FROM RESEARCH TO INDUSTRY

cea tech

CEA TECH SERVICES FOR CYBERSECURITY

Technology for cybersecurity challenges:

CHALLENGES FOR CYBERSECURITY

Industrial systems and SCADA (supervisory control and data acquisition)
Protecting utility grids, manufacturing plants, and transportation, banking, internet, and other infrastructure; ensuring resilience at system-level

Personal data protection
Data confidentiality (healthcare, communication, etc.); the Internet of Things; cloud computing; aligning security levels with user needs

CEA Tech technology

- Secure software
- Data processing
- Pre-certification evaluations
- Communication and protocols
- Secure implementation on hardware
- Embedded systems and components
- Integrated circuit architectures
- Characterization
- Cryptography

Evaluation
Regulatory compliance; evaluation of electronic systems and components; architectures based on certified components; software

Safer by Design
E-to-E security; protection from threats; identifying weak security links and threats to reliability (hardware and software); contactless technologies

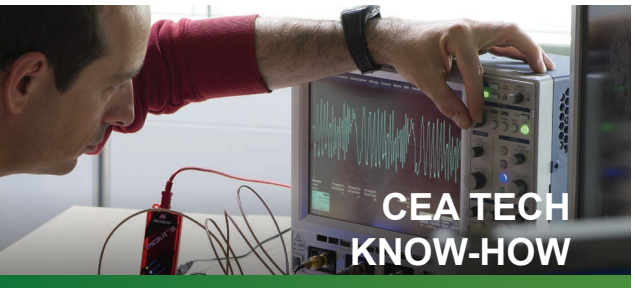
Data security
Counter-espionage; cyber-threat detection; security and behavioral data analysis; protection of public data

Cryptography
Protocols; secure implementation; suitability in terms of performance, cost, and security requirements

CEA Tech can help the following businesses:

- Component and systems manufacturers
- Software developers and security service providers
- Critical infrastructure manufacturers and operators
- Manufacturers in the transportation and aerospace industries
- Government agencies

Here are some of the ways CEA Tech can support your development:



Consulting and business intelligence	Security system and solution audits (aligning security levels with actual needs; implementation strategies; identification of threats and breaches)
Software security	Software security and reliability; identification of weak security links; design tools; risk assessments
System architecture for security	Intrinsically-secure architectures; secure integrated circuits (digital, RF, and near-sensor) including using advanced technologies (FDSOI, 3D); systems-on-chip; virtualization; secure embedded platforms
Security evaluation of systems and components	Multiple accreditations, including for the banking sector (Common Criteria, EMVCo, Visa, MasterCard)
Characterization	Evaluating system and component resistance to physical threats (fire, electromagnetic, laser, glitches, etc.); hardware cryptanalysis
Cryptography	Secure, effective implementation of cryptographic protocols; advanced cryptography (homomorphic encryption, pairing)
Communication and secure protocols	Contactless solutions; wireless communication (RFID, Wi-Fi, ultra wide band, ZigBee); network infrastructure; strong authentication; secure protocols for sensor networks
Big Data and data analysis; behavior analysis; data mining	Event-based early alert detection (e.g. cyber-attacks); business intelligence
Sensor (capacitive, pressure, etc.) systems and integration	Biometric systems (fingerprint, retina, iris); voice recognition
Nanoelectronics (PCRAM, OxRAM, CBRAM, MRAM)	Memory component reliability and robustness; security characterization of emerging technologies (FDSOI)
...	...