Secure by design

Like most industries, security has become a top priority for utilities. The exponential increase of cyber threats over the past decade is progressively disconcerting. Sensus is prepared to help utilities embrace the level of cybersecurity required today. All Sensus solutions are designed and built from the ground up to provide end-to-end protection.

CIA Triad

Sensus applies an industry standard process to mitigate risks during the design, development, testing, and operation of solutions. This strategy encompasses the full spectrum of products: from the end points, across the network, to the head-end system and the data center, extending to the back office software. This process is guided by three elements – the need to maintain confidentiality, integrity and availability - also known as the CIA Triad.

Confidentiality of data
Sensus products promote confidentiality through mechanisms like tamper resistance, data encryption, and role-specific access privileges. Sensus also enables utilities to comply with law enforcement and regulatory requirements by offering robust logging and auditing of data.

Integrity of data
Integrity (the precise transmission and storage of data) is ensured by the proper use of encryption, authorization and authentication. Transactions cannot be changed or tampered with as they are protected with digital signatures (ECDSA).

Availability of services
Service continuity is ensured through redundancy and resiliency provided by the Sensus FlexNet® communication network which securely transmits data at over two times the power of competitive systems. Sensus is the only provider of a private, FCC protected, licensed spectrum network. Our private network means you'll never have transmission interference or have to share frequencies. A private point-to-multipoint network, by its nature, provides an unmatched standard of resilience and availability.

SDLC – Secure Development Lifecycle

Sensus follows the SDLC model to ensure security is built into all stages of product development.

Security is top of mind in the requirements gathering phase of product development.	Creating the most secure architecture and design is based on balancing risk and cost. Risk assessments and threat modeling are conducted.	All software and hardware engineers are trained on secure coding practices and regulatory compliance.	Continuous testing and quality assurance is practiced during development to ensure protection and catch threats up front.	Internal and 3rd party testing, auditing and certifications are applied and earned to guarantee additional levels of protection.	Ongoing vulnerability management is provided through bug fixes, patches, antivirus software and additional measures to maintain security after deployment.

Design — **Development, QA** — **Reviews, audits, maintenance**

Third Party Testing, Certifications, Standards Compliance

Sensus employs external experts to assess security in both theory and in practice. This includes, but is not limited to:

- IBM, NCC Group (formerly Matasano Security) - Architecture and code reviews
- Rapid7 – End-to-end penetration testing of the Sensus operations environment
- GE-Wurldtech, SAIC – End-to-end security assessment and penetration testing of customer environments

Sensus monitors the following for standards/ regulatory compliance:

- NIST (IR 7628)
- SGIP
- AMI-SEC
- NERC-CIP
- ZigBee
- ICSJWG

Sensus is the industry's first security-certified company.

The Achilles Practice Certification from GE-Wurldtech was awarded to Sensus for achieving compliance with industry standard security best practices, covering areas such as hardening, anti-malware, patch management, network, and data security. The certification verifies the entire system lifecycle from organizational governance, through solution design and services development, testing, and commissioning, to maintenance and support.

Sensus FlexNet communication network is the industry's first security-certified AMI.

The Achilles Communication Certification from GE-Wurldtech verified the network robustness and end-to-end secure architecture, proving FlexNet's overall resilience against intrusion and other security breaches.

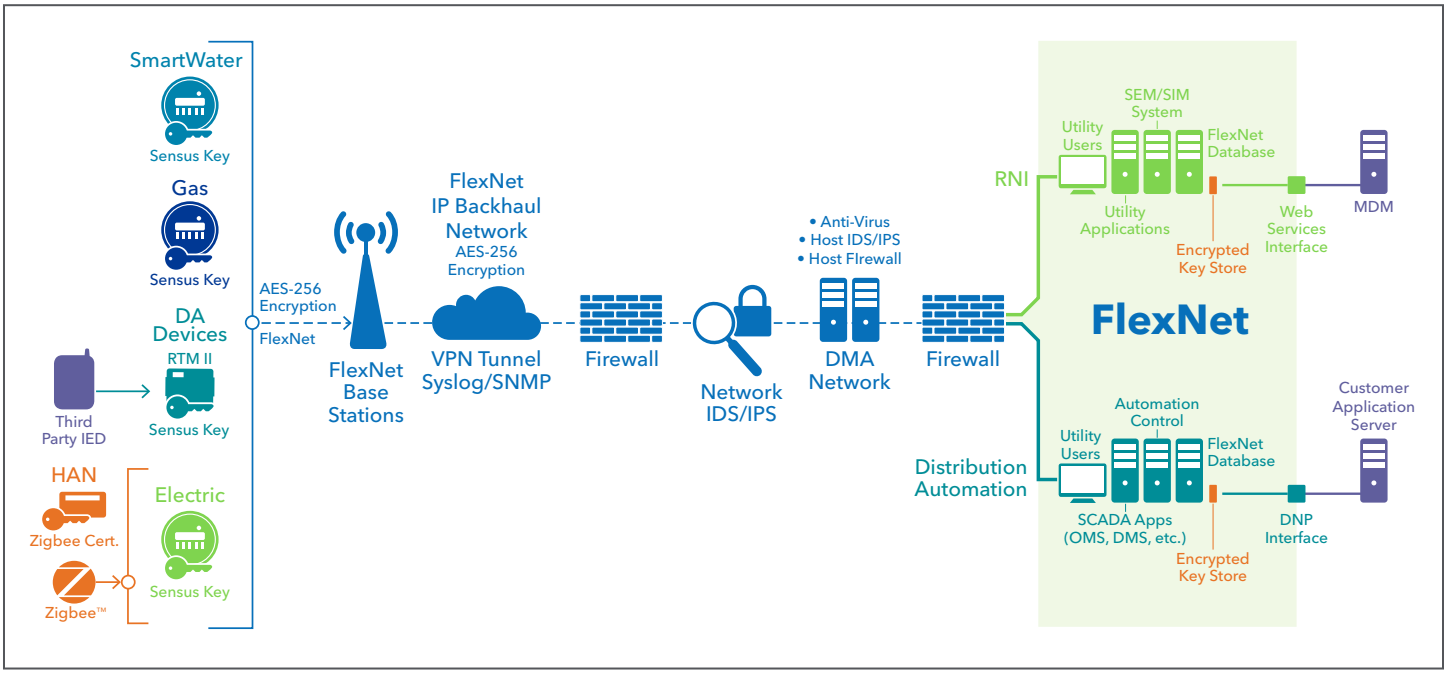
Security Architecture

End to end security layers include:

- Enterprise DC - Firewalls, DMZ, VPNs
- OS/App hardening, patching, A/V
- Remote access, multi-factor authentication
- Role based access control
- Intrusion based detection/prevention, auditing/ logging, SEIM
- Redundant communication channels, disaster recovery
- Encryption, HSM, digital signatures, non-repudiation

Advances in cyber technology

Sensus is committed to staying on the forefront of the latest advancements in cybersecurity. One such advancement becoming more prevalent in every industry, including utilities is Blockchain. Blockchain technology stores cryptographically protected information across a decentralized, distributed network, making it difficult for a hacker to take down an entire network. For example, Blockchain technology can help with secure certificate/key distribution to millions of end points, as well as peering and smart contracts.



Security Architecture

Learn more at sensus.com/cybersecurity

sensus
a xylem brand

SSB-10002-01

 1-800-638-3748 sensus.com