STSAFE-A & STSAFE-L
Robotics applications

Authentication solutions for robotics

1 Robots & authentication needs

2 STSAFE-A and STSAFE-L authentication chips

3 STSAFE countermeasures

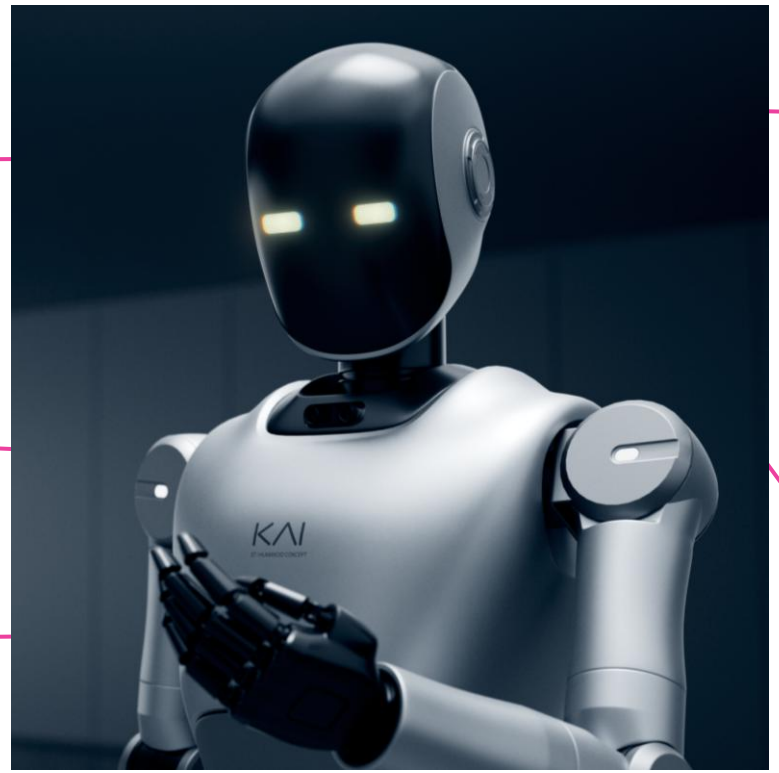
Robots & authentication needs

Designing robots: Why authentication is essential

Part of an upper global system **connected to the Cloud**

Many different **subcomponents** and consumables

No standard available



Heterogeneity of robot's **architecture**

Same constraints as for embedded devices

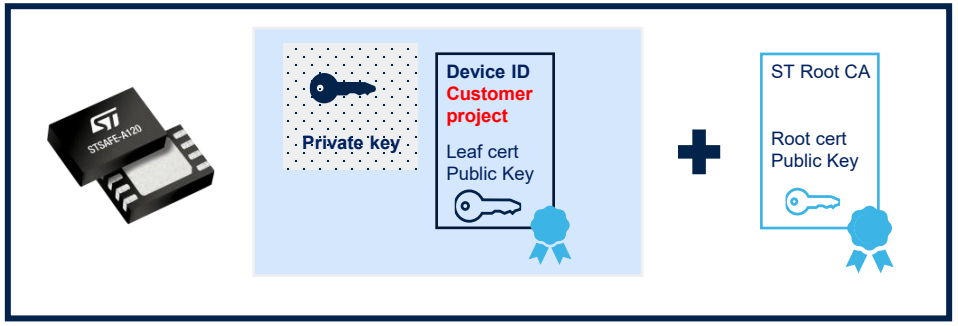
- Real-time local processing for decision-making
- Connectivity
- Data sensing
- Mechanical actuation

About STSAFE-A and STSAFE-L

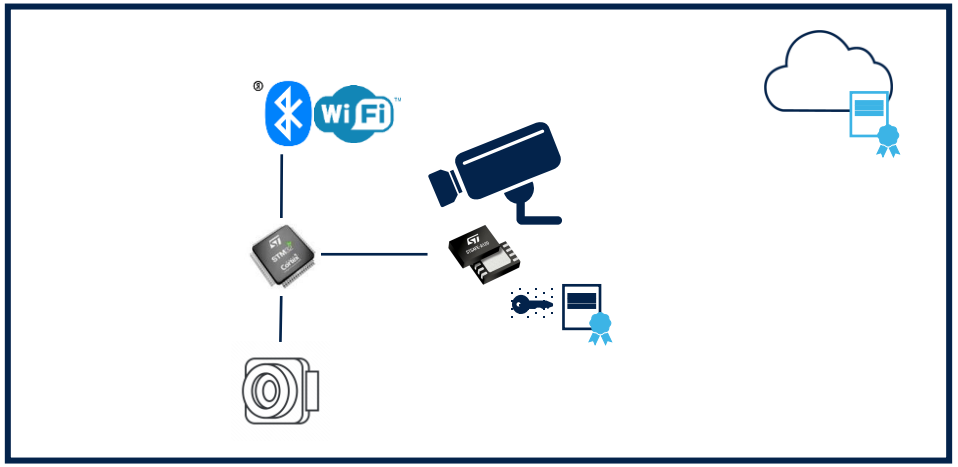
Why choose STSAFE-A120?

Authentication chip optimized for connected equipment

Deliverables



Integration

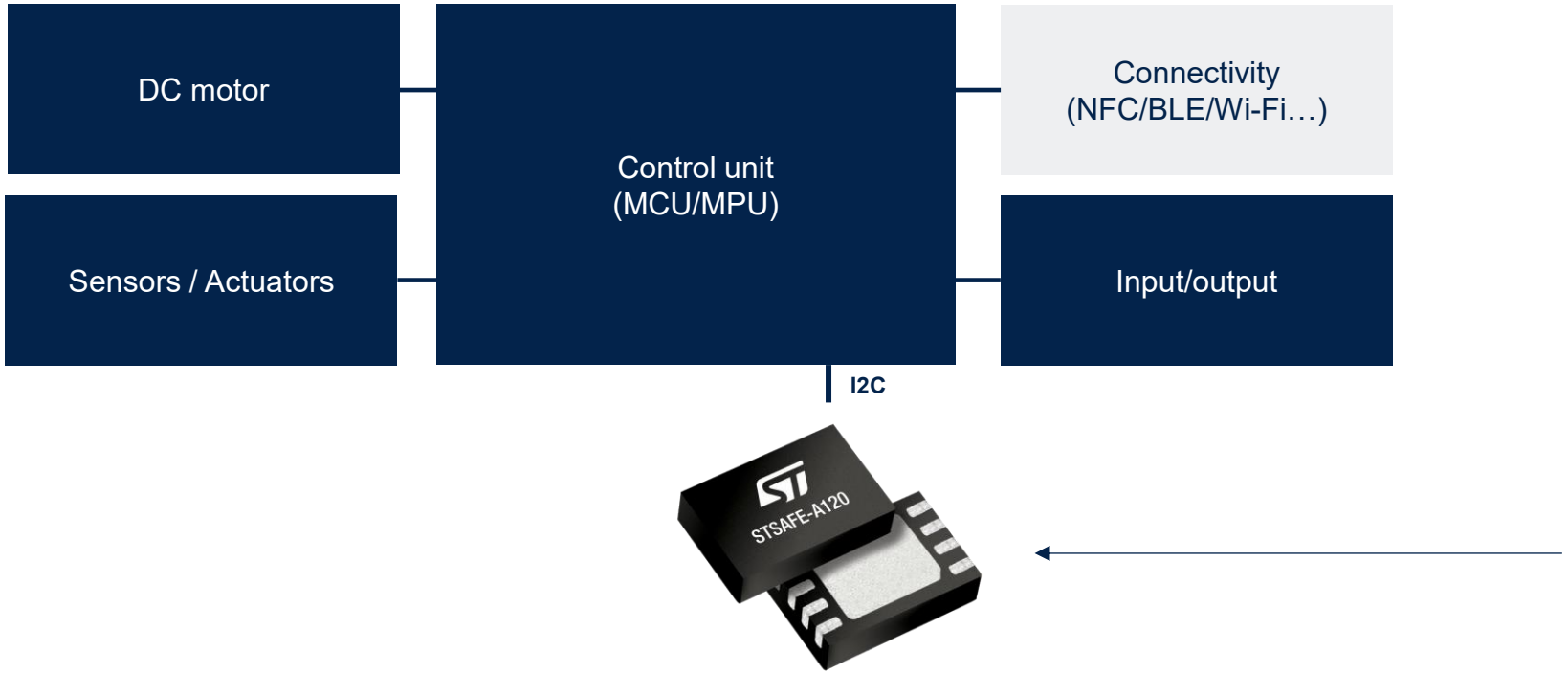


- Equipment authentication with personalized certificate(s)
- Data exchange protection against manipulation
- Data flow protection against manipulation and privacy breach with TLS
- Equipment platform integrity with signature verification
- EAL5+ Common Criteria certified chip

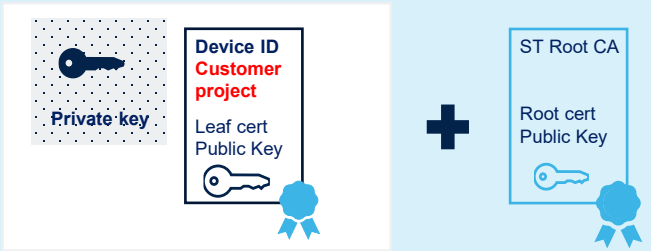
Personalization service available
at ST certified manufacturing site

STSAFE-A120
for head units and smart subcomponents

Typical robot architecture with STSAFE



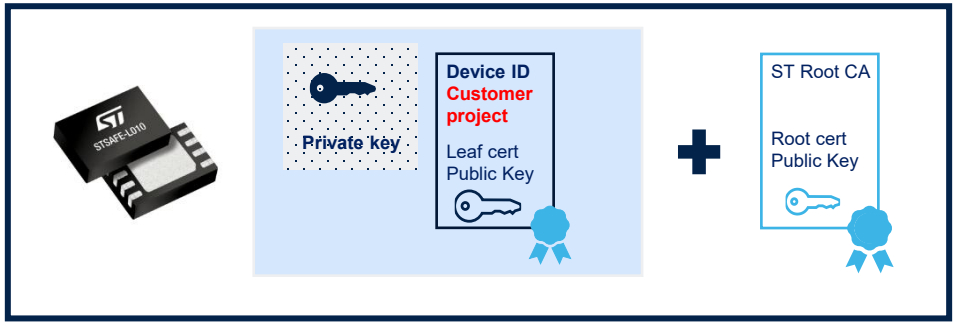
What's inside?



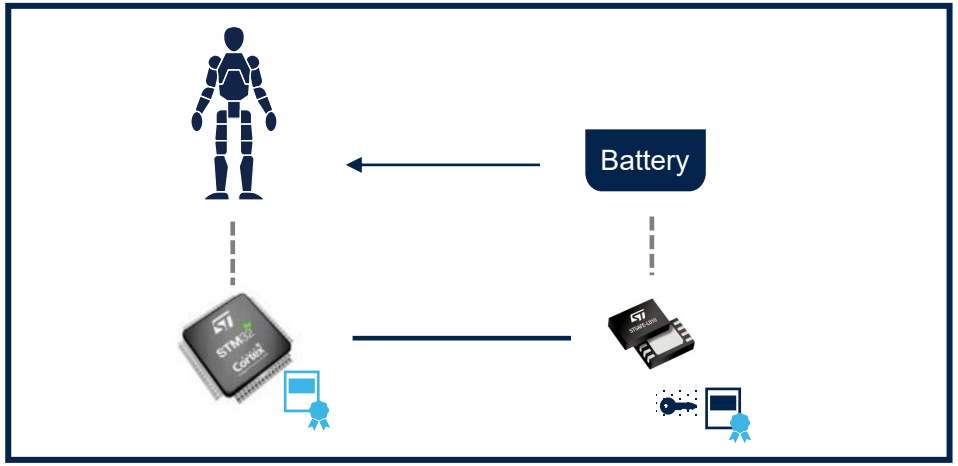
Why choose STSAFE-L010?

Authentication chip optimized for consumables, batteries, & peripherals

Deliverables



Integration



- Anti-cloning with authentication with personalized certificate(s)
- Consumable number of usage control with secure counters, secure data storage

Personalization service available
at ST certified manufacturing site

STSAFE-L010
for genuine consumables & subcomponents

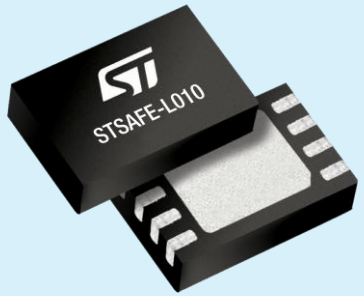
Robot typical architecture with STSAFE

Robot smart-components

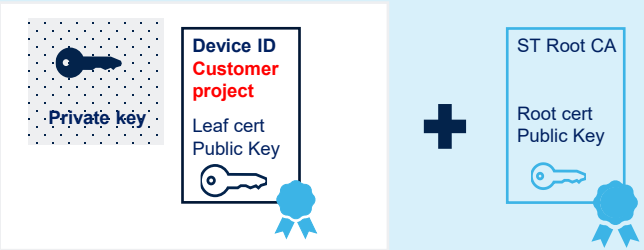
Control unit
(MCU/MPU)

ST1Wire
I2C

Consumable / passive subcomponents integrates



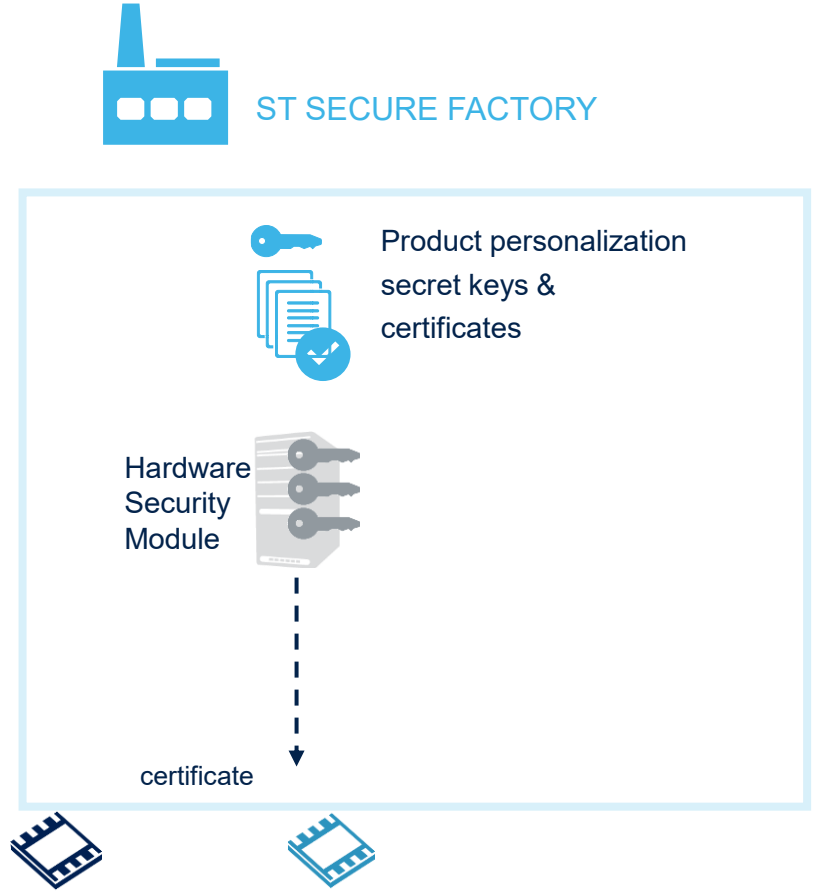
What's inside?



STSAFE provisioning at ST factory

Personalization at ST secure factory
Available from 5K units (MOQ)

Cloud zero-touch provisioning



Benefits for customer industrialization

- No secret or sensitive data to manipulate
- No need for specific investment on customer production line
- No need for specific investment in security skills
- No need for online data loading
- No risk of a production stoppage
- Select external partners or EMS without concern for security

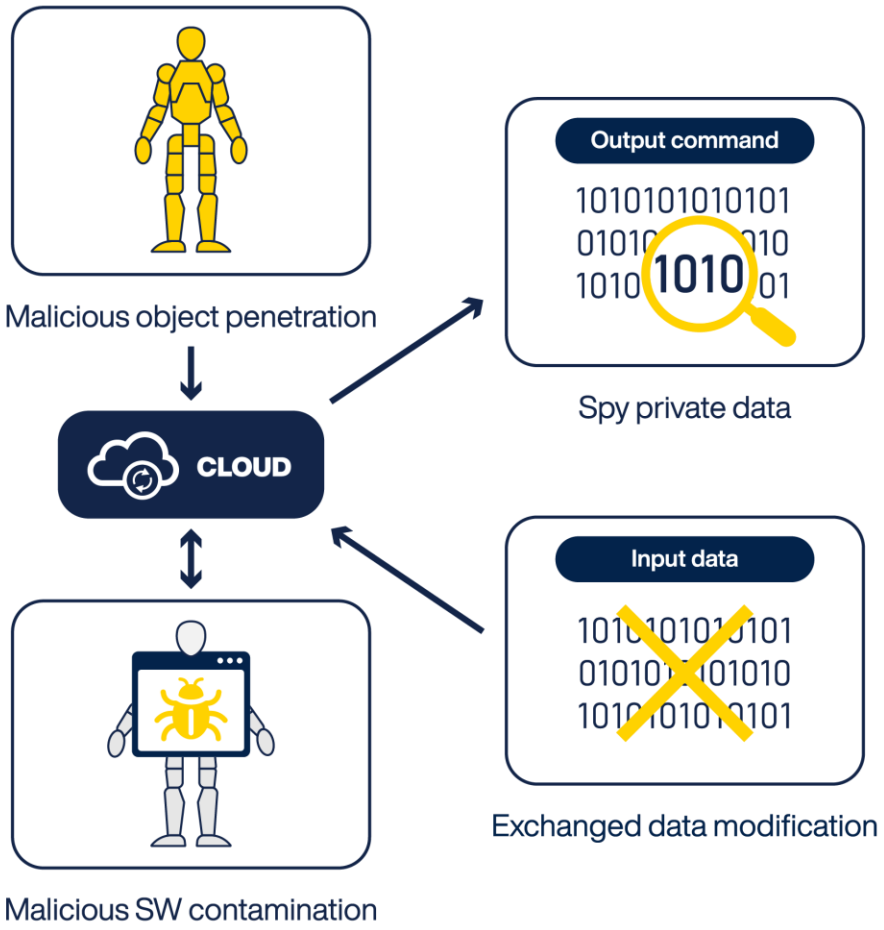
Chip development and packaging → Personalization → Customer delivery

certificate

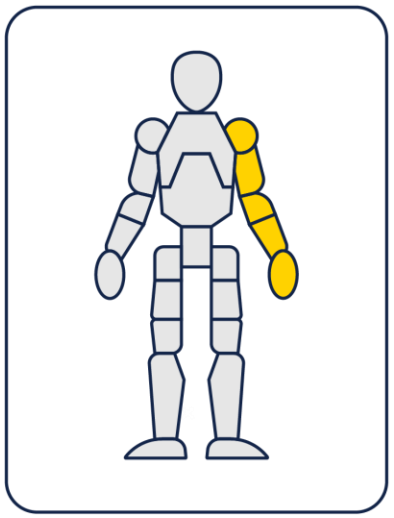
About STSAFE countermeasures

Robots – Threats schematic

Cloud-based attacks



Device-based attacks



Cloning counterfeiting
Abuse of usage limits

STSAFE secure element
Overall system stays secure

Overall system threats	Risks	Countermeasures
Denial of service with robot ID cloning	IDs or X.509 certificates can be cloned to be injected in a malicious equipment. Risk of denial of service or data theft. *=>X.509 certificate and associated key could be stolen in final equipment or at equipment manufacturing*	• Prevent private key theft in final equipment by **storing the key in a tamper-proof STSAFE**. • Prevent private key theft during equipment manufacturing by using an **STSAFE pre-loaded with secret keys** at ST-certified secure manufacturing site.
Denial of service by data manipulation	Data transiting from robot to cloud could be manipulated on the way by malicious equipment in the middle	• Exchanged **data is signed with the STSAFE**'s private key, so the cloud can verify its integrity.
Patient data privacy breach	Data transiting from robot to cloud could be spied on the way by malicious equipment in the middle Patient private data could be collected	• Exchange data can be cyphered by a TLS session initiated with X.509 certificate and the private key of STSAFE.
Denial of service and/or data theft by virus	Robot could become malicious by being contaminated by malicious software at production or after application update. It could conduct to denial of service and/or privacy breach	• Robot application integrity should be verified with credentials loaded in STSAFE at ST secure manufacturing site. Verification should be local and remote at cloud level

STSAFE secure element
Subcomponents stay secure

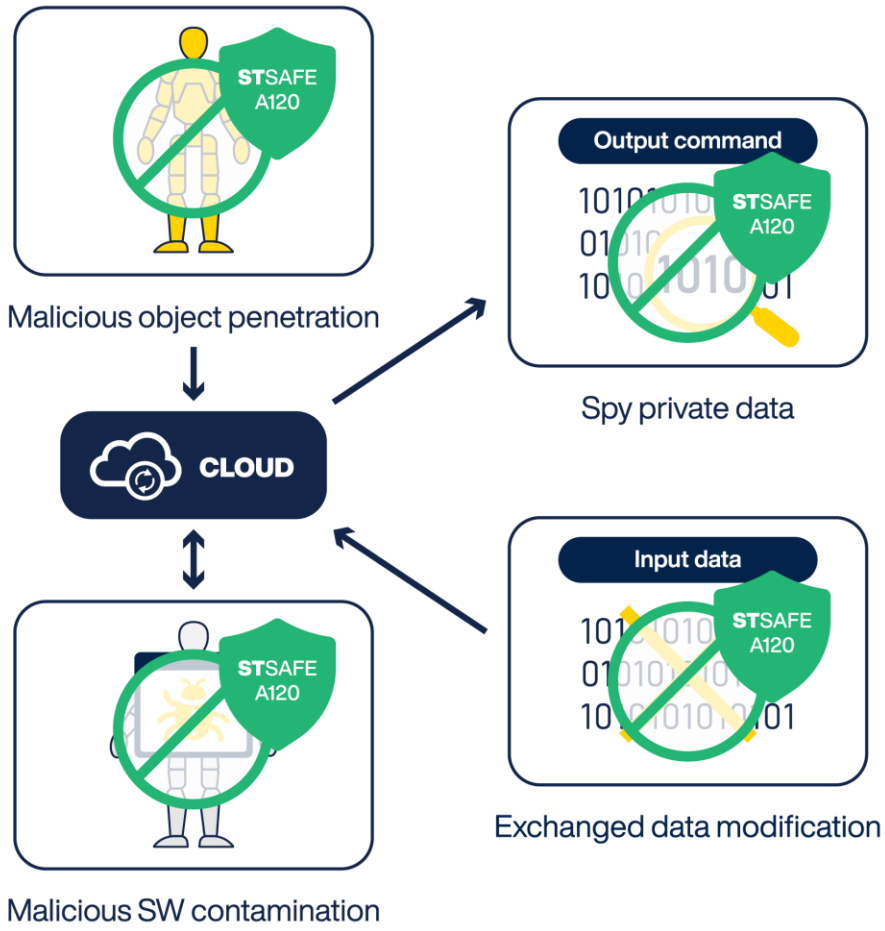
Subcomponents threats	Risks	Countermeasures
Business theft	IDs or X.509 certificate can be cloned to be injected in a cloned equipment. .Loss of business revenue .Risk on system quality and performance *=>X.509 certificate and associated PR key could be stolen in final equipment or at equipment manufacturing*	• Prevent private key theft in final equipment by **storing the key in a tamper-proof STSAFE**. • Prevent private key theft during equipment manufacturing by using an **STSAFE pre-loaded with secret keys** at ST-certified secure manufacturing site.
Denial of service and/or data theft due to virus	Sub-components could become malicious by being contaminated by malicious software at production or after application update It could conduct to denial of service and/or privacy breach	• Subcomponent application **integrity verified** using the credentials loaded in STSAFE at ST secure manufacturing site. Local verification and remote at cloud level

STSAFE secure element
Consumable & passive objects stay secure

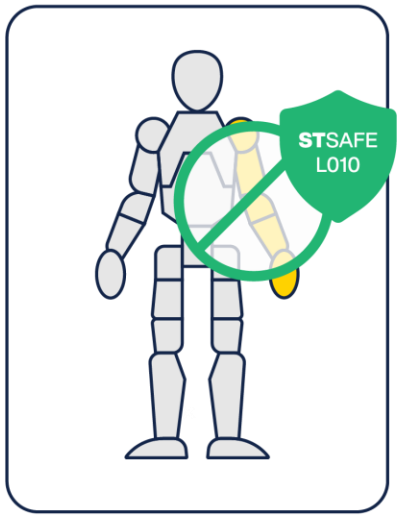
Consumable or passive objects threats	Risks	Countermeasures
Business theft	IDs or X.509 certificates can be cloned to be injected in a cloned equipment. *=>X.509 certificate and associated PR key could be stolen in final equipment or at equipment manufacturing*	• Prevent private key theft in final equipment by **storing the key in a tamper-proof STSAFE**. • Prevent private key theft during equipment manufacturing by using an **STSAFE pre-loaded with secret keys** at ST-certified secure manufacturing site.
Lifespan extension	Some applications (e.g., medical robotics) may require to limit number of usage of certain consumables and/or subcomponents for care quality and liability *=> Easy hack or unrestrained clones could allow to extend consumables or sub-component lifespan.*	• Control consumables and/or subcomponents number of usage with STSAFE secure counters

Robots – Threats schematic & STSAFE contribution

Cloud-based attacks



Device-based attacks

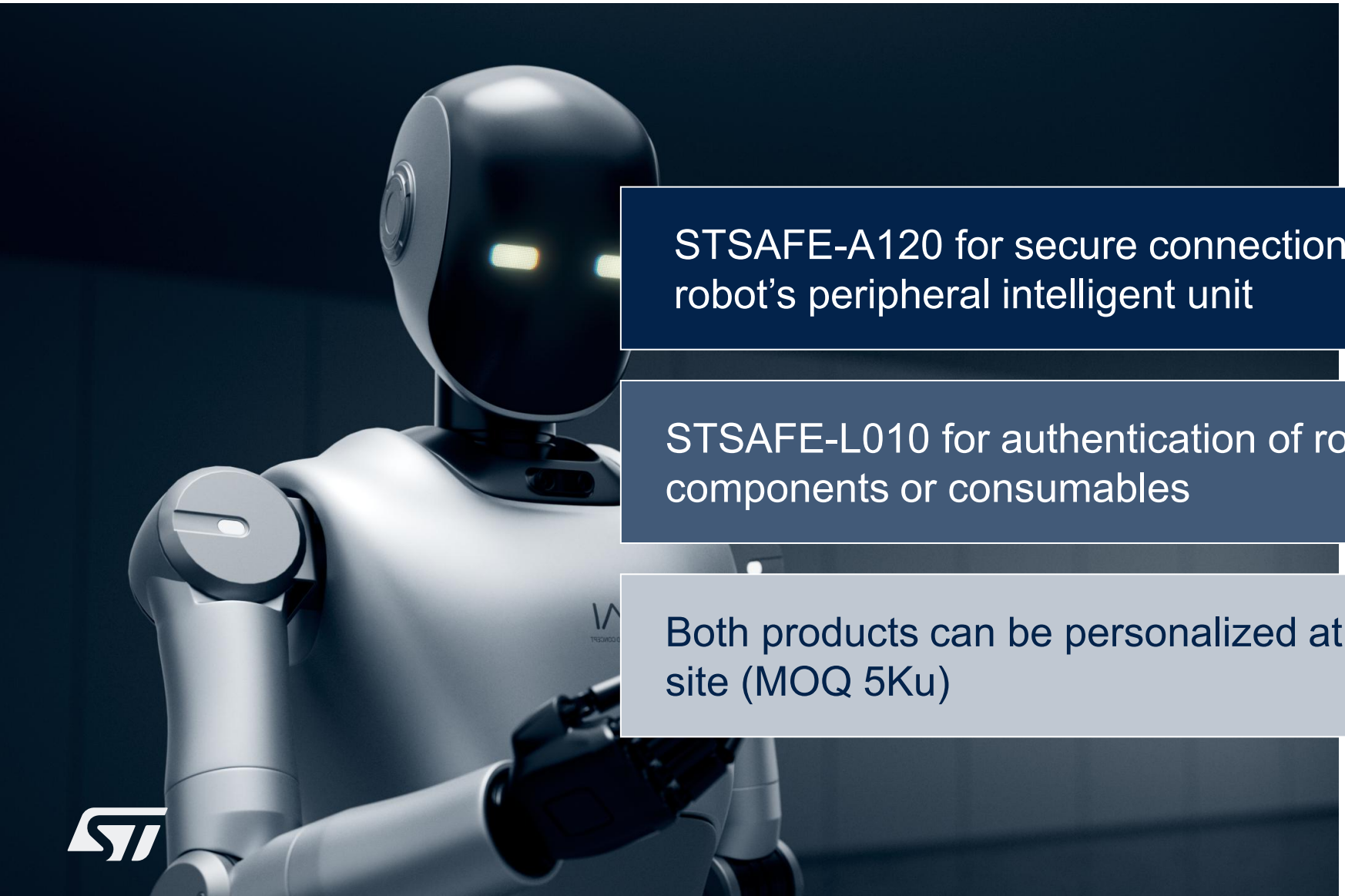


Cloning counterfeiting
Abuse of usage limits

Authentication companion chips

	STSAFE-L010 Consumables & accessory authentication	**STSAFE-A120** Connected devices & anti-cloning
Ecosystem protection against malicious penetration or cloning with authentication	✓	✓
Device lifecycle / number of usage tracking	✓	✓
Protection against exchange data manipulation		✓
Protection against privacy breach (e.g., TLS)		✓
Robot SW application integrity at boot and/or update		✓

STSAFE for robots – takeaways



- STSAFE-A120 for secure connection of robot's head unit and robot's peripheral intelligent unit
- STSAFE-L010 for authentication of robot's dummy sub-components or consumables
- Both products can be personalized at ST secure manufacturing site (MOQ 5Ku)

Our technology starts with You

Find out more at st.com/stsafe