Cybersecurity considerations for STMicroelectronics automotive serial EEPROMs

Introduction

ISO 21434 is an international standard that provides guidelines for cybersecurity risk management within the automotive industry. This standard aims to ensure that vehicles are designed with robust cybersecurity measures.

From July 2022, the UNECE UN regulation No.155 on cybersecurity management systems has become officially applicable and enforceable.

This technical note provides related documentation to support the cybersecurity activities of STMicroelectronics integrators:

According to the definition of the figure D.1 in the ISO/SAE 21434:2021 report, EEPROMs from STMicroelectronics are not cybersecurity relevant in terms of integrity (1), confidentiality (2), and availability (3) for user data. The integrator is responsible for protecting user data.

However, for the stored parameter data, the STMicroelectronics EEPROMs support the functional integrity and availability of such data.

For operating features and AC/DC parameters, refer to product datasheets available on the STMicroelectronics website.

The table below contains the list of products concerned by this technical note.

Table 1. Applicable products

Series	Root part number		
	M95xxx-Axxx	M24xxx-Axxx	M93xxx-Axxx
Automotive serial EEPROM	M95M04-A1x5	M24M02-A125	M93C86-A125
	M95M02-A125	M24M01-A125	M93C76-A125
	M95M01-A1x5	M24512-A125	M93C66-A125
	M95512-A1x5	M24256-A125	M93C46-A125
	M95256-A1x5	M24128-A125	-
	M95128-A1x5	M24C64-A125	-
	M95640-A1x5	M24C32-A125	-
	M95320-A1x5	M24C16-A125	-
	M95160-A1x5	M24C08-A125	-
	M95080-A1x5	M24C04-A125	-
	M95040-A1x5	M24C02-A125	-
	M95020-A1x5	-	-

1. *Data has been transmitted/processed as intended by the originator.*
2. *Data is accessible for intended users only.*
3. *Data can be accessed during an intended window of time.*

1 Integrator responsibility

STMicroelectronics EEPROMs were not originally designed to include embedded security features. As we advance into an era where cybersecurity is paramount, if the integrator expresses their desire to protect data, they should implement their own security procedures or features to ensure data confidentiality, such as scrambling and/or encryption.

Despite the previously mentioned points, it is the responsibility of the integrator to ensure data integrity and availability by implementing additional procedures.

Given the design and purpose of EEPROM, any cyberattack which may occur on our automotive EEPROMs are not due to the lack of actions taken by STMicroelectronics.

2 Functional features

2.1 Integrity

The list below contains the features present in STMicroelectronics EEPROMs that offer functional data integrity:

- **Identification page**:
  The identification page serves as an extra page that can be set to a permanent read-only status. Users can use this page to store particular application settings.
- **ECC** (error correction code):
  The built-in ECC logic feature rectifies errors concerning data storage. This ECC logic is applied to automotive EEPROMs for every group of one or four bytes, depending on the memory density. The operation of this function is completely invisible within the EEPROM communication protocol.
- **PoR** (power on reset):
  It is essential to adhere to the power-up and power-down protocols outlined in the corresponding datasheets. Following these guidelines ensures the optimal setup and use of the product.
- **Environment protection**:
  Due to a robust test flow (AEC-Q100 Grade 0) and proficiency in chip encapsulation, STMicroelectronics EEPROMs are safeguarded out of operating limits.
- **True byte granularity**:
  The STMicroelectronics EEPROM byte granularity enables the writing of individual bytes without impacting the adjacent data that was initially saved on the page. This capability removes the necessity to overwrite extensive data blocks for minor updates, enhancing the longevity of the STMicroelectronics EEPROMs.

2.2 Availability

- **High data retention performance**:
  The aim of EEPROMs is to maintain data storage without any loss over a designated timeframe. Owing to its high data retention capabilities, STMicroelectronics EEPROMs maintain data integrity (no data loss) over an extended period, and without the need to refresh.
- **High cycling endurance performance**:
  Cycling endurance denotes the quantity of write operations that the memory can execute before it fails to correctly record data. STMicroelectronics EEPROMs, with its high cycling endurance performance, handle a large number of write operations while the data remains accurate.
- **ESD (electrostatic discharge) protection**:
  STMicroelectronics EEPROMs provide a specialized protection circuit against HBM (Human body model) and undergo a rigorous qualification process in line with AEC-Q100 standards. This is a safeguard against internal component damage and data corruption due to electrostatic discharge.

2.3 Confidentiality

STMicroelectronics EEPROMs do not provide built-in features for data confidentiality protection. Consequently, if the data stored is sensitive, it is the integrator's responsibility to implement suitable security measures. Any cyberattack targeting STMicroelectronics automotive EEPROMs should not be seen as a consequence of inaction by STMicroelectronics, given the device design and intended use.

3 Statement

The functional features of the EEPROM products are described within a framework of normal use and compatibility with the product parameters that are specified in the datasheet.

4 Conclusion

STMicroelectronics EEPROMs are not originally designed to embed security features.

To protect against cyberattacks, the integrator must implement security procedures or features that ensure the integrity, the confidentiality, and the availability of user data.

In addition, the integrator has to support confidentiality for parameter data.

Revision history

Table 2. **Document revision history**

Date	Version	Changes
04-Jun-2025	1	Initial release.

Contents

List of tables