Development of SCU Application Systems leading to Social Implementation

Electronic Commerce Security Technology Research Association (ECSEC-TRA), Yokohama National University (YNU), Tokyo University, Kobe University, Tohoku University, Nara Institute of Science and Technology (NAIST), Mitsubishi Electric Corporation, National Institute of Advanced Industrial Science and Technology (AIST)

Application Area

Semiconductor / Packaging | IoT | Manufacturer | Infrastructure | Building / Smart City

The Secure Cryptographic Unit "SCU®" protects IoT devices and serves as the "Root of Trust" in the Society5.0 era.

Technology Features

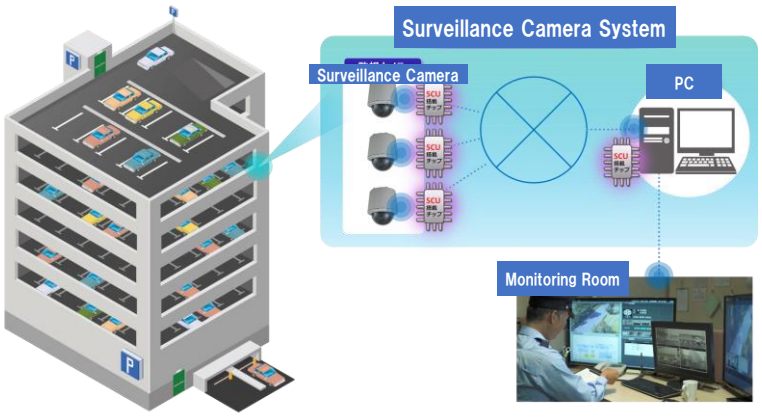
- The "SCU®" is a compact, low-power security chip that protects IoT end nodes (devices) such as sensors and actuators, which are currently nearly defenseless due to limitations in terms of embedded space, power supply, and processing capacity.
  - Equipped with
    - ✓ public key cryptography (world's best record in each compactness, energy savings, and speed as an elliptic curve cryptography (ECC) engine), symmetric key cryptography, random number generator
    - ✓ an access control mechanism to detect and prevent unauthorized access to the cryptographic engine.

Effects

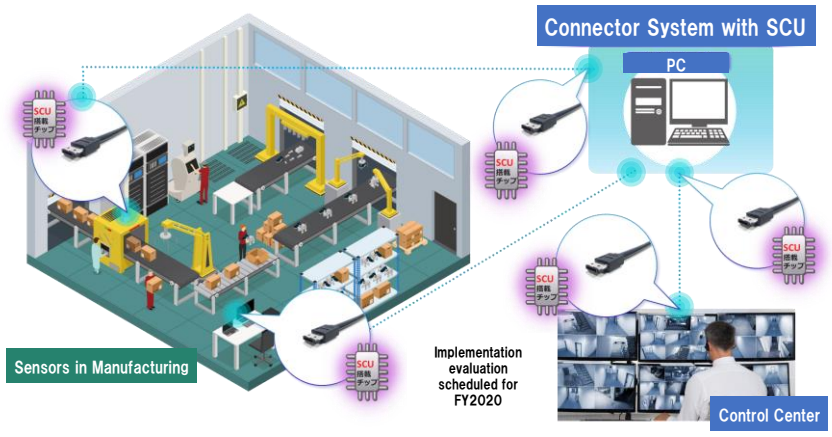
- Enhancing "Endpoint Security" based on "Zero Trust".
- With the "Connector System with SCU", all you have to do is attach the connector (adapter) to the IF section, and there is no need to replace existing equipment.

Use case

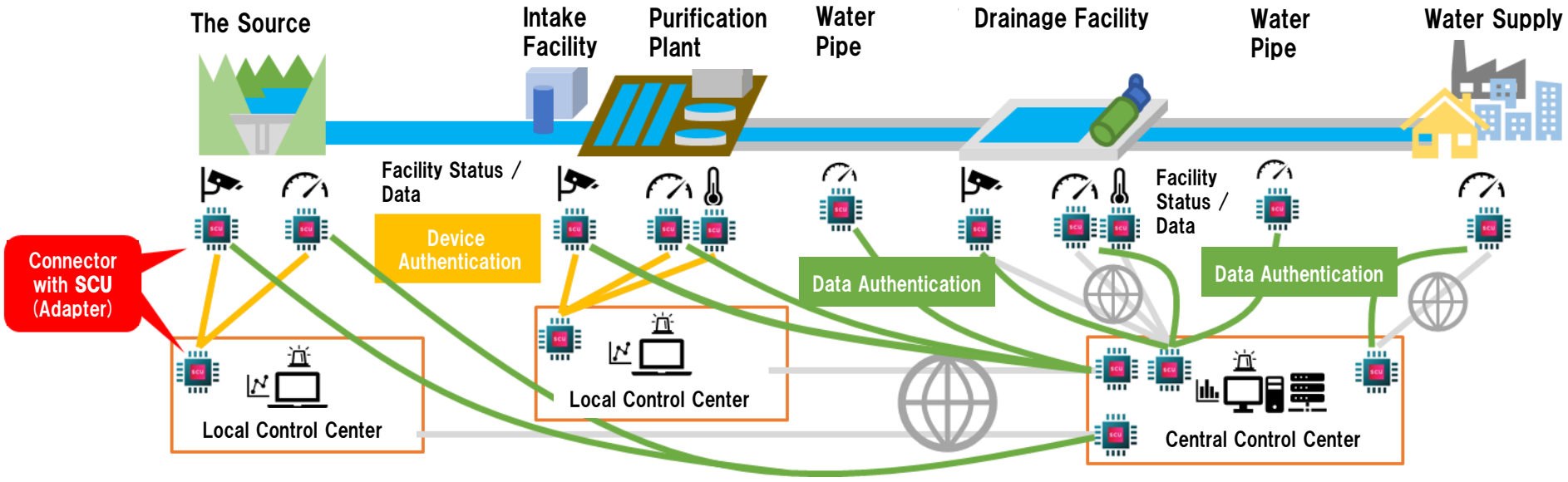
General Embedded Systems



Ultra-Small Embedded Systems



Implementation in Infrastructure (Waterworks)



① Development of SCU Application Systems leading to Social Implementation

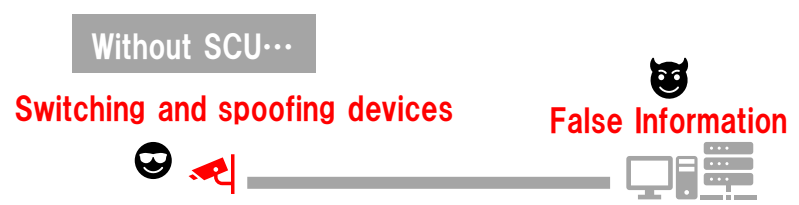
Electronic Commerce Security Technology Research Association (ECSEC-TRA), Yokohama National University (YNU), Tokyo University, Kobe University, Tohoku University, Nara Institute of Science and Technology (NAIST), Mitsubishi Electric Corporation, National Institute of Advanced Industrial Science and Technology (AIST)

Technology Description

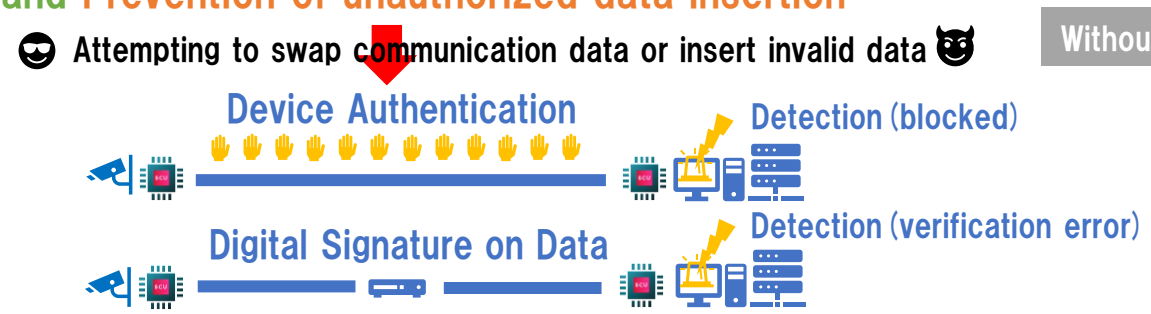
■ Secure Cryptographic Unit (SCU) as the Root of Trust in the IoT Era

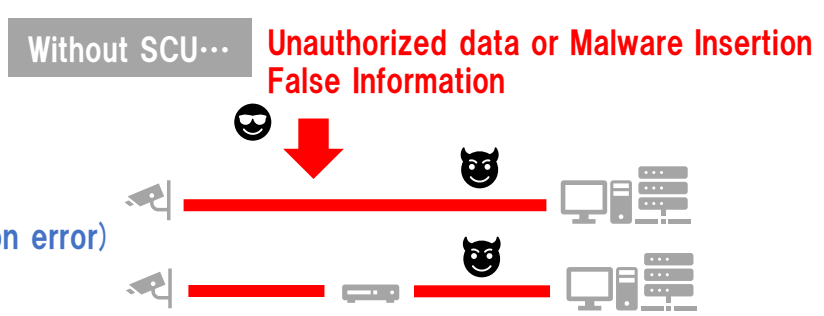
➢ **"SCU®" will enable the Root of Trust for CPS in the Society5.0 era by the followings:**

- **Prevention of switching and spoofing of IoT devices and end nodes**

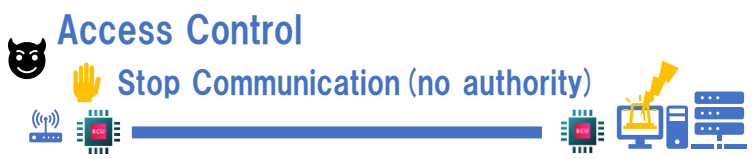


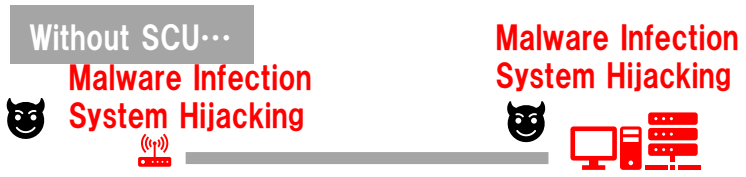
- **Prevention of switching of communication data from IoT devices and end nodes, and Prevention of unauthorized data insertion**





- **Prevention of infection and hijacking of/from IoT devices and end nodes**





- **Encryption of communication data (public key method) from IoT devices and end nodes**

■ Technological superiority

➢ We have achieved the world's best record in each compactness, energy savings, and speed for ECDSA (Elliptic Curve Cryptography) processing. This has given us the technology to manufacture cryptographic units of a critically small size.

➢ We have made it possible to implement public key cryptography in small embedded devices for IoT.

Lowest power ever reported

Smallest ever reported

Fastest ever reported

	Platform	#Gate [kG]	Area [mm²]	#Clk	Vdd [V]	Freq [MHz]	Tsg [ms]	Pow. [mW]	E [μJ]
SCU KM14	65nm	13	0.03	19.4M	0.45		800	0.092	74
					0.75	77	279	0.58	161
					1.2		141	3.2	448
SCU KM15	65nm	1,580	5.64	6.9k-7.5k	0.45	35.7	0.21	15.6	3.28
					0.75	98.7	0.076	123	9.32
					1.4	240	0.0313	1,227	38.7
(1)	Stratix II (90nm)	9,177ALM +96DSP	--	107k	--	157	0.32	--	--
(2)	90nm	540	2.72	22.3k	--	131	0.17	--	--
(3)	65nm	1,370	1.92	34.7k	0.25		11	0.15	1.68
					0.3		2.3	0.69	1.68
					1.1		0.33	42.9	13.9
(4)	65nm	2,500	--	15k	--	236	0.06	--	--
(5)	AMD EPYC7601 (14nm)	NA (64-thread)	NA	157.4		2.2-3.2GHz	0.072	180,000	12,900

Contact

Electronic Commerce Security Technology Research Association
+81-3-5259-8077 Email: researchers@ecsec.org

内閣府 Cabinet Office NEDO SIP Cross-ministerial Strategic Innovation Promotion Program