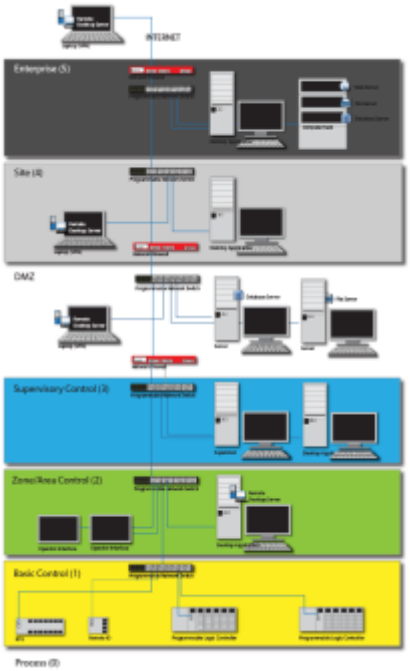
Kenexis Industrial Cybersecurity

Industrial Network Security, Performance & Reliability Services

Industrial Control System protocols are modified Ethernet protocols and were created originally as serial communications before the wide spread use of Ethernet networking. They support proprietary inter-process communications and were built to provide reliable, and deterministic communications long before Ethernet security was a consideration. The Ethernet capable devices like industrial programmable controllers (PLCs) and other industrial controllers including devices like variable speed drives and instrumentation, do not have the capability to protect themselves. In fact, many even lack means of authentication or integrity checking and are vulnerable to potential attack or just mistakes. Consequently, it is up to all of us to protect industrial purpose made controllers from attack using solid, proven engineering and security techniques.

DESIGN & MIGRATION PLANNING

Our Security Services are staffed by seasoned industrial control system experts. Our services start either by designing a robust, secure, and performance based network or by analyzing the design and planning your migration path to your ideal industrial network. Design services are based on solid industrial control system network design with secure communication and reliability as defined in ISA/IEC 62443 and other standards as required by your industry or region of the world. Our design services focus on providing secure and reliable industrial networks that will serve your business well with better visibility, secure remote connectivity, and less unexplained downtime. Kenexis offers industrial cyber security services designed around your process lifecycle to assist your organization with establishing a secure and reliable industrial network throughout the system's lifecycle.



POLICY & PROCEDURE DEVELOPMENT

We work closely with your organization to develop an industrial control system network policy and procedures based on your concerns and the appropriate standards and regulations applicable to your industry and region. We will work with your team to insure agreement, rollout, and adoption. The established policy & procedures will drive security focused behaviors without compromising performance and connectivity. It will also establish a method for budgeting decisions, and accountability.

ACCEPTANCE TESTING

Our team will work with yours to verify that the detailed design as built, meets the security functions defined in the cyber design. These test can be performed onsite for systems/equipment constructed and installed locally or performed offsite where the skid is built. In some cases, it is possible to conduct analysis without actual access; contact Kenexis for more information on remote acceptance testing. Test are designed to prevent the introduction of vulnerabilities into your system.

Kenexis Industrial Cybersecurity

Industrial Network Security, Performance & Reliability Services

COMPLIANCE ASSESSMENT

Our service verifies compliance with either a policy, procedure, standard, or regulation. An assessment can also measure awareness and other attributes on a global scale for large corporations seeking to understand where they should focus. Periodically it is good practice to test both policy awareness and policy compliance. We will work with your team to develop questionnaires and interview strategies as you desire using a variety of methods.

VULNERABILITY ASSESSMENT

A Vulnerability assessment evaluates the ICS network for security, performance, and reliability. Prior to assessment, we typically review network architecture, assets, technologies, data flows, and previous assessments including risks assessments like HAZOP. Vulnerability testing includes passive scanning, and on written request active scanning, for device discovery and service enumeration as well as vulnerabilities. A penetration test can be performed with written permission to pursue vulnerabilities further into the system. Data aggregation and collation is followed by in depth analysis using a variety of tools and Kenexis Dulcet Analytics. We identify vulnerabilities and rank them, remove false positives, and develop prioritized recommendations. Our final report includes asset inventory, vulnerabilities discovered & severity ratings, recommendations, comparisons, overview of tools and methods utilized and findings including the destruction or return of all raw data.

STRATEGIC PLANNING & INCIDENT RESPONSE

If we plan correctly from the beginning, incident response should rarely if ever be required. If required, then our organization can dispatch rapidly to assist your team's response and recovery. Strategic planning can encompass all the above services to insure your industrial network and team are ready to act based on procedure in the event you are attack or a network mishap occurs. Our incident Response service will help you develop a plan including most of the services listed above and assist during an incident. Our incident response focuses on remediating the problem as quickly as possible and not specifically on forensics unless specified in writing. Regardless, we use the same forensics techniques in either case, but emphasis shifts depending on the response requested.

About Kenexis

Kenexis is an independent engineering consulting firm headquartered in Columbus, Ohio, with offices in Houston, Singapore, and Abu Dhabi. Kenexis was established in 2004, and is a privately held. Kenexis clients span the globe in many industries.

Industry Experience:

Oil & Gas, Petrochemical, Chemical, Pharmaceutical
Power Generation including Nuclear, Gas, Coal, and Hydro
Manufacturing including Automotive, Metal, Food & Beverage
Transit including Rail, Shipping, and Terminals
Government & Municipalities including Military, Research,
Water & Wastewater