KENEXIS

Professional Profile

Jim Gilsinn, CEH

- ***Senior Investigator, Kenexis***
- ***Co-Chair, ISA99 Committee***
- ***Co-Chair, ISA99, WG2 Security Program***
- ***Liaison, ISO/IEC JTC1/SC27***

Fields of Competence

- Industrial Cyber Security
- Industrial Networking and Wireless
- Network Performance
- Software Architecture and Development

Experience Summary

Mr. Gilsinn has over 20 years of engineering experience including 14 years in industrial control system performance and cyber security. Mr. Gilsinn's background focuses on control systems, software architecture and development, standards development, test tools, network performance, industrial security, wireless networking, system administration, and web development. Mr. Gilsinn's industry experience includes discrete part manufacturing, automotive, petro-chem, and electrical transmission and distribution.

At Kenexis, Mr. Gilsinn is responsible for designing and assessing secure and reliable industrial control system networks and security programs utilizing his experience with the ISA-62443 and ISO/IEC 2700x series of standards. Before joining Kenexis, he spent the first 20 years of his career at the U.S. National Institute of Standards and Technology (NIST). He has 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 before joining Kenexis Consulting in 2012.

He is also the Co-Chair of the ISA99 committee, the Co-Chair of ISA99 Working Group 2 developing an industrial security program, a Managing Director with the ISA Standards & Practices Board, a subject matter expert in the ODVA EtherNet/IP Implementors Workshop series, and a subject matter expert on the U.S. Department of Energy (DoE) Electricity Sector Risk Management Process.

Key Assignments

- Lead developer of Kenexis Gemini analysis system for mathematical and statistical analysis of ICS networks.
- 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.
- Main developer for two year STTR project for the U.S. Air Force to develop an anomaly detection system for ICS. Designed and developed the system architecture to detect anomalies on the network. Developed the real-time software implemented on an industrial PC for installation on the ICS network. Designed and built the analysis software capable of reporting anomalies. Implemented the system at a water & waste water utility and analyzed the results.
- Developed industrial Ethernet network performance metrics, tests, analysis methodologies, and tools to allow vendors to improve their products and end-users to evaluate products consistently. Built performance testing system utilized by the ODVA performance testing laboratory through a cooperative research agreement. Developed the open-source Industrial Ethernet Network Performance (IENetP) test tool capable of analyzing Wireshark captures for industrial network performance and the Factory Equipment Network Testing (FENT) framework for conducting and analyzing network performance tests.
- Developed the Security Level Vector concept for representing different aspects of security as increasing levels to aid end users during their risk assessment process engineering the cyber security solution.

Credentials

- Certified Ethical Hacker (CEH)
- 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
- ODVA EtherNet/IP Implementors Workshop

KENEXIS

Professional Profile

Presentations

- 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
- Cybersecurity for the Industrial Environment: An Intro to ISA/IEC 62443, 2012 BSidesDE Conference
- Network Packet Analysis with Wireshark, 2012 ISA Safety & Security Symposium
- Test Tool for Industrial Ethernet Network Performance, 55th International Instrumentation Symposium (Best in Show)

Articles and Technical Papers

- Gilsinn, Lee, Michaloski, Proctor, Song, “Factory Equipment Network Testing Framework: Concept, Requirements, and Architecture,” NIST Technical Note 1755
- Gilsinn, Lee, Michaloski, Proctor, Song, “Factory Equipment Network Testing Framework: Universal Client Application, Application Programming Interface,” NIST Technical Note 1754
- 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., Zhou, H., Damazo, B., Fu, J., Silver, R., “Nano-Lithography in Ultra-High Vacuum (UHV) for Real World Applications”, NanoTech2004 Conference, March 9, 2004.
- Gilsinn, J., “EtherNet/IP Race Track: Performance Metrics & Testing For Your Industrial Network Interface”, ISA Ethernet Technical Conference, October 9, 2003.
- Gilsinn, J., Lee, K., Schneeman, R., Huang, H., “Second Workshop on Wireless Sensing: Proceedings”, Sensors Expo & Conference, October 4, 2001, NISTIR 6930.
- Gilsinn J., Damazo B., Silver R., Zhou H., "A Macro-Micro Motion System for a Scanning Tunneling Microscope", World Automation Congress, International Symposium on Robotics & Applications, June 9-13, 2002.
- Gilsinn J., Lee K., "Wireless Interfaces for IEEE 1451 Sensor Networks", SIcon'01: Sensors for Industry Conference, Rosemont, IL, November 5-7, 2001.
- Lee K., Gilsinn J., Schneeman R., Huang H., “First Workshop on Wireless Sensing: Proceedings”, Sensors Expo & Conference, June 4, 2001, NISTIR 6823.
- Rippey W., Gilsinn J., Flitter L., “Networking of Welding Applications: A Tutorial”, Welding Journal, January 2000, pp. 49-53.
- Quinn T., Gilsinn J., Rippey W., “A Welding Cell With Its Own Web Site”, Welding Journal, January 2000, pp. 46-48.
- Gilsinn J., Rippey W., “A Remote Welding Cell That Supports Remote Collaboration”, Ninth International Conference on Computer Technology in Welding, September 29, 1999.