked on several projects for several large companies, developing cases that emphasize the growing need for information security in such environments. Before Chemtech, he worked with cryptography and PKI, developing systems and libraries to improve security levels of well known market applications.

Venkat Pothamsetty, Business Development Manager, Cisco

Venkat Pothamsetty is an industrial control systems security expert. He has been working in the area of industrial control systems for the past five years. He has authored several papers in the area and is the author of the industry first SCADA firewall (<http://modbusfw.sf.net>) and industry first SCADA honeynet (<http://scadahoneynet.sf.net>).

Venkat has been working at Cisco for the past eight years. He started as a security engineer in Cisco's Security Technologies Assessment Team and joined Critical Infrastructure Assurance Group as a research engineer. He is now a Business Development Manager in Infrastructure Security Research and Development Team. Venkat has a MS in computer science from Wright State University and a MBA from University of Texas at Austin.

Jeff Potter, Security and IT Integration Manager, Emerson Process Management

Jeff Potter is a member of Emerson Process Management's Wireless team, specializing in Security and IT integration issues. Prior to joining Emerson in Chanhassen, MN, he worked for Chevron for 24 years in a wide range of US and international positions involving upstream Oil & Gas technology development, delivery, and support.

Jeff was actively involved in the security aspects of the HART7 specification, is chair of the ISA100.11a Security Task Group and is an informational member of the ISA99 Working Group.

Ernest Rakaczky, Principal Security Consultant, Enterprise Architecture & Integration, Invensys Process Systems

Ernest Rakaczky is currently the Principal Security Architect for Invensys Process Systems and a key member of the Control Security Team, in this position; Mr. Rakaczky manages the overall development and implementation of the Customer Support infrastructure and Support Services to meet today's current Security needs. Mr. Rakaczky also participates in the efforts underway at ISA within SP99, NIST within PCSRF, MSMUG and plays an active role in the various Security initiatives with DOE, DHS, INL, NRC, IAEA, PCSF and SANDIA, with most recently being appointed to the PCSF Governing Board as the Control Vendor Community representative. Founding member to the Canadian Industrial Cyber Security Council, with most recently be appointed by Public Safety Canada to chair an active working group to define the Cyber Security Requirements for the Canadian Critical Infrastructure. With the formation of the ISA Security Compliance Institute (ISCI) has been elected as the Marketing Chair of the initial Governing Board.

Mr. Rakaczky has played an active role within the Process Control arena for over 30 years, his focus and efforts during this time have always been with a Customer Support role. From his early years with ABB (AccuRay) to his current role at Foxboro, Mr. Rakaczky has leveraged his Customer focus to ensure an understanding of their requirements, expectations, and business drivers are part of every Support Solution being introduced. Within his various support roles, he has had the opportunity to gain knowledge of the various Industry processes, requirements and synergies.

Daniel C. Rees, Vice President, Scientech – A Curtiss-Wright Flow Control company

Mr. Rees, is a Vice President with Scientech. Mr. Rees served as one of the lead designers of the Vulnerability Self-Assessment Tool (VSAT™) for both Water and Wastewater Systems, developed for the Association of Metropolitan Sewerage Agencies under a grant from the USEPA. He has led the VAs of several wastewater and water utilities including the update of their ERPs and development of their master security plan. He has also conducted several workshops on the VSAT™ methodology and software usage for the Water Environment Federation. He was recently involved in the RAMCAP development for the Water Sector and performed pilot applications of RAMCAP using a modified VSAT™ at four utilities. He has performed numerous vulnerability assessments for utilities, including water and wastewater facilities, nuclear generating plants, and coal-fired electric facilities. He has also performed risk assessments for petrochemical plants, oil and gas facilities, government buildings, and other high-risk facilities throughout the world. He has been responsible for management of complex risk assessment projects for utilities, nuclear power plants, petrochemical complexes, and other high-risk facilities throughout the world, including security vulnerability and risk assessments and emergency plan development, upgrades and testing.





Al Rivero, PE, Director, Profesional Services, Telvent

Al Rivero has worked in the petrochemical industry for almost 30 years in a variety of assignments, ranging from project engineering, staff consulting positions to managing technology in a variety of organizations within the Telvent and Chevron family. He has run a successful consulting practice facilitating system integration for his clients. Mr. Rivero has a strong foundation in oil and gas operations, electronic controls, automation, communications, and information technology. He is currently Director of Business Development for Telvent's Energy Group working with clients to develop an integrated strategy toward their IT infrastructure and to facilitate system integration. Mr. Rivero has a Bachelor's degree in Mathematics from the University of California at Irvine (UCI) and an Electrical Engineering degree from Cal State Fullerton (CSF).

Tim Roxey, Technical Assistant to the Vice Chairman, Constellation Energy & Deputy Chairman, Nuclear Sector Coordinating Council (NSCC)

Tim Roxey is the Deputy to the Chair for the Nuclear Sector Coordinating Council and also the Technical Assistant to the Vice Chair for Constellation Energy. Mr. Roxey has 27 years of experience in the nuclear utility industry serving in organizations such as Operations, Information Technology, Licensing, Security, among others. Mr. Roxey also has over 30 years of computer related experience working on many different OS's and in many different languages.

In his present position as Deputy Chair of NSCC and his TA role for the Vice Chair of Constellation Mr. Roxey is involved in a variety of both physical and cyber security related issues across the entire nuclear sector of the United States. Mr. Roxey also serves by invitation on two Presidential Commissions helping to prepare guidance for the next administration.

In early 2007 a difficult Cyber vulnerability was brought to the attention of the Private Sector through a series of briefings from the US Department of Homeland Security. These briefings led to Mr. Roxey being given the leadership position for the entire private sector on the newly disclosed control systems vulnerability called Aurora. In this capacity Mr. Roxey has interacted with many different Federal organizations including Congressional Committees, the White House, DOE, DoD, NERC, FERC and the NRC.

Craig Schiro, I&C/Secure Networks, Exxon-Mobil

Mr. Schiro has 29 experience in Refining and Chemicals. His current assignment is: EMDC Facilities Engineering; Instrument Control Electrical (ICE) Function, and Control Systems / Secure Network Engineering. Mr. Schiro has 20 years experience with Exxon USA Refining, 5 years as President, InfoTech Engineering Co. LLC, and 4 years EMDC ICE Function. Mr. Schiro earned a BS in Electrical Engineering from Louisiana State University.

Bryan Singer, Vice President of Security Services, Wurldtech™ Security Technologies

Bryan Singer was named Vice President of Security Services of Wurldtech™ in 2007 and is charged with leading the security team focused on improving the overall reliability, efficiency, and security of the systems and networks that operate industrial automation and critical infrastructure worldwide.

Mr. Singer joined Wurldtech™ from FluidIQ's where he led the development and implementation of specialized security services for more than 3,000 industrial facilities worldwide, across numerous vertical industries. Prior to joining FluidIQ's, Mr. Singer was the Manager of Network and Security Services at Rockwell Automation. He began his professional career with the US military focusing on issues such as physical, systems, network security, and force protection. Since that time, he has worked in software development in over 25 professional coding languages; worked in UNIX and mainframe systems; supported large scale ERP, MES, LIMS, and SPC implementations; and has spent significant time in cyber security projects focusing on risk analysis, vulnerability testing, penetration testing, risk mitigation strategies, and enterprise architecture and design including technical and policy-based countermeasures and remediation strategies. Mr. Singer is the founding chairman and now co-chairman of ISA SP99, Industrial Automation and Control Systems Security Standards Committee, a standards body focusing on the security issues of the control systems environment. He is also a US Technical Expert to multiple IEC standards bodies, a representative to the Idaho National Labs Recommended Practices Commission, a previous board member to the Process Control Systems Forum (PCSF), and is active globally as an industry advocate in industrial security and critical infrastructure protection. Mr. Singer has over 16 years experience working in industrial automation and critical infrastructure sectors such as Power & Energy, Oil & Gas, Transportation, and Water. Mr. Singer has a Bachelor's degree in Computer Information Systems from Phoenix University and holds the CISSP and CISM certifications.

Paul M. Skare, Director, Security & Deployment, Siemens

Paul M. Skare (Minnetonka, MN) is the Director of Security & Deployment for Siemens Power Transmission and Distribution. Paul is responsible for product Cyber Security, Standards, Patents, and deploying products from development out to projects. Paul has been a Product Manager of SCADA/EMS and Substation Automation Products. Paul is the Convenor of IEC TC57 Working Group 19 (Architecture, Harmonization) as well as a member of WG13 (CIM) and WG15 (security). Paul is in numerous cyber security groups and has twice testified to the US Congress about cyber security and control systems.

Rhett Smith, GSEC, CISSP, Development Manager, Schweitzer Engineering Laboratories, Inc.

Rhett Smith is a Development Manager for the security solutions group at Schweitzer Engineering Laboratories, Inc. (SEL). In 2000, he received his BS degree in Electronics Engineering Technology, graduating with honors. Before joining SEL, he was an application engineer with AKM Semiconductor. Rhett has his GSEC, GIAC Security Essentials Certification, and is a Certified Information Systems Security Professional (CISSP).

Larry Spoonemore, IT Business Analyst, Southern Company Services

Information Technology Generation

Staff Analyst: Responsible for the Leadership and Strategic direction of Southern Company's Plant Cyber Security Program developed to protect critical infrastructure

Background

- Information Technology (IT): Managing the application of Information Technology to the business processes of Electric Generating plants
- Digital Control Systems (DCS): Managing the engineering design and installation of control systems for the purpose of controlling power plant operations and energy management
- Related experience and education: 30+ years Power Plant Instrumentation & Controls design and support, electrical engineering design, computer systems design, and critical infrastructure protection

Kevin Staggs, Engineering Fellow, Honeywell Process Solutions

Kevin is a 31 year employee of Honeywell. He has 25 years of experience in the engineering of control systems as either a hardware, software or systems engineer. In Kevin's current position as the Global Security Architect he is responsible for the security architecture for all of Honeywell Process Solutions products. He is also responsible for defining the security processes and architectural methodology so that all HPS products are designed for security. Kevin has been involved in system security since Honeywell first introduced open system platform based products. He was the lead system engineer and architect for Honeywell's HP-UX based UxS product which was introduced in the early 1990s. He defined the original high security model which was deployed as part of Honeywell's TPS system in 1996. In addition to his day job, Kevin is also co-chair of ISA SP99 Working Group 4 which is defining technical security requirements of Industrial and Automation Control Systems and he is the Technical Chairman of the ISA Security Compliance Institute.

René Struik, Cryptographic Standards Specialist, Certicom Corporation

Dr. Struik has been with Certicom Research since 2001. Over the last five years, he has gained considerable insight and experience in security and trust lifecycle aspects of sensor and control networks, both from a research perspective, from active standardization participation, e.g., with IEEE 802.15.4, ZigBee, and ISA SP100.11a, and from discussions, e.g., with the energy and utility sectors. His other interests include efficiency improvements for cryptographic and security building blocks, trust lifecycle management, and "security and ease of use." René holds an MSc degree in Computer Science and a PhD degree in Mathematics, both from Eindhoven University of Technology, The Netherlands.

Kevin Sullivan, Senior Security Strategist, Trustworthy Computing-Critical Infrastructure Protection, Microsoft

Kevin Sullivan is a Senior Security Strategist with Microsoft's Critical Infrastructure Protection program in the Trustworthy Computing group. The goal of the Critical Infrastructure Protection program at Microsoft is to improve infrastructure security and resiliency worldwide by aligning Microsoft technology, capabilities, and strategy with stakeholders' needs. Kevin earned a Bachelor of Science in Information Science from Northeastern University. He also holds the MCSE: Security, CISSP, and ITIL Foundation certifications.

David Teumim, Consultant, Teumim Technical, LLC

Mr. Teumim is an independent consultant specializing in control systems security. He has taught seminars and chaired conferences for ISA in this area, and he has written the first book on this subject, *Industrial Network Security*, which was published in 2004 by ISA Press. Mr. Teumim has a Master's degree in chemical engineering and is certified as a CISSP. Recently, he has focused on the application of control security to the area of rail transit.





Michael Torppey, PCSF Program Manager & Manager, Noblis, Inc.

Mike Torppey is a manager with Noblis and program manager of the Process Control Systems Forum (PCSF). He has more than 10 years of information technology management experience and is an accomplished software engineer. As director of operations with Victory Springs, Inc., he directed the development, production and testing, and maintenance programs behind Smart E-Records™, a Web-enabled medical records portal application.

Mr. Torppey has presented at numerous meetings and symposia on topics including information technology, requirements planning, application design, health-care technology, and the Process Control Systems Forum. He holds a Bachelor of Arts degree in economics from Rutgers University.

Avner Truniansky, Director of Product Marketing, Waterfall Solutions, Ltd.

Following a military career spanning two decades, Avner has held several product management and business development posts before joining Waterfall Solutions, accumulating almost 25 years of employment in communications and networks' protection and security. He holds a BSc and MSc in Chemistry from the Hebrew University and has lectured on science, communication, and security issues at international conferences and events.

Zachary D. Tudor, CISSP, CISM, PMP; Program Director, SRI International

Zach Tudor is currently a Program Director in the Computer Science Laboratory at SRI International. Zach supports operational and research and development cyber security programs for the US Department of Homeland Security.

Prior to his work at SRI, Zach led a team of cyber security engineers and analysts directly supporting the Control Systems Security Program (CSSP) at the National Cyber Security Division of DHS, whose mission is reducing the cyber security risk to critical infrastructure control systems in the US and its strategic partners world wide. He has held several senior-level consulting positions, including Vice President of SAIC's Enabling Technology Division and Senior Manager for Department of Defense programs at BearingPoint's Security Practice. Zach is a retired US Navy Submarine Electronics Officer, where he served in numerous technical and management positions at sea and ashore.

Al Valdes, Senior Computer Scientist, SRI International

Alfonso Valdes has led or participated in several research projects in information security for such clients as the Defense Advanced Research Projects Agency (DARPA) and the Advanced Research and Development Activity (ARDA), and the US Department of Homeland Security. He is an expert on statistical algorithms for detection and modeling and the application of such techniques in the information security arena. He has led statistical algorithm development in SRI's Next-Generation Intrusion Detection Expert System (NIDES) and later EMERALD. Mr. Valdes has implemented a high-speed Bayes component to detect network intrusions, as well as an innovative probabilistic approach to correlation of reports from heterogeneous intrusion detection sensors. He holds two patents in the field of computer intrusion detection. Over the last three years, he has taken an interest in the security of critical infrastructure systems such as the distributed control and SCADA systems that operate refineries and pipelines in the Oil and Gas sector.

Mr. Valdes is also an expert on a wide variety of statistical and classification techniques, including likelihood theory, decision analysis, neural networks, simulation, and Bayesian formalisms. He has applied these methods with great success in a number of problem domains, including signal processing and environmental and medical sciences, in addition to information security.

Steve Venema, Associate Technical Fellow, The Boeing Company

Steven Venema is an Associate Technical Fellow at The Boeing Company, working in the Architecture and Networked Systems organization of Boeing Phantom Works. Before joining Boeing, he earned his MS and PhD degrees in Electrical Engineering at the University of Washington where his research focused on real-time control systems, robotics, and haptic simulation. At Boeing, his work the past several years has focused on information technology, networks and security – particularly as they relate to manufacturing systems. He is the systems architect behind the development and ongoing deployment of Boeing's new Network Location Service, an enterprise-wide service for supply chain, asset, and work-in-process visibility. His recent work has focused on addressing the growing need for scalable, secure connectivity for controls and SCADA devices over shared enterprise and even public network infrastructure.

Jules Vos, Programme Manager, Process Control Architecture, Shell Global Solutions International

Jules has over 20 years of experience in process control, mainly gained in the capital-intensive industry. His professional development includes different angles. It includes 12 years of hands-on DCS programming as engineer and technical project lead of automation projects in the Oil & Gas industry as well as over 10 years of IT consultancy and project management experience.

This combination of IT consultancy skills and in-depth process control knowledge forms a solid basis for his current role as implementation programme manager of the evolved Shell exploration and production process control architecture standard.

Apart from his responsibility as implementation programme manager, Jules has made a considerable contribution to the development of the Shell process control domain security standards.

He always has had a warm interest in integration of the process control domain and business administration domain. Jules has been chairman of a Dutch platform that aimed for providing guidance for beneficial integration of these domains.

Jim Watters, Lead INFOSEC Engineer, The MITRE Corporation

Jim Watters has 11 years of INFOSEC experience, mainly involving risk assessments and security certification of Air Force systems. His is a primary developer of RiskMAP (Risk-to-Mission Assessment Process). Jim holds a BS in Aeronautical Engineering and an MS in Astronautical Engineering. He has worked in space launch operations, flight test engineering, and satellite communications test and integration before joining MITRE in 2000 and concentrating on INFOSEC projects.

Rita Wells, Energy Sector Lead, Idaho National Laboratory

Rita Wells is the Energy Sector Lead for supervisory for the Critical Infrastructure Protection/Resilience division at the Idaho National Laboratory. She is responsible for making the technical decisions, strategy, and direction of testing and assessment activities at the Supervisory Control and Data Acquisition (SCADA) and control systems test beds. Rita has worked with the Federal Energy Regulatory Commission, US Department of Homeland Security, US Department of Energy, and industry (vendors and asset owners), and other entities as a subject matter expert for cyber security of control systems for four years. She has worked at the lab for 18 years and has served as a technical lead for integrating control systems into a data management system for transuranic waste which resulted in 2 national awards for the product developed. Her process control experience includes the training simulator for the advanced test reactor, HVAC for nuclear waste storage facilities, and command and control for military projects. Rita has served as a subject matter expert for networks and security for a large military integration program. Prior to the lab, she worked for a university computer center responsible for their network infrastructure while getting her degree in Computer Information Systems.

Jeff Whitney, Founder/Principal, Berkana Resources Corporation

Mr. Whitney is an entrepreneur and computer professional with over 25 years of management and technical experience in Real Time (Mission Critical) Process Control Systems. He has extensive experience assisting pipeline companies with SCADA system integration, SCADA security, SCADA consulting, and Compliance. His SCADA experience includes Pipeline Control Center consolidations, SCADA system migrations, SCADA system upgrades, SCADA Security audits, and Industry and Regulatory Compliance for major Oil & Gas Companies. He currently serves on several non-profit boards, as well as the University of Houston Industrial Advisory Board, and is an owner/principal of Berkana Resources Corporation (BRC). BRC provides integration, security, compliance, and audit services to customers utilizing Supervisory Control and Data Acquisition (SCADA) applications. As an independent integrator, BRC provides these services using a wide range of SCADA applications in the Oil & Gas, Water, and Utilities markets.

Andrew Wright, Chief Technology Officer, N-Dimension Solutions, Inc.

Andrew holds a PhD in Computer Science from Rice University. He has published over 20 technical papers and has 16 years of experience in industrial research and development. Prior to joining N-Dimension, he was a Technical Leader in Cisco's Critical Infrastructure Assurance Group (CIAG) where he developed cyber security solutions for critical infrastructure, particularly Industrial Control Systems and SCADA. He established the Cisco Secure Control Systems lab in Austin TX, was the key architect of the AGA-12 serial SCADA encryption protocol, and was a founding developer of CVSS, the Common Vulnerability Scoring System. He is currently working with IEEE working group 1711 to standardize AGA-12 as an IEEE standard, with Idaho National Lab to develop best practices for securing industrial control networks, and with ISA's SP99 Working Group 4 on secure control system requirements.





**Process Control Systems
Industry Conference**

3150 Fairview Park Drive South, MS F310
Falls Church VA 22042
www.pcsforum.org