

SCADA Security & Reliability

Industrial Network Security, Performance & Reliability Services



Industrial control system cyber security should be treated as an engineering problem, and it can be solved. Considering the industrial process, business concerns, and associated risks, we are able to work with you to create a robust industrial network.

Without a solid network design that considers secure communication and reliability, all the device patches and vendor upgrades in the world won't solve the problem. A well-designed network will serve business well with better visibility; secure remote connectivity, and less unexplained downtime.

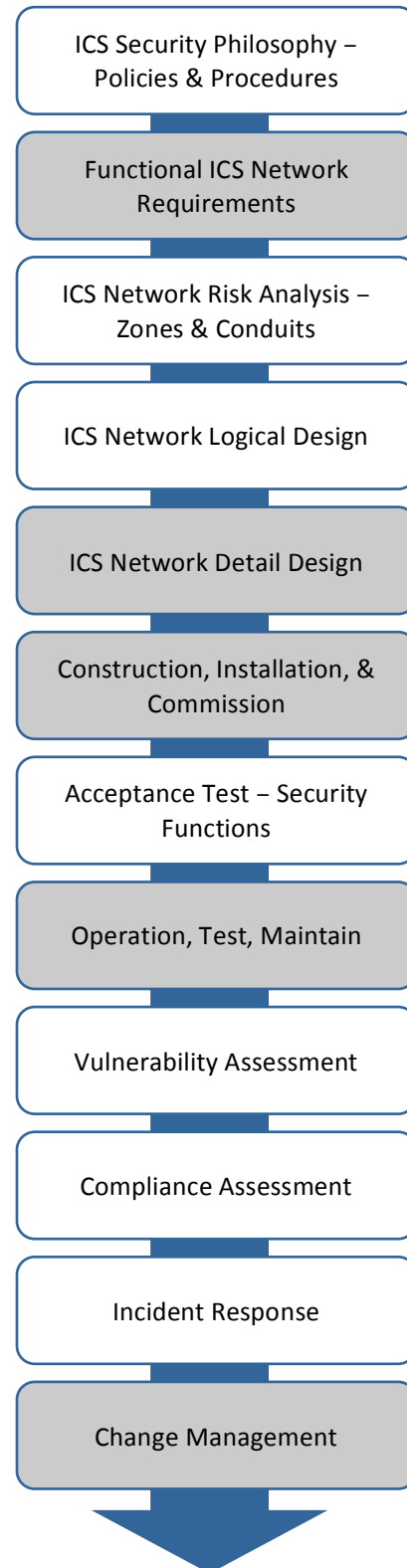
The process for solving this challenge and maintaining a secure and reliable network begins with awareness. The organization needs to establish an executive-sponsored corporate philosophy including tolerable risk, policies, and procedures. Once these objectives are understood and a functional network requirement is available, the network (and associated processes) should be analyzed for risks so that adequate protections can be built into the system. Mechanical devices like over speed trips, over pressure reliefs, and temperature shutdowns should be applied before the network is modified to compensate.

Where a system or process is still vulnerable, we utilize established best practices and standards to architect a logical design including an electronic security perimeter (ESP) for operations with secure connections to the business and remote access including vendors. Inside the ESP, security and performance are evaluated and mitigated with the use of network segmentation including zones of control and conduits as described in ISA-62443.

After the network detail design is established and the system is installed, part of your acceptance test should be to verify that the security functions have been met in the commissioned system.

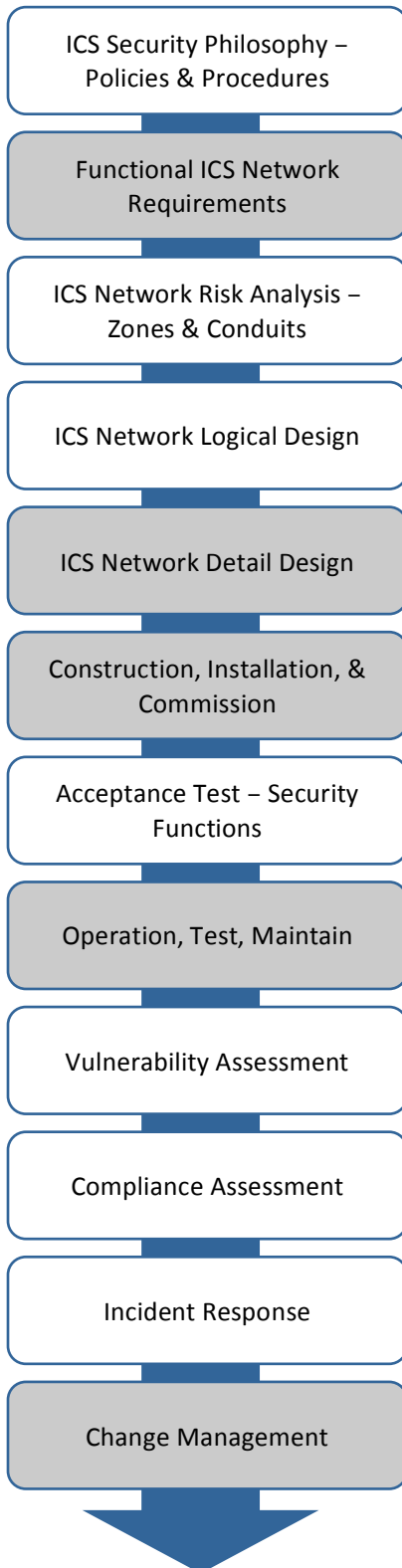
Once operational, vulnerability and compliance assessments are designed to determine the security or performance of an existing system. A vulnerability assessment can be included in a nondestructive penetration test also.

Kenexis offers standard services to assist your organization with establishing a secure and reliable industrial network.



SCADA Security & Reliability

Industrial Network Security, Performance & Reliability Services



ICS Security Philosophy offering includes consulting services to help your organization develop an operational security philosophy including risk matrixes, policies, and procedures. We can also assess these against standards and regulations applicable to your industry and region.

ICS Network Risk Analysis provides consulting services to assess risks by zone once you have a Functional ICS Network Requirement.

ICS Network Logical Design service develops a logical network design that a system integrator can use to develop a detailed design.

Acceptance Test verifies that the detailed design as built, meets the security functions defined in the logical design.

Vulnerability Assessment evaluates the ICS network for security, performance, and/or reliability. A vulnerability assessment may be designed to check performance or conduct a nondestructive penetration test on the system.

Compliance Assessment service verifies the Detailed Design against the security requirements.

Incident Response service will help you develop a plan and provide assistance during an incident.

About Kenexis

Kenexis is an independent engineering consulting firm providing a range of services that are geared toward identifying the risks posed by process plants and manufacturing facilities and then assisting in the implementation of technical safeguards to mitigate those risks. Kenexis services fall into four main categories:



SAFETY
INSTRUMENTED
SYSTEMS



PHA
LOPA
QRA



FIRE &
GAS
MAPPING



SCADA
SECURITY
& RELIABILITY

Our services help our clients to comply with appropriate regulations and standards, and benchmark their performance and processes against industry best practices. These services allow our clients to have best in class safety, security, and reliability.