Cybersecurity information for certified products

Introduction

This document provides public security and certification information for a STMicroelectronics certified product such as Common Criteria (CC) or SESIP.

In the context of CC and SESIP evaluations, this document:

- Summarizes the evaluated security properties and assurance levels achieved for the product (target of evaluation).
- Explains how these evaluations support customers' regulatory and conformity assessment efforts, including the EU Cyber Resilience Act (CRA) and the EU Cybersecurity Act (CSA).
- Provides public information to users expected by CSA, article 55, including security characteristics, secure usage conditions, limitations, and vulnerability handling.

This document is intended to:

- Inform users, customers, and end-manufacturers about the scope and conditions of the certification.
- Provide the minimum-security information necessary to use the product securely.
- Describe the main security characteristics, limitations, and vulnerability handling processes.

This document is a high-level overview and does not contain all security-relevant details. Detailed information is available to customers under NDA (or controlled access), according to confidentiality protection rules.

For access to detailed secure documentation, contact your usual STMicroelectronics representative or your STMicroelectronics sales / support channel.

1 Regulatory context

This document is intended to support compliance efforts of integrators and end-manufacturers using the *product* in the context of current and upcoming cybersecurity regulations.

In particular, this document contributes to:

- Providing users with the information required by CSA, article 55, including security characteristics, limitations, secure usage conditions, and vulnerability management.
- Demonstrating that the *product* underwent an independent security evaluation in line with CC or SESIP, as referenced in the CSA and cybersecurity certification schemes.

This document is informative and does not constitute a legal opinion on CRA, CSA, or any other regulation. Responsibility for assessing and demonstrating regulatory compliance for the final *product* or system lies with the end-manufacturer placing it on the market.

1.1 Acronyms and definitions

Table 1. Glossary

Term	Definition
CC	Common Criteria
CRA	EU Cyber Resilience Act
CSA	EU Cybersecurity Act
EAL*n*	Evaluation Assurance Level *n* (*n* = 1, 2, 3, 4, 5, 6, 7) (Common Criteria)
EUCC	European Union Cybersecurity Certification Scheme on Common Criteria
Product	In this documentation, *product* refers to the target of evaluation (for CC: TOE, for SESIP: platform)
PSIRT	Product Security Incident Response Team
PSIRT webpage	https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html
SBOM	Software bill of materials
SESIP	Security Evaluation Standard for IoT Platforms
SESIP*x*	SESIP assurance level *x* (*x* = 1, 2, 3, 4, 5)
TOE	Target of evaluation
Platform	Equivalent of TOE used in CC for SESIP

2 Product and certification overview

2.1 Product identification

All information on the *product* identification is stated in the certification report or public security target documents.

The certified *product* and its evaluated configuration are uniquely identified by:

- Product name and family
- Hardware and/or software version, including firmware build identifiers
- Configuration and options as specified in the public security target and certification report documents

Users must ensure that the product version, configuration, and associated guidance used in their system matches one of the configurations explicitly covered by the certificate.

2.2 Certification details

All information on certification, including the standard used, the scheme, and *product* evaluation assurance level, is provided in the certificate and the public security target.

The certificate remains valid as long as it is listed as such by the issuing scheme and is not suspended or withdrawn.

Key documents resulting from CC / SESIP evaluation include:

- The public security target defines:
  - Logical and physical scope of TOE under evaluation
  - Security problems to solve
  - Security objectives
  - Security functional requirements (SFRs)
  - Security assurance requirements (SARs)
- The certification report summarizes:
  - Evaluation outcome
  - Assurance level
  - Restrictions/limitations
  - Known residual risks
- The guidance documentation (AGD) shows:
  - How to install and configure securely
  - How to operate and maintain securely

These documents are essential to use the *product* correctly and do not assume higher security than actually evaluated.

The certification is performed under a recognized cybersecurity certification scheme (for example, EUCC or SESIP), in accordance with the CSA principles for EUCC.

The assurance level (for example, EAL*n*, SESIP*x*) reflects:

- The attack potential considered in the evaluation as stated in the public security target.
- The depth of assurance components (assurance classes: development review, testing, vulnerability analysis, life-cycle, and patch management evaluation, etc.).

The *product* is evaluated according to recognized cybersecurity certification standards and schemes.

The exact combination of EAL*n* and augmentation components applicable to a specific *product* or part number is stated in the corresponding public security target and certification report.

The main certification levels used by STMicroelectronics are:

1. CC EAL4+, EAL5+, and EAL6+ with the following meaning:
   The “+” indicates additional assurance components, for example, enhanced vulnerability analysis or life-cycle support.
   - EAL4+ (Methodically designed, tested, and reviewed, with selected augmentations)
     - Suitable for products where a substantial level of assurance is required.
     - Includes systematic design documentation, structured testing, and vulnerability analysis against a defined attack potential (often “high” or “enhanced basic”, as stated in the certificate).
   - EAL5+ (Semi-formally verified designed and tested, with selected augmentations)
     - Appropriate for security-critical applications where a strong, independently validated level of security is required.
     - High assurance level, including more detailed design descriptions and semi-formal design methods.
     - Vulnerability analysis is more extensive, typically targeting high attack potential adversaries.
   - EAL6+ (Semi-formally verified design and tested, with selected augmentations)
     - Used where failure could have major safety, financial, or regulatory consequences.
     - Very high assurance level, with semi-formal design verification and extensive testing and vulnerability analysis.
     - Assurance is additionally gained through a formal model of select TOE security policies and a semi-formal presentation of the functional specification and TOE design.
     - Intended for products that must resist highly skilled attackers with significant resources, within the attack potential defined in the public security target.
2. SESIP 3 with the following meaning:

- SESIP 3 targets a substantial attack potential and requires:
  - Rigorous testing and vulnerability analysis against software and logical attacks
  - Depending on the SESIP profile, analysis of certain physical attack vectors.
- The evaluation focuses on platform security services (for example, secure boot, secure storage, cryptographic operations and services, identity, platform identification, secure update and lifecycle management) typically used as a basis for connected devices and IoT platforms.

While CC and SESIP certifications are not, by themselves, a guarantee of compliance with the CRA or other regulations, they provide independent, auditable evidence that:

- Security objectives and requirements have been defined and systematically addressed.
- The *product* includes mechanisms to support secure integration and secure operation throughout its life cycle.
- Vulnerability management and update processes have been evaluated (where life-cycle components such as ALC_FLR are included).

Relationship to CRA and CSA (EUCC/SESIP)

- CC EAL*n* and SESIP*x* provide independent, auditable evidence that:
  - The *product*’s security functions have been designed and implemented using secure-by-design and secure-by-default principles appropriate to the targeted risk level.
  - Vulnerability handling and life-cycle processes have been evaluated (for example, ALC_* components, ALC_FLR.* for flaw remediation).
- Under CSA or CRA, EUCC and SESIP-based schemes can be leveraged as part of the evidence in a conformity assessment.
- These certifications support end-manufacturers in demonstrating alignment with CRA essential cybersecurity requirements, but do not alone guarantee full CRA compliance. CRA conformity must be assessed at system level by the end-manufacturer placing the final product on the market.

The valid certificate identifiers and scheme details are listed in the respective:

- EUCC certification reports.
- SESIP certification report.

2.3 Certificate URLs

2.3.1 Where to find EUCC certificates

The main public repositories for EUCC certificates are:

- EUCC portal:
- – ENISA: https://certification.enisa.europa.eu/certificates_en
- Common Criteria portal:
  - CC: https://www.commoncriteriaportal.org/products/index.cfm

2.3.2 Where to find SESIP certificates

- GlobalPlatform SESIP portal (or scheme operator's site):
  - Typically, the GlobalPlatform SESIP portal, accredited laboratories, or the scheme operator publish evaluated products.
- Some SESIP certificates are also listed via lab / scheme websites, with downloadable:
  - SESIP evaluation report (public summary)
  - SESIP security target or profile reference

3 Scope of evaluation (target of evaluation)

3.1 Target of evaluation (TOE)

The target of evaluation (TOE) is the subset of the product that is evaluated and certified.

For details, refer to the certification report and public security target.

The TOE scope is critical when considering CRA requirements. The evaluation covers only the subset of hardware, firmware, and/or software defined as the TOE in the public security target.

Customers and end-manufacturers must:

- Explicitly consider which parts of their system architecture are outside this TOE
- Perform complementary risk assessments and security measures for those out-of-scope components (for example, host OS, cloud back-end, mobile app, custom application logic).

For CC EAL*n*, the TOE is defined in the public security target and typically includes:

- The specific product hardware, firmware and/or software versions implementing the evaluated security functions.
- Security-relevant configuration items such as boot configuration, fuse settings, protection features, and interfaces in scope.
- The operational environment and assumptions that must be held to ensure that the evaluation results remain valid.

For SESIP*x*, the *platform* is described in the SESIP security target/ protection profile and typically includes:

- The platform security services (for example, secure boot, secure storage, cryptographic primitives, key management, identity provisioning).
- The life-cycle and update mechanisms relevant to IoT/connected platform security.

Customers and end-manufacturers must ensure that the product version and configuration used in their design:

- Match one of the configurations explicitly covered by the CC or SESIP evaluation
- Are addressed by a valid certificate

Deviations from the evaluated TOE configuration can reduce the effective security level. These deviations may no longer be covered by the claims associated with EAL*n* or SESIP*x*.

3.2 Elements explicitly out of scope

The following elements are **not** covered by the certification:

- Any configuration or usage of the *product* that deviates from the assumptions and secure configuration described in the official guidance and public security target.

For CRA and other regulatory compliance, the following items are explicitly out of scope of the certification and must be covered by the end-manufacturer own risk management and conformity assessment:

- Overall system security architecture and its alignment with CRA essential requirements.
- Security of added external components (for example, third-party libraries, cloud services or companion apps)
- Organizational processes (for example, secure development or incident response)

4 Main security functions

The main security functions contribute to fulfilling typical cybersecurity objectives as required by regulations such as the CRA, including:

- Identification and authentication:
  Supports controlled access to security-relevant functions and assets, mitigating unauthorized use of the *product*.
- Access control and isolation:
  Provides logical separation between different applications, users, or security domains, reducing the impact of a compromise and supporting defense-in-depth.
- Data protection and confidentiality:
  Protects data in transit and at rest against unauthorized disclosure (for example, through cryptographic mechanisms as defined in the public security target).
- Integrity and authenticity:
  Supports detection of unauthorized modifications (for example, secure boot, code integrity or firmware authenticity verification).
- Security audit and monitoring:
  Enables logging and monitoring of security-relevant events, facilitating detection of suspicious activity and supporting incident response obligations.
- Protection against attacks:
  Includes countermeasures against a defined set of attack methods and attack potentials (as specified in the public security target and certification report).

Customers and end-manufacturers should map these security functions to their CRA essential requirements and system-level threat model to demonstrate how the certified *product* contributes to overall risk reduction.

The precise list of security functional requirements and the level of resistance to attacks are defined in the public security target and the certification report published by the certification authority.

The security functions have been evaluated at EAL*n* under CC and/or SESIP*x* (depending on the *product* variant). This implies:

- Systematic and methodical verification that the functions meet the Security Functional Requirements (SFRs) defined in the public security target.
- Extensive vulnerability analysis and penetration testing considering attackers with a low up to high attack potential, within the boundaries defined by the specific EAL*n* or SESIP*x* evaluation.

When mapped to CRA essential cybersecurity requirements, the evaluated security functions contribute to:

- Identification and authentication
  - EAL*n* / SESIP*x* evaluation confirms robustness against common bypass techniques (for example, brute force, replay, protocol misuse) within the defined attack potential.
- Access control and isolation
  - Evaluated mechanisms enforce partitioning, least privilege, and domain separation, reducing the risk of lateral movement between components or applications.
- Data protection and confidentiality
  - Cryptographic services are validated for correctness and robustness against misuse and certain classes of attacks, as described in the evaluation reports.
- Integrity and authenticity
  - Secure boot, code authenticity checking, and integrity protection mechanisms are tested against attempts to introduce or execute unauthorized code.
- Security audit and monitoring
  - Security events and logs provided by the *product* help meet CRA expectations around detection and investigation of cybersecurity incidents.
- Protection against attacks
  - Certification reports describe the attack potential and attack methods, providing transparent information on the evaluated resistance level and residual risks.

5 Security assumptions, operating conditions, and end-manufacturers responsibilities

The effective cybersecurity level achieved in deployment depends on the correct fulfillment of the assumptions documented in the public security target and all guidance provided with the *product*.

In the context of the CRA, end-manufacturers must treat these assumptions as mandatory controls to be implemented in their system-level design, including:

- Secure deployment and configuration
  - Install and configure strictly according to the STMicroelectronics guidance.
  - Change default credentials, keys, and configuration before connecting to any production or public network.
  - Disable unused interfaces, services, and debug features in production deployments when possible.
- Secure environment
  - Ensure that physical protections are aligned with the attack potential assumed in the evaluation (for example, need for tamper resistance, restricted physical access) as specified in the public security target.
  - Provide adequate network protections (segmentation, firewall rules, secure protocols).
- Identity, key, and credential management
  - Use approved cryptographic algorithms and key sizes as specified in the *product* documentation and public security target.
  - Implement secure key lifecycle management (generation, storage, rotation, revocation, destruction).
- Software and update management (if needed)
  - Deploy only trusted firmware and software versions listed as part of the evaluated configuration, or versions explicitly covered by an updated certificate or maintenance report.
  - Implement processes to distribute and apply security updates within a timeframe consistent at least with CRA expectations.

Failure to comply with these conditions may significantly reduce the level of protection and could invalidate certification assumptions. Under the CRA, the end-manufacturer of the final product remains responsible for ensuring that configuration and deployment satisfy these conditions.

End-manufacturers are responsible for performing a system-level risk assessment, considering:

- The threats addressed by the *product* (as per the public security target).
- Additional threats that arise from their specific architecture and use cases.
- Any compensating controls needed to meet CRA essential requirements not fully covered by the *product*.

From a CC EAL*n* and SESIP*x* perspective, the assumptions and operational conditions described in this section:

- Form an integral part of the evaluated security model.
- Are explicitly documented in the public security target and evaluation reports.

If these assumptions are not met in deployment:

- The effectiveness of the evaluated security functions may be reduced.
- The assurance level associated with the certificate (EAL*n* or SESIP*x*) may no longer represent the actual security posture of the deployed system.

In the context of CRA:

- Customers and end-manufacturers must ensure that these assumptions are:
  - Captured in their system-level security architecture and risk assessment
  - Reflected in their own user documentation and configuration guidance for the final product in order to meet CRA article 13 and CSA article 55 obligations.

6 Limitations and residual risks

Even with certification, certain limitations and residual risks apply:

- The certification confirms that the *product* meets specified requirements within the scope and attack potential defined in the public security target.
- The certificate does not guarantee protection against:
  - Threats or attack methods beyond the evaluated attack potential.
  - Misconfiguration, insecure integration, or operational misuse.
  - New vulnerabilities or attack techniques discovered after the certification date.

Customers and end-manufacturers should integrate the *product* into their own risk management and defense-in-depth strategy and must not rely solely on the certification as the only security measure.

In line with CSA article 55 and CRA annex II, end-manufacturer must be informed about limitations and residual risks. For the *product*:

- The security mechanisms mitigate a defined threat model and are evaluated against a specified attack potential, as described in the public security target and certification report.
- Residual risks may include, but are not limited to:
  - Possibility of new vulnerabilities in the *product* or underlying technologies becoming public after the evaluation.
  - Misuse or misconfiguration of security features due to incorrect integration or operation.
  - Attacks that exceed the assumed attack potential (for example, very high-resource attackers).
- The *product* can rely on external components (for example, host OS, network stack, back-end services, applications) whose vulnerabilities can impact overall security, even if the certified functions behave correctly.

End-manufacturer must:

- Integrate the *product* into a defense-in-depth architecture, with complementary security controls at device, network, and back-end levels
- Monitor vulnerability advisories and apply recommended security measures in a timely manner (refer to Section 7: Security guidance for customer and end-manufacturer)
- Consider residual risks as part of their CRA-aligned risk management and provide appropriate information and documentation to their own customers and users.

Evaluation of boundaries and attack potential example

- For EAL4+, the evaluation confirms that the *product* withstands a substantial attack potential, with methodical testing and vulnerability analysis as defined in the public security target.
- For EAL5+, the evaluation includes more detailed design analysis and semi-formal methods, targeting a high attack potential attacker, including more sophisticated logical and, when specified, physical attacks.
- For EAL6+, the evaluation involves very detailed design and semi-formal verification and targets highly skilled attackers with significant resources, still within the specific attack potential defined in the public security target.
- For SESIP level 3, the evaluation focuses on substantial attack potential against platform security services, especially software, and logical attacks and selected physical threats.

Attacks that:

- Exceed the evaluated attack potential (for example, well-funded, nation-state-level adversaries)
- Use novel techniques beyond those considered “state of the art” at the time of certification may still compromise the *product* or its integration.

Under CRA, customers and end-manufacturers are expected to:

- Consider these residual risks in their own risk management and technical documentation.
- Implement additional defenses (for example, system-level monitoring, network segmentation, hardening, secure supply-chain) to address threats beyond the scope of the TOE and the evaluated attack potential.

7 Security guidance for customer and end-manufacturer

STMicroelectronics provides detailed security guidance to support secure deployment and operation of the *product*, including:

- Installation and software development support
- Secure configuration options and recommended settings
- Secure update and maintenance procedures
- Guidance on logging, monitoring, and incident response related to the *product*

In the context of CSA article 55, this guidance is intended to provide:

- Clear instructions for secure installation, configuration, operation, and maintenance of the *product*.
- Information on security capabilities and limitations, including how to enable, configure, and monitor security features.
- Information on how to apply security updates and mitigations when new vulnerabilities are communicated.

The following documentation supports customer and end-manufacturer in preparing their own CRA documentation (for example, EU declaration of conformity, technical documentation):

- Public documentation
  - Product public security target
  - Public certification reports (for example, EUCC, SESIP)
  - *PSIRT webpage* and public security advisories
  - Documentation accessible on STMicroelectronics website.
- Confidential documentation (under NDA or controlled access)
  - Detailed guidance on secure integration, secure boot, key management, and other sensitive aspects
  - Security application notes, reference designs, or platform security architecture

Customer and end-manufacturer are responsible for:

- Obtaining from STMicroelectronics and following the relevant security guidance corresponding to their requirement.
- Ensuring internal procedures are aligned with the recommendations.

End-manufacturer should reference this documentation when compiling:

- The system-level threat model and security architecture description.
- Evidence of secure configuration and security controls, to support CRA conformity assessment.

The *product* may provide logging and monitoring hooks (for example, security event flags, error reporting, audit logs). Integrators are responsible for:

- Capturing these events in their own logging infrastructure.
- Defining alerting, correlation, and incident response procedures aligned with their overall security operations and regulatory obligations.

For *products* evaluated at EAL*n* and/or SESIP*x*, the guidance documentation referenced in the public security target typically includes:

- Detailed installation procedures that enforce secure-by-default configuration.
- Configuration options that influence the evaluated security perimeter (for example, enabling/disabling debug ports, secure boot, or hardware protection features).
- Recommendations for key management, identity provisioning, and secure update processes that were considered during evaluation.

In the context of CSA article 55 and system-level conformity assessment, end-manufacturer can use:

- This public security and certification information document
- The public security target(s) and certification reports for EAL*n* and SESIP*x*
- The detailed (possibly under NDA or controlled access) guidance documents

and does:

- Document how the *product's* security features are used in their design
- Demonstrate secure configuration to notified bodies or market surveillance authorities
- Provide accurate security information to their own customers and users

8 Vulnerability disclosure and lifecycle management

To support continuous security throughout the product lifecycle, STMicroelectronics operates a vulnerability management and disclosure process, including:

1. Reporting of vulnerabilities
   - Potential security vulnerabilities can be reported to:
     - *PSIRT webpage*
2. Assessment and remediation
   - Reports are assessed, including impact on the certified scope or relevant regulation bodies (including communication with certification bodies).
   - Where needed, STMicroelectronics provides patches, configuration changes, or updated guidance.
3. Communication to customers
   - STMicroelectronics communicates:
     - Public security advisories via *PSIRT webpage*
     - Dedicated communication under NDA or controlled access.
   - Customers are expected to:
     - Monitor these channels
     - Evaluate the impact on their deployments
     - Apply recommended patches or mitigations in a timely manner

In compliance with industry best practices and aligned with the expectations of the CRA, STMicroelectronics maintains a structured vulnerability management process, covering:

- Proactive monitoring of publicly disclosed vulnerabilities relevant to the *product's* technology stack.
- Triage and risk assessment for each reported or identified vulnerability, considering impact on confidentiality, integrity, and availability, as well as on certified security properties.
- Development and validation of patches, configuration changes, or compensating controls.

Security update support period

STMicroelectronics commits to providing security updates for this *product* at least for the duration of the certificate validity period. For precise support timelines, refer to the *product's* commercial and lifecycle documentation or contact your STMicroelectronics representative.

In the context of CRA:

- End-manufacturer integrating this *product* into their own devices or systems remain responsible for:
  - Distributing updates to their end customers.
  - Providing end-user documentation and notifications about security advisories and required actions.
  - Ensuring that updates are applied within a timeframe consistent with the risk level.
- STMicroelectronics provides:
  - Public security advisories via the PSIRT webpage for issues that can be disclosed publicly.
  - Customer-specific notifications under NDA where appropriate (for example, when details could enable exploitation).

The *product's* CC and SESIP evaluations typically cover life-cycle and flaw remediation processes (for example, ALC_CM.*, ALC_DEL.*, ALC_FLR.*), providing independent assessment of:

- How STMicroelectronics manages configuration control and secure delivery.
- How STMicroelectronics handled security vulnerabilities from discovery to remediation and communication.

This supports CRA expectations that:

- End-manufacturers maintain vulnerability handling and coordinated disclosure processes.
- Security updates are made available and communicated for a defined period, coherent with the expected lifetime of the *product*.

End-manufacturer should:

- Integrate STMicroelectronics security advisories and updates into their own product maintenance processes.
- Ensure distribution and application of patches to end users, consistent with their own CRA obligations.

Note: Where the product includes third-party software or libraries, STMicroelectronics:

- *Tracks these components in its internal configuration management system.*
- *Monitors publicly disclosed vulnerabilities affecting these components.*
- *Assesses their impact on the product and communicates relevant mitigations or updates via the PSIRT process.*

End-manufacturers should maintain their own SBOM at system level and take into account dependencies introduced by additional software or hardware in their solution.

9 CRA and EUCC/SESIP compliance support

This section provides informative guidance on how the *product* and its certification may be used within a CRA or CSA compliance framework.

1. Contribution to CRA essential requirements
   The *product's* security mechanisms and its independent security evaluation (CC, SESIP) provide evidence supporting several CRA essential requirements, including:
   – Secure-by-design and secure-by-default principles.
   – Protection of confidentiality, integrity, and (where applicable) availability of data and services.
   – Mechanisms for secure updates and vulnerability handling.
2. Contribution to CRA conformity assessment
   Customer and end-manufacturer integrating this *product* can reference:
   – The public security target and certification report as objective evidence of implemented security controls.
   – This document as part of the information to users package.
   – STMicroelectronics PSIRT processes and life-cycle evaluation components as support for continuous security management.
3. Limitations
   – Certification and this document do not, by themselves, guarantee full compliance with the CRA or any other regulation.
   – CRA compliance must be assessed for the final product placed on the market, considering all hardware, software, and cloud components, as well as organizational processes.
4. Customer support for regulatory questions
   STMicroelectronics can support customers with additional documentation, under NDA or controlled access, to help:
   – Map *product* security features to CRA requirements and harmonized standards when available.
   – Provide more detailed evidence on secure development and life-cycle processes used for the *product*.

9.1 Cybersecurity information in accordance with CSA article 55

(a)

Guidance and recommendations to assist users with the secure configuration, installation, deployment, operation, and maintenance can be found in the security target on the ENISA site:

https://certification.enisa.europa.eu/certificates_en

Follow the certificate number and then the "Certification Documents".

(b)

The product is maintained during the validity of its certificate.

(c)

Information about accepted methods for receiving vulnerability information from users can be found at:

https://www.st.com/content/st_com/en/about/security-and-privacy/psirt.html

(d)

Vulnerabilities, if available, are listed on ENISA's European Vulnerability Database (EUVD):

https://euvd.enisa.europa.eu/

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
30-Mar-2026	1	Initial release.

Contents

List of tables

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.