KENEXIS

# Professional Profile

## *Jim Gilsinn, CEH, CISSP*

***Principal Consultant, Kenexis***

### Fields of Competence

- Industrial Control Systems (ICS)
- Cyber Security
- Networking and Wireless
- Network Security Monitoring (NSM)
- Security Incident and Event Management (SIEM)
- Software Architecture and Development

### Experience Summary

Mr. Gilsinn is the Principal Consultant for ICS and cyber security at Kenexis, leading a team of experts in assisting customers with developing, designing, and assessing secure and reliable ICS. He has over 25 years of engineering experience including over 15 years in ICS network performance and cyber security. Mr. Gilsinn's background focuses on control systems, software architecture and development, standards development, test tools, network performance, cyber security, wireless networking, system administration, and web development. Mr. Gilsinn's industry experience includes discrete part manufacturing, oil & gas, nuclear and other electrical power generation, transmission and distribution, automotive, and petro-chem.

At Kenexis, Mr. Gilsinn has conducted both standards-based conformance assessments as well as technical vulnerability assessments and penetration tests for ICS/SCADA customers. He has also helped ICS/SCADA customers develop security programs based upon ISA/IEC 62443, ISO/IEC 27001 and 27002, NIST SP800-53/82, NIST Cybersecurity Framework, NEI 08-09, and NERC CIP.

Mr. Gilsinn's research efforts are in network security monitoring (NSM), including the developing performance and network reliability monitoring software, Dulcet Analytics. This software is capable of building a baseline of ICS/SCADA network reliability and performance utilizing network capture data along with mathematical and statistical analysis. It is also capable of comparisons against the baseline for anomaly detection.

Before joining Kenexis, he spent the first 20 years of his career at the U.S. National Institute of Standards and Technology (NIST). He worked on a variety of projects including autonomous vehicles, automated welding systems, sensor development, system integration, wireless smart sensors, industrial Ethernet network performance, and industrial cyber security.

He is also the Co-Chair of the ISA99 committee on Security for Industrial Automation and Control Systems (IACS), the Co-Chair of ISA99 Working Group 2 developing an IACS security program based upon the ISO/IEC 27001 and 27002 standards and a Managing Director with the ISA Standards & Practices Board.

### Credentials

- Certified Ethical Hacker (CEH) v8
- Certified Information Systems Security Professional (CISSP) # 559905
- ISA/IEC 62443 Cybersecurity Expert
- Masters of Science in Electrical Engineering, Johns Hopkins University
- Bachelors of Science in Electrical Engineering, Drexel University

### Affiliations

- Co-Chair, ISA99 Committee
- Co-Chair, ISA99 Working Group 2 on IACS Security Program
- Managing Director, ISA Standards & Practices Board
- Organizing Committee, BSidesDC Conference

### Key Assignments

- Team lead and project manager for integrating a security information and event management (SIEM) system for multiple nuclear power generation facilities.
- Certified Process Control Network (PCN) Conformance Assessor for a large oil & gas customer conducting assessments against the NIST Cybersecurity Framework for various facilities within their organization.
- Developer for the Kenexis Dulcet Analytics network reliability monitoring software for ICS/SCADA.
- Developed facility and enterprise industrial DMZ architecture for a major international food and beverage manufacturer.
- Evaluated a network segmentation device vendor's product line to build a capability security level list against the foundational and system requirements in ISA-62443-3-3.
- Conducted security and network assessments on industrial customers from the water & wastewater, automotive, and chemical manufacturing industries.
- Developed disaster scenarios and use cases for cyber security utilized by a major industrial insurance corporation.
- Developed the Security Level Vector concept used in ISA-62443-3-3 for representing different aspects of security as increasing levels to aid end users during their risk assessment process engineering the cyber security solution.

KENEXIS

# Professional Profile

## Selected Presentations

- *Practical Uses of Cyber Security Standards*, ISA Cleveland Conference and Exposition, March 2017
- *Practical Approaches to Securely Integrating Business and Production*, 201 ISA Process Control & Safety Symposium, November 2016
- *What's the Big Deal with Assessing ICS/SCADA?*, BSidesDC 2017, October 2017
- *ICS Cyber Security & Remote Maintenance*, FlexThink Tech Conference, October 2016
- *Network Reliability Monitoring Using Statistical Modeling and Data Analysis to Measure the Health and Security of ICS,* 71st Annual Instrumentation and Automation Symposium for the Process Industries, January 2016
- *Mechanics of an ICS/SCADA Man-In-The-Middle Attack,* 2015 BSidesDE Conference
- *Network Reliability Monitoring for ICS: Going beyond NSM and SIEM,* 2015 BSidesDC Conference
- *Integrating the Alphabet Soup of Standards,* 2014 ICS Cyber Security Conference
- *ICS Performance Analysis,* 2014 ISA Process Control & Safety Conference
- *ICS Cyber & Process Attack Scenarios,* OPC Foundation 2014 Innovation Revolution
- *Using Cyber Vulnerability Assessment During for a Turnaround,* 2014 Emmerson Exchange
- *System-Level Cyber Security vs. ISA 62443-3-3,* 2014 Spring ICSJWG
- *Low-Cost ICS Network Performance Testing,* SCADASides 2014
- *You Name it, We Analyze It!,* 2014 S4 Conference
- *Rorschach Plots and Network Performance Analysis,* 2013 BSidesDC Conference
- *Process Control Cyber Security,* 2013 Saudi Aramco Global Reliability Forum
- *Network Packet Analysis with Wireshark,* 2012 ISA Safety & Security Symposium
- *Test Tool for Industrial Ethernet Network Performance,* 55th International Instrumentation Symposium (Best in Show)

## Selected Articles and Technical Papers

- *Network Reliability Monitoring: Measuring the Health & Security of ICS Networks*, Kenexis White Paper
- Gilsinn, J., *"Network Reliability Monitoring Using Statistical Modeling and Data Analysis to Measure the Health and Security of ICS,"* Proceedings from 71st Annual Instrumentation and Automation Symposium for the Process Industries, January 2016
- Gilsinn, J., Schierholz, R., *"Security Assurance Levels: A Vector Approach to Describing Security Requirements,"* ISA Automation Week 2011
- Gilsinn, J., Johnson, F., *"Test Tool for Industrial Ethernet Network Performance,"* 55th International Instrumentation Symposium, 2009.
- Gilsinn, J., Knake, K., *"EtherNet/IP Interoperability Recommendations,"* ODVA 2009 Conference & 13th Annual Meeting
- *Performance Test Terminology for EtherNet/IP Devices, v1.1,* ODVA, March 14, 2005.
- *Performance Test Methodology for EtherNet/IP Devices, v1.0,* ODVA, March 14, 2005.
- Falco, J., Gilsinn, J., Stouffer, K., *"IT Security for Industrial Control Systems: Requirements Specification and Performance Testing,"* 2004 NDIA Homeland Security Conference & Exposition, May 25-27, 2004.
- Gilsinn, J., *"Real-Time I/O Performance Metrics and Tests for Industrial Ethernet,"* ISA Automation West, April 28, 2004.
- Gilsinn, J., *"EtherNet/IP Race Track: Performance Metrics & Testing For Your Industrial Network Interface,"* ISA Ethernet Technical Conference, October 9, 2003.