

Typical security measures for an LTE IoT device to support CRA Annex I compliance

8 telemetry-module functions

9 cross-feature requirements

CONTENTS

PAGE

01	Product scope System components / Functional boundary	02
02	Telemetry acquisition and processing Feature #1	03
03	Module identity, provisioning, and inventory Feature #2	05
04	LTE cloud communication Feature #3	07
05	Local buffering and cloud synchronization Feature #4	09
06	Cloud telemetry monitoring and authorized access Feature #5	11
07	Remote diagnostic logs Feature #6	12
08	Remote configuration and command handling Feature #7	13
09	Telemetry-module OTA update Feature #8	14
10	Cross-feature requirements Security rules that apply to the whole system	15

SCOPE

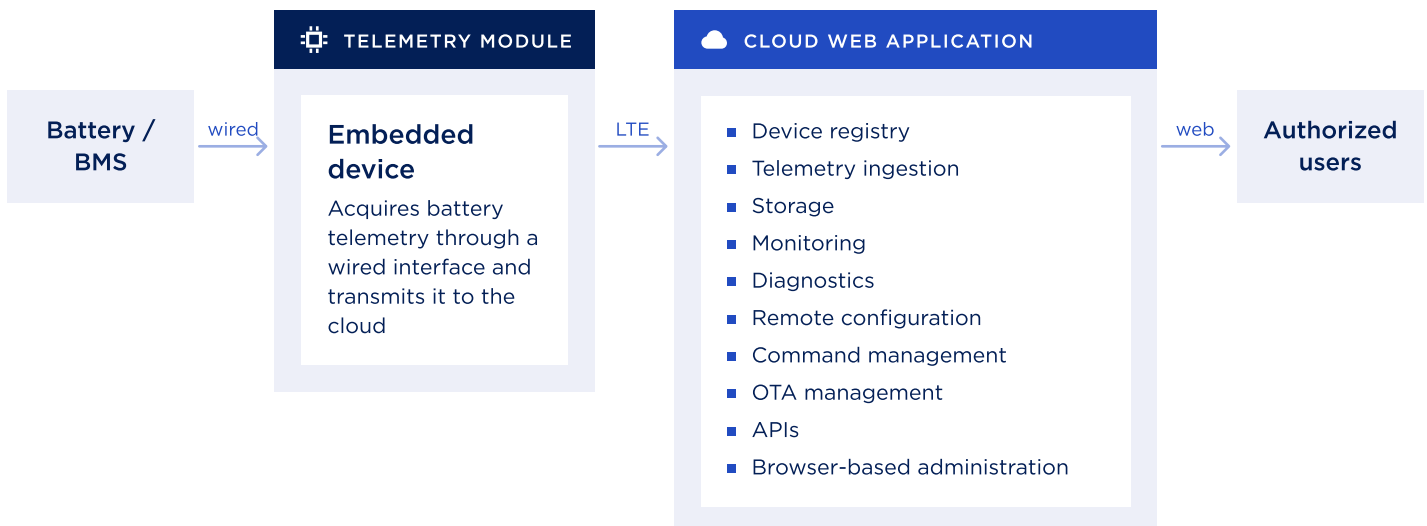
Product scope

The example is based on a Battery Management System telemetry module that reads battery data from a BMS and transmits it to a cloud platform over LTE. The scope is intentionally reduced to 8 telemetry-module functions, excluding battery control, balancing, contactor control, charging control, and direct modification of safety-critical BMS parameters.

! IMPORTANT

The technologies suggested here are examples of possible implementation approaches, not technologies mandated by the EU Cyber Resilience Act. CRA Annex I is outcome-based and requires selecting controls based on the product's cybersecurity risk assessment and specific functionality.

System components



Functional boundary

What the telemetry module does, and what is outside its boundary.

✓ INCLUDED

- Battery telemetry acquisition and validation
- Telemetry buffering during LTE outages
- Transmission of telemetry and module status to the cloud
- Restricted module configuration
- Execution of explicitly defined module commands
- Remote diagnostics and health information
- Authenticated software updates
- Secure provisioning, reset, reassignment, and decommissioning

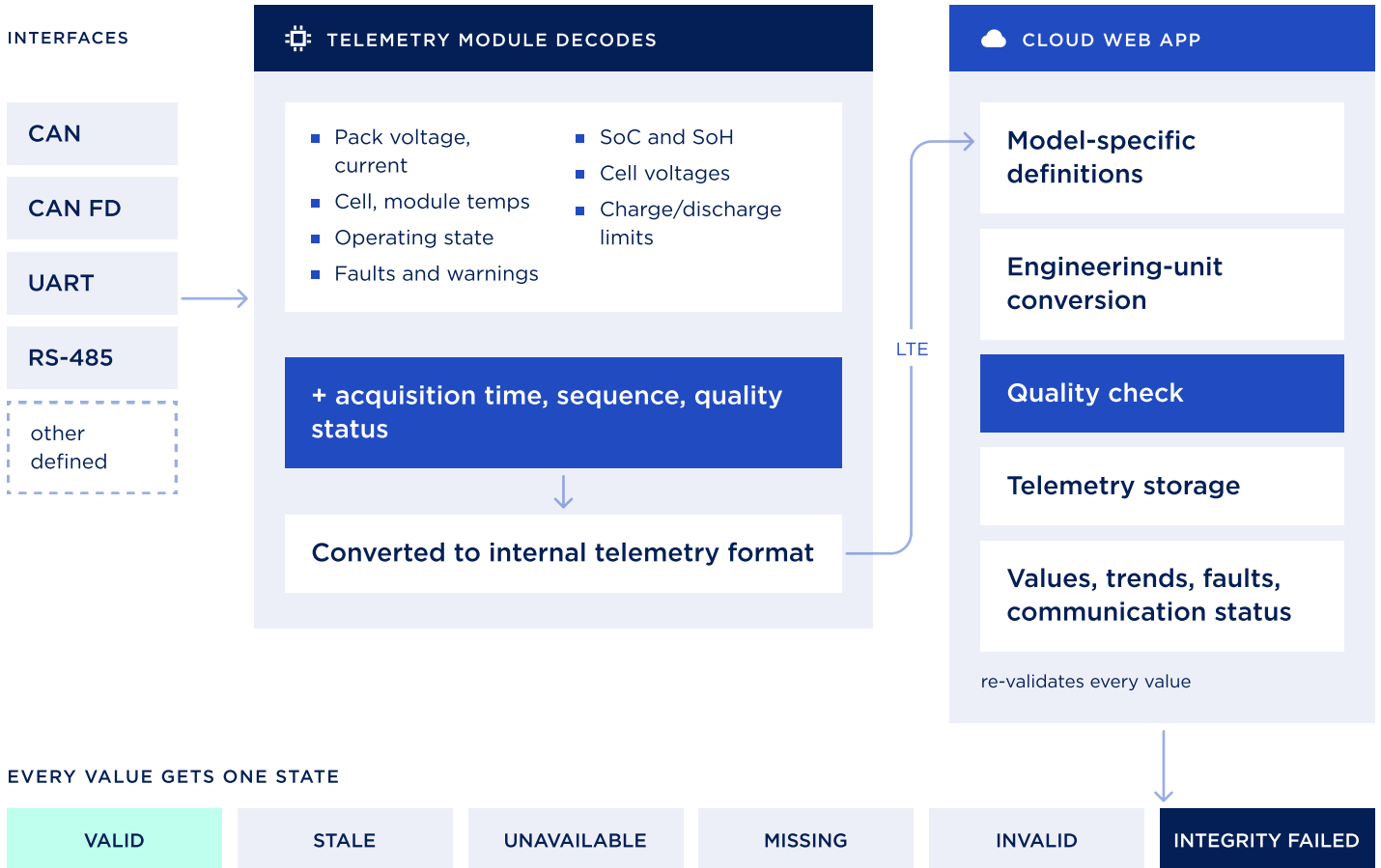
⊘ EXCLUDED

- A general cloud-to-CAN or cloud-to-serial tunnel
- Arbitrary wired-interface message transmission
- Direct remote control of protection, contactors, balancing, charging, or safety thresholds
- Arbitrary operating-system or modem commands
- Unrestricted remote shell access
- Remote read or write access to arbitrary memory
- Unsigned firmware, configuration, or recovery images

FEATURE #1

Telemetry acquisition and processing

Basic functionality



The telemetry module reads battery data over a wired interface such as CAN or RS-485, while decoding the measurements, and tagging each value with acquisition time and data-quality status. The cloud application converts the values into engineering units, stores current and historical data, flags missing or invalid values, and displays trends, faults, and communication status.

✓ CRA FOCUS

Support data integrity, report corrupted input, minimize unnecessary data processing, reduce attack surface, handle malformed data safely, and limit adverse effects on connected systems.

FEATURE #1

Typical security measures

TELEMETRY MODULE

- Treat all incoming frames as untrusted input.
- Allowlist supported CAN identifiers, protocol commands, and message types.
- Validate:
 - frame identifier; payload length; protocol version; signal offset and width; byte order and signedness; allowed ranges; rolling counter; CRC or integrity field; expected message frequency.*
- Do not interpret a communication CRC as sender authentication. A CRC primarily detects accidental corruption.
- Distinguish valid, stale, unavailable, unsupported, out-of-range, and integrity-failed data.
- Use bounded receive queues and parser execution limits.
- Isolate the telemetry parser from LTE, OTA, and diagnostic components through separate tasks, processes, or memory-protection regions.
- Restrict outgoing traffic on the wired interface to explicitly permitted messages. Do not provide a general cloud-to-CAN or cloud-to-serial bridge.
- Protect protocol profiles and decoding definitions against unauthorized modification.
- Test decoders with malformed lengths, counters, identifiers, values, timing, and state transitions.

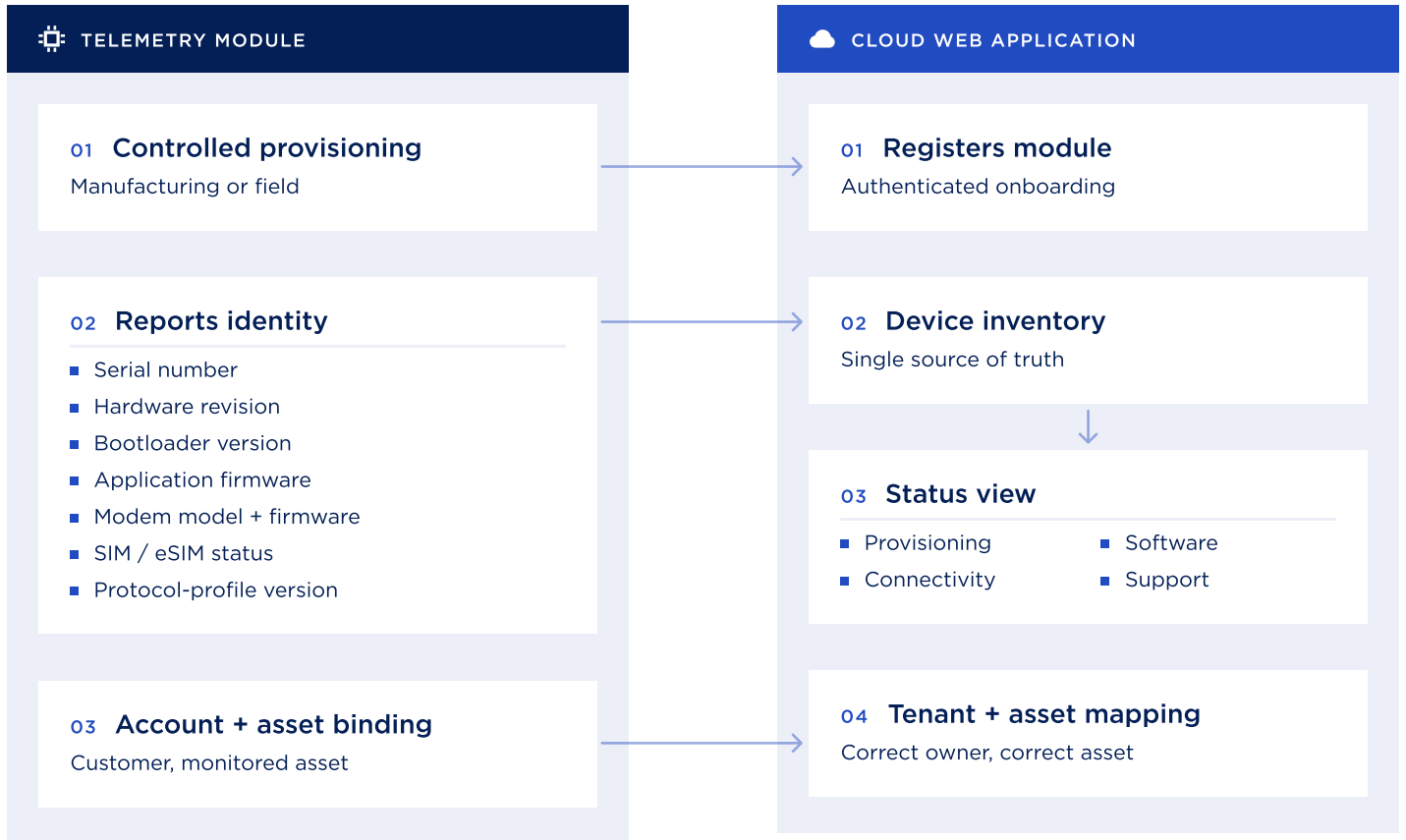
CLOUD WEB APPLICATION

- Validate all telemetry again before storage or processing.
- Use a versioned schema tied to the registered telemetry-module model.
- Verify message type, schema version, field types, units, ranges, sequence number, timestamp, and quality state.
- Reject unknown critical fields and unsupported message versions.
- Do not use stale or invalid telemetry to update the displayed current state.
- Apply authorization to detailed telemetry, fault records, history, and exports.
- Retain only telemetry required for monitoring, diagnostics, support, or applicable record-keeping requirements.

FEATURE #2

Module identity, provisioning, and inventory

Basic functionality



✓ CRA FOCUS

Support secure defaults, unauthorized-access prevention, integrity of identity and inventory information, vulnerability identification, and secure transfer or removal of asset associations and credentials.

FEATURE #2

Typical security measures

TELEMETRY MODULE

- Assign a unique product identity and unique device credential.
- Prefer an asymmetric key pair generated and retained in a secure element, hardware key vault, or protected MCU storage.
- Store serial number and hardware revision in protected manufacturing data.
- Obtain software-version information from signed firmware metadata.
- Keep cellular identity and product identity separate. Do not use the ICCID, IMSI, phone number, or IP address as the only cloud identity.
- Remove development keys, shared credentials, engineering accounts, and test certificates before release.
- Disable or authenticate JTAG, SWD, bootloader, USB, UART, and factory-test interfaces (test points).
- Never expose private keys, SIM secrets, tokens, or onboarding secrets through logs.

CLOUD WEB APPLICATION

- Require an authenticated manufacturing, installer, or administrator identity to provision a module.
- Require cryptographic proof that the module holds the registered private key.
- Use a short-lived provisioning transaction containing expected module, tenant, asset, requester, and expiration.
- Prevent one physical module from being assigned simultaneously to unrelated tenants.
- Reject unknown, revoked, expired, or duplicated credentials.
- Maintain lifecycle states such as manufactured, provisioned, active, suspended, transferred, revoked, and decommissioned.
- Record provisioning, reassignment, credential renewal, revocation, and decommissioning.
- Use the inventory to identify modules running vulnerable, recalled, or unsupported software.
- Maintain a software component inventory for released firmware.

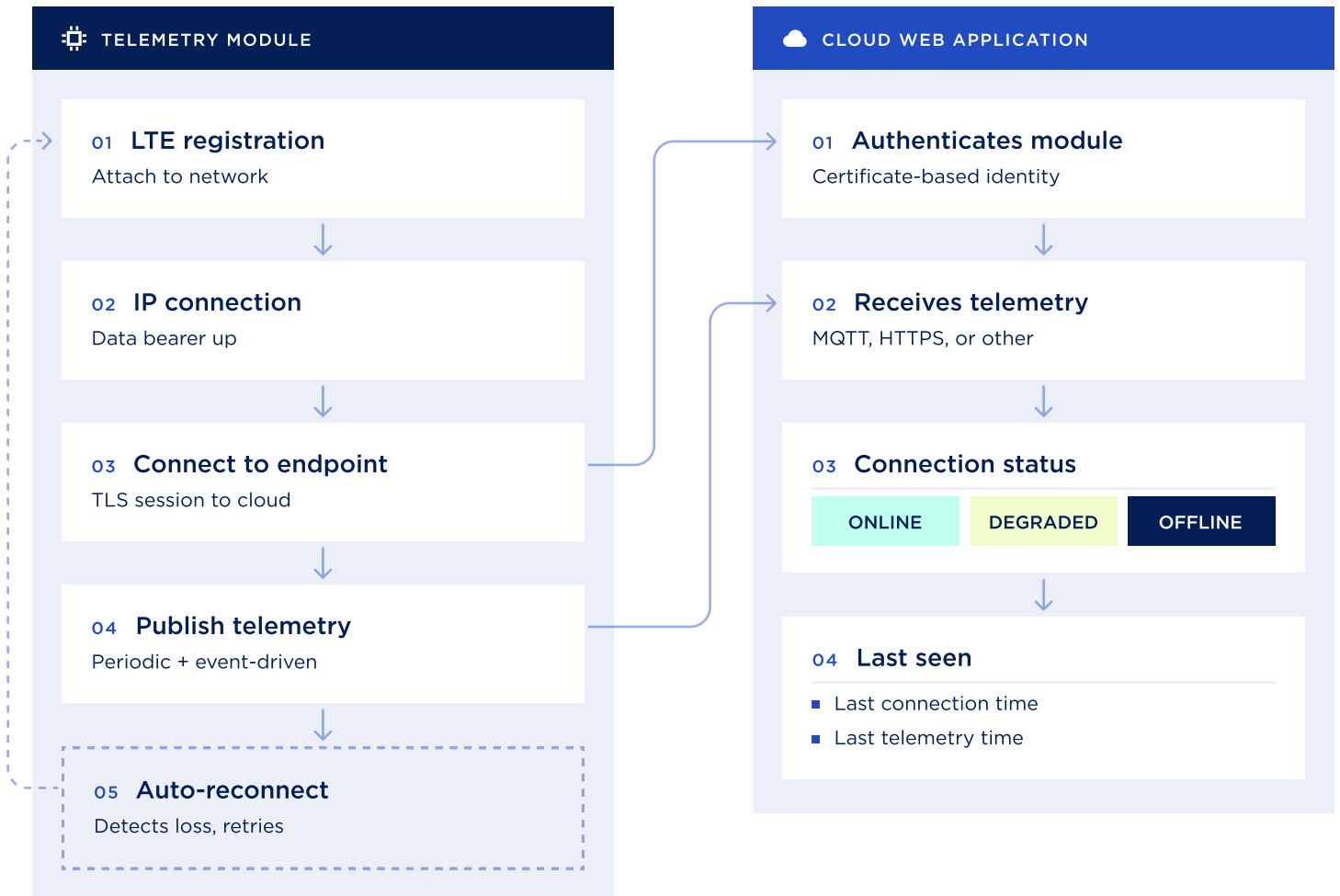
IMPORTANT

Cellular network identity is managed through LTE mechanisms, but it does not replace application-level device authentication to the cloud. 3GPP SA3 is responsible for security and privacy architectures, protocols, and cryptographic aspects for LTE and other 3GPP systems.

FEATURE #3

LTE cloud communication

Basic functionality



CRA FOCUS

Support confidentiality and integrity of transmitted data, unauthorized-access protection, secure defaults, reduced external attack surface, availability protection, and reporting of possible unauthorized access.

FEATURE #3

Typical security measures

TELEMETRY MODULE

- Use LTE subscriber authentication through SIM, eSIM, or eUICC.
- Disable unused cellular services such as voice, SMS control, modem administration, and obsolete radio fallback when not required.
- Restrict modem control to a dedicated component. Do not expose unrestricted remote AT-command access.
- Use TLS 1.3, or a controlled TLS 1.2 configuration when required by the selected modem or service.
- Validate the cloud certificate chain, hostname, validity, key usage, and configured trust anchor.
- Never disable certificate validation following a connectivity, DNS, or clock failure.
- Prefer mutual TLS using a unique module certificate.
- Store the private key in protected hardware or secure storage.
- Restrict connections to authorized hostnames, ports, and protocols.
- Use exponential reconnection backoff with random jitter.
- Limit connection attempts, payload size, publication rate, and queued messages.
- Monitor unexpected SIM changes, roaming state, operator changes, registration failures, modem resets, and abnormal data consumption.

MQTT IMPLEMENTATION

MQTT is a lightweight publish-and-subscribe protocol for constrained and IoT environments. It supports at-most-once, at-least-once, and exactly-once delivery levels.

- Use MQTT only over TLS.
- Assign a unique MQTT client identity to each module.
- Bind the MQTT client identity to the authenticated module credential.
- Apply per-device topic authorization.
- Do not allow unrestricted wildcard publishing or subscriptions.
- Use QoS 0 for replaceable measurements and QoS 1 for important events where duplicate processing is supported.
- Include an event identifier or sequence number for deduplication.
- Limit maximum packet size, inflight messages, topic length, and session lifetime.
- Avoid retained messages for sensitive telemetry unless explicitly required.

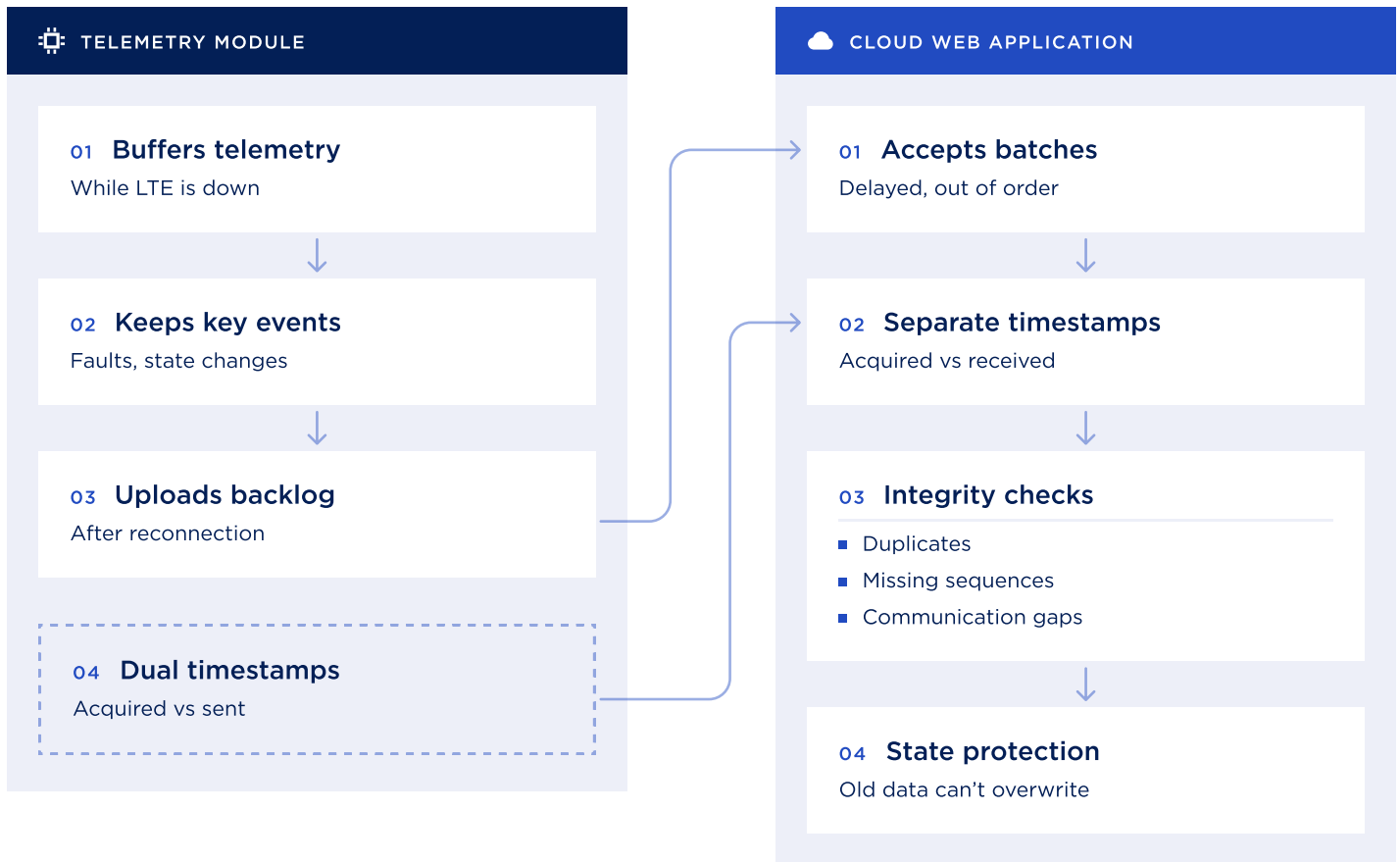
CLOUD WEB APPLICATION

- Authenticate each connection independently.
- Do not treat IP address, APN address, IMSI, or MQTT client identifier alone as authentication.
- Enforce per-device publishing permissions.
- Apply connection, rate, bandwidth, message-size, and storage quotas.
- Separate public ingestion endpoints from databases, administrative services, and OTA signing systems.
- Record authentication failures, authorization denials, certificate failures, and excessive traffic.
- Prevent one compromised module from consuming resources required by other modules.

FEATURE #4

Local buffering and cloud synchronization

Basic functionality



During LTE outages, the telemetry module buffers data, retaining important fault and state-change events, and uploading the backlog after reconnection — with acquisition time stored separately from transmission time. The cloud application accepts delayed batches, detects duplicates and gaps, and stops old data from overwriting the current state.

✓ CRA FOCUS

Support confidentiality and integrity of stored data, data minimization, availability after a connectivity incident, secure recovery, and protection against storage, network, and cloud resource exhaustion.

FEATURE #4

Typical security measures

TELEMETRY MODULE

- Use a bounded ring buffer or quota-controlled persistent queue.
- Prioritize fault events and state changes over ordinary periodic measurements.
- Reserve storage for high-priority events.
- Define deterministic behavior when storage is full.
- Store an event identifier, sequence number, acquisition time, quality state, schema version, and integrity value with each record.
- Use transactional or journaled storage that tolerates interrupted power.
- Apply CRC for accidental corruption detection.
- Use a keyed MAC or authenticated encryption where storage manipulation is part of the threat model.
- Protect sensitive local telemetry using a device-specific encryption key.
- Restrict access to the buffered data.
- Rate-limit backlog transmission after reconnection.
- Securely erase buffered telemetry during authorized reassignment, factory reset, or decommissioning.

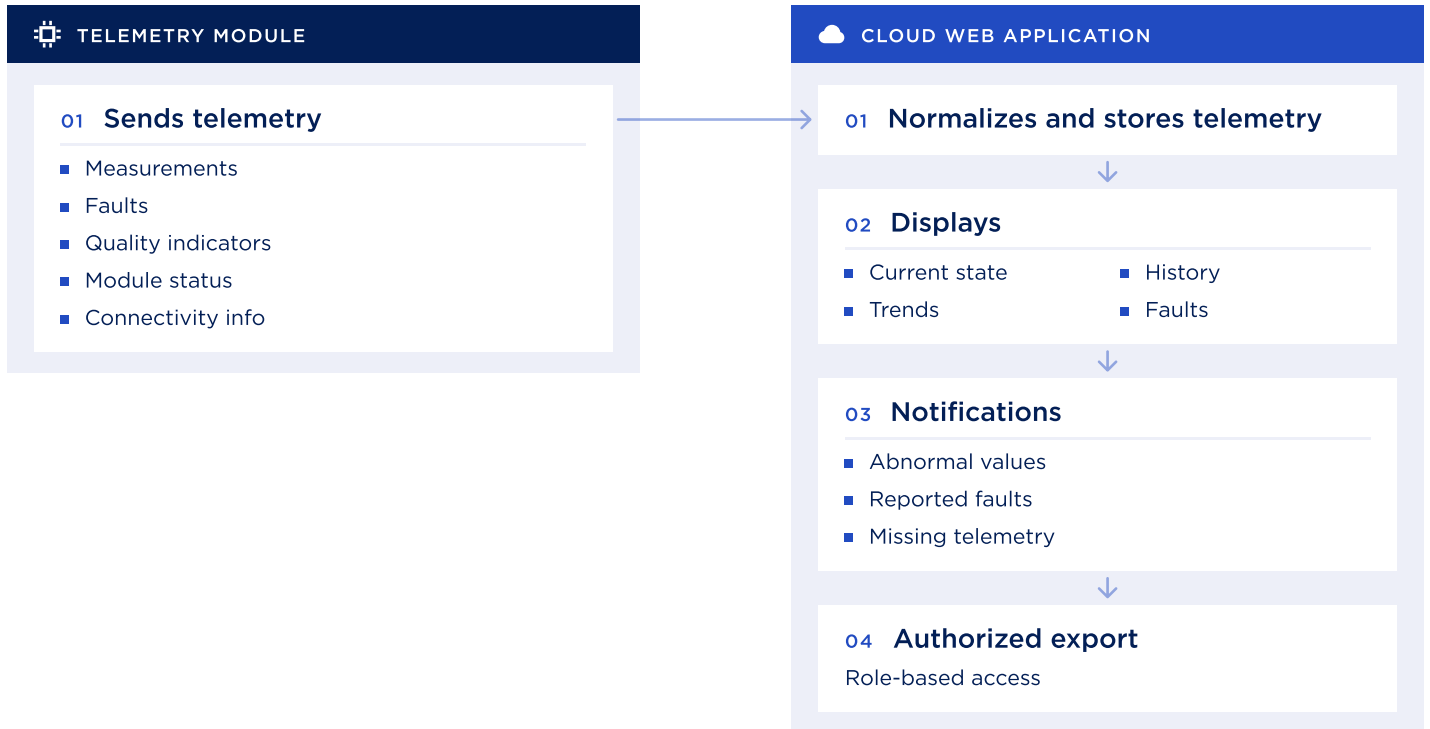
CLOUD WEB APPLICATION

- Deduplicate using module identity, event identifier, and sequence number.
- Do not rely only on module-provided timestamps.
- Preserve acquisition time, transmission time, and cloud-receipt time separately.
- Reject unexplained sequence rollback.
- Prevent delayed events from overwriting fresher current state.
- Limit batch size, decompressed size, date range, and processing time.
- Detect abnormal backlog volume, repeated duplicates, malformed batches, and unacceptable timestamps.
- Authenticate backlog uploads in the same way as live telemetry.

FEATURE #5

Cloud telemetry monitoring and authorized access

Basic functionality



✓ CRA FOCUS

Support access control, confidentiality and integrity of processed information, data minimization, monitoring of relevant activity, reporting of unauthorized access or corruption, and protection of service availability.

Typical security measures

⚙️ TELEMETRY MODULE

- Minimize collected and transmitted information to the declared monitoring purpose.
- Avoid transmitting credentials, modem secrets, unnecessary personal data, or raw memory content.
- more...

☁️ CLOUD WEB APPLICATION

- Use strict, versioned schemas for JSON, CBOR, Protocol Buffers, or the selected format.
- Validate identity, message type, field length, range, units, sequence, timestamp, and quality state.
- more...

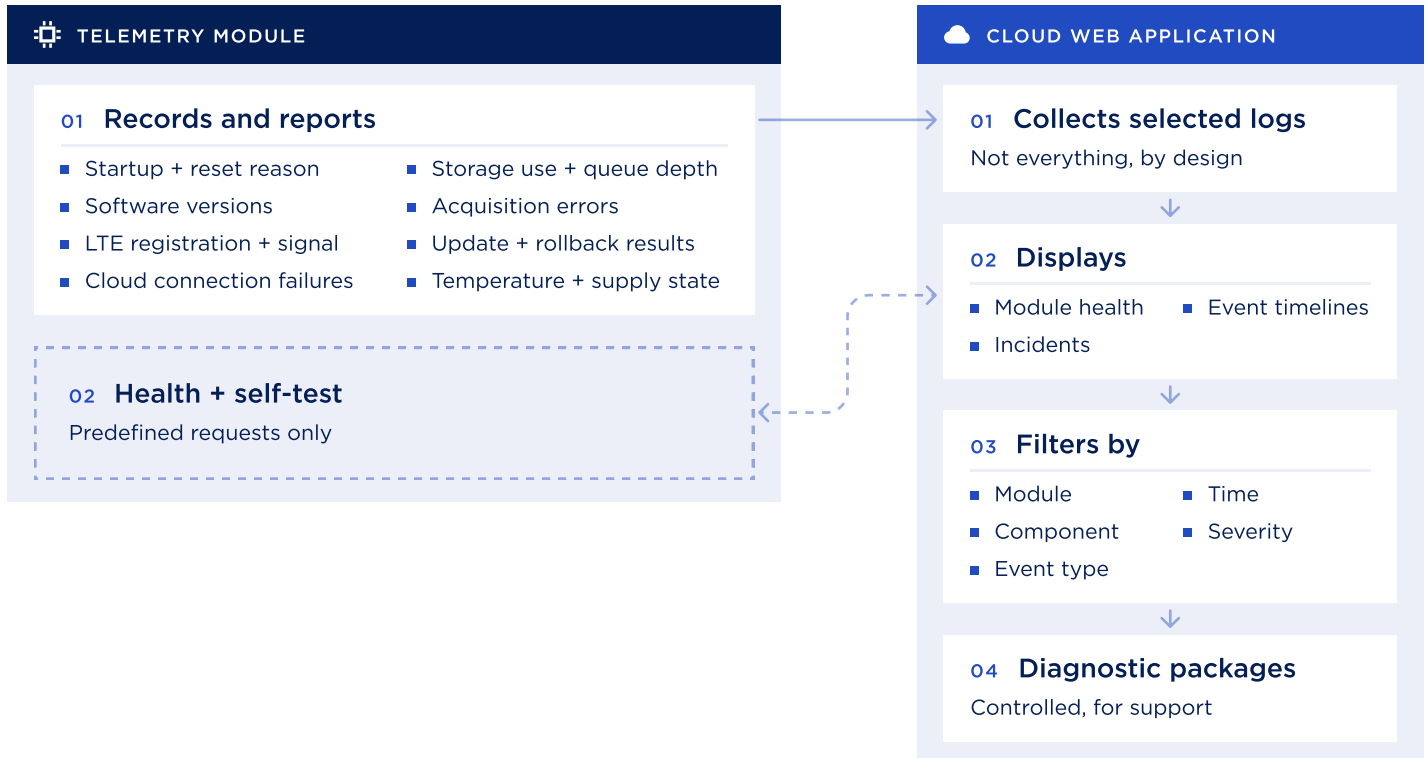
More security measures for access control, exports, and monitoring

GET IN TOUCH

FEATURE #6

Remote diagnostic logs

Basic functionality



✓ CRA FOCUS

Support the recording and monitoring of relevant internal activity, detection and reporting of possible unauthorized access or corruption, data minimization, log confidentiality and integrity, and preservation of essential functionality if diagnostics fail.

Typical security measures

TELEMETRY MODULE

- Use a fixed event catalog with numeric event identifiers.
- Include a timestamp or uptime, severity, component, event code, and bounded parameters.
- Never log private keys, SIM credentials, passwords, full tokens, or unnecessary customer information.
- more...

CLOUD WEB APPLICATION

- Limit diagnostic access to authorized operational and support roles.
- Use time-limited, attributable support access.
- Record who accessed logs, what was retrieved, and which diagnostic operation was requested.
- more...

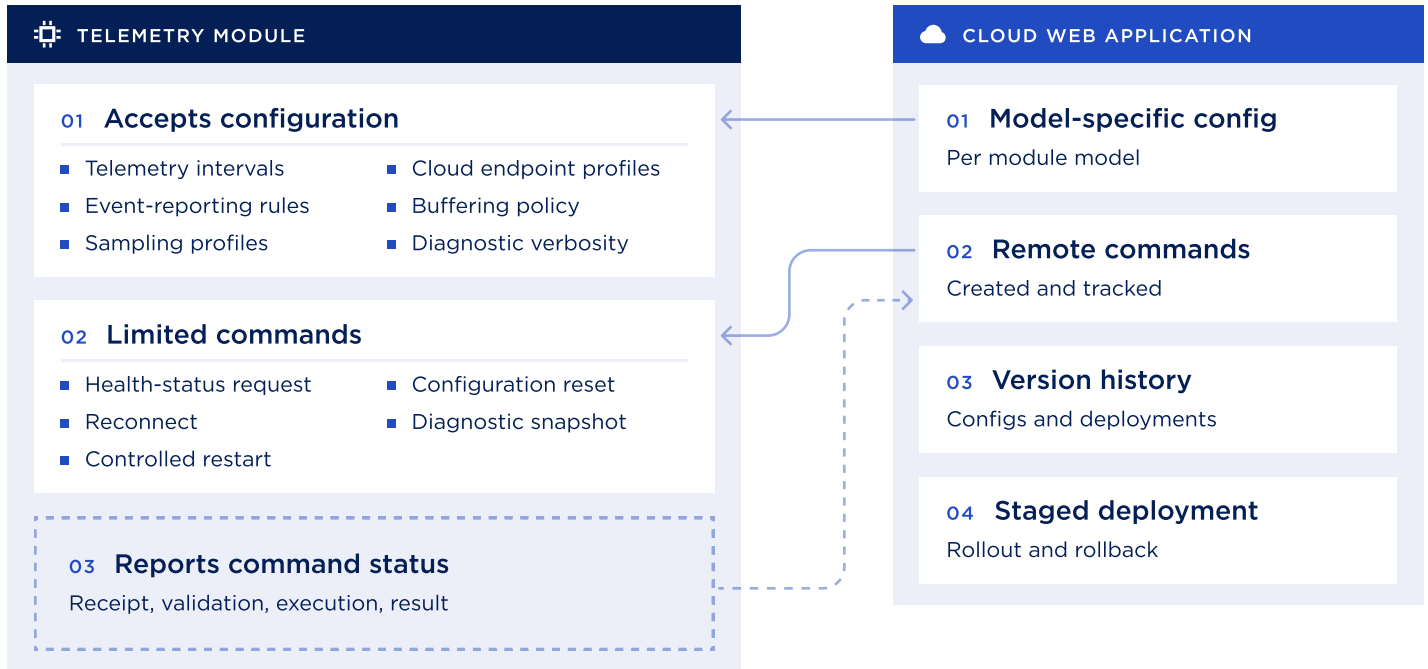
Discover the security measures for diagnostic data protection and support access

[CONTACT FOR MORE INFO](#)

FEATURE #7

Remote configuration and command handling

Basic functionality



CRA FOCUS

Support protection against unauthorized access, integrity of commands and configuration, secure defaults, reduced attack surface, reporting of corruption, and continued availability when malformed or abusive commands are received.

Typical security measures

TELEMETRY MODULE	CLOUD WEB APPLICATION
- Accept configuration and commands only through the authenticated cloud channel. - Validate: <i>target module; model and hardware revision; command or schema version; issue and expiry time; unique command identifier; allowed fields; value ranges; authorization; integrity protection.</i> - Use a restricted command allowlist. - more...	- Require object-level authorization for every command and configuration operation. - Restrict endpoint, trust-anchor, update-policy, reset, and diagnostic settings to privileged roles. - Require recent re-authentication for high-impact commands. - more...

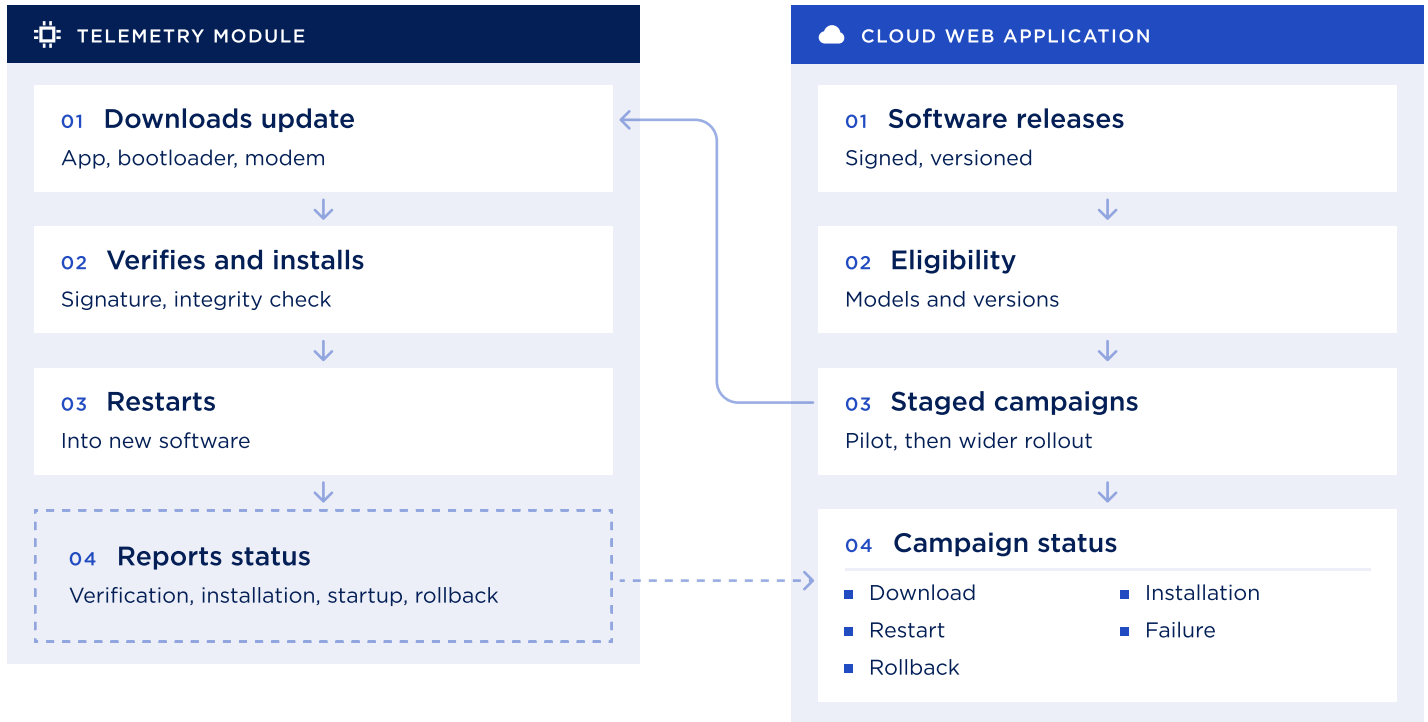
Explore more security measures for remote configuration and commands

GET IN TOUCH

FEATURE #8

Telemetry-module OTA update

Basic functionality



✓ CRA FOCUS

Support vulnerability remediation, program integrity, secure update delivery, secure defaults, availability after failed updates, incident-impact reduction, and lifecycle vulnerability handling.

! IMPORTANT

The CRA requires products to support vulnerability remediation through security updates. Where applicable, automatic security updates must be enabled by default, installed within an appropriate timeframe, communicated to users, and accompanied by postponement and opt-out mechanisms.

Discover security measures for secure OTA updates

TALK WITH OUR EXPERT

RULES

Cross-feature requirements

Some security rules apply to the whole system, not just one function. The key ones are:

01

Unique identity

Every module must use unique device and cloud credentials.

02

Secure defaults

Unused modem functions, interfaces, commands, debug ports, and cloud permissions must be disabled.

03

Least privilege

Grant module components, cloud services, users, support staff, and integrations only the permissions they need.

04

Defense in depth

Apply independent controls for LTE, TLS, authentication, authorization, secure boot, updates, validation, and monitoring.

05

Fail safely

Loss of LTE, DNS, cloud connectivity, storage, trusted time, or credentials must not create an insecure fallback.

06

Data minimization

Collect, transmit, expose, and retain only data needed for telemetry, diagnostics, maintenance, and security.

07

Vulnerability handling

Keep component inventories, assess vulnerability reports, identify affected versions, develop and test fixes, distribute security updates, and retain remediation evidence.

08

Verification

Test input validation, TLS authentication, credential revocation, tenant isolation, delayed data, command authorization, secure reset, update signature rejection, rollback, and resource exhaustion.

09

Traceability

Trace each security requirement to a cybersecurity risk, CRA Annex I objective, implementation component, verification method, evidence, and residual-risk decision.

ABOUT LEMBERG SOLUTIONS

Lemberg Solutions is a tech consulting and product engineering company with 15+ years of experience in embedded systems, IoT, AI, cloud, and cybersecurity.

For over 15 years, we have been helping companies to design, build and maintain connected products across regulated and safety-critical industries.



Digital
Experiences



Cloud & Devops



Embedded
Engineering



Data & AI

ISO 27001

ISO 9001

ISO 13485

Get a CRA readiness assessment for your device

Our engineers will identify security gaps in your product and define the controls and evidence you need to move toward compliance.



LinkedIn

Nazir Kohut 

TALK TO OUR CRA EXPERT



Program Manager at
Lemberg Solutions