Site Security Target - Sipi Metals Corporation

Rev. 1.3 — 11 September 2020 **Objective evaluation document**

Revision History

Revision history

Revision number	Date	Description
1.0	25.06.2020	Initial version of the document, created first Version by NXP DITA Oxygen XML Template.
1.1	29.06.2020	SIPI specific information added reduced scope to reflect site services
1.2	13.07.2020	Update after AST comments from Brightsight
1.3	11.09.2020	Updated after additional comments

Classification

Company Public

1 SST Introduction

This document is based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors. Therefore, the term 'client' in this document refers directly to NXP Semiconductors.

1.1 Reference

Title:	SIPI_SST_Rev. 1.3
Version:	1.3
Date:	11th September 2020
Company:	Sipi Metals Corporation
Name of site:	Sipi Metals Corporation
EAL:	SARs taken from EAL6

1.2 Identification of the Site

The site Sipi Metals Corporation is located at:

```
1720 N. Elston Avenue
Chicago, Illinois 60642-1579
United States
www.sipicorp.com
```

The type of site is: Secure Destruction.

1.3 Site Description

1.3.1 Physical Scope

The entire building and the surrounding fenced area specified in Section 1.1 are in the scope of the SST. SIPI receive secured materials and have no knowledge or interaction with the content. SIPI is purely for the destruction of NXP materials. All NXP assets are constantly stored in the sealed drum therefor SIPI have no knowledge or interaction with the contents.

1.3.2 Logical Scope

The building specified in Section 1.1 supports activities of many other organizations, but only the secure destruction of NXP assets are in the scope of this SST. No classified logical information is transferred between SIPI and NXP. Activities of other organizations are not in scope of this SST.

2 Conformance Claim

This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, [2]

- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, [3]

For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017., [4]

- Minimum Site Security Requirement Version 3.0, February 2020 [10]

This SST is CC Part 3 conformant.
There are no extended components required for this SST for the SIPI Site.
The evaluation of the site comprises the following assurance components[2]:

- ALC_DVS.2,
- ALC_LCD.1,

3 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site.

Where necessary the items in this section have been re-worked to fit the site.

3.1 Assets

NXP assets involved in this process include wafers, die, masks, etc. for secure recorded destruction. The assets are all packed in a sealed drum.

3.2 Threats

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialised equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

T.Unauthorised-Staff: Unauthorised employees or subcontractors get access to assets, so that the confidentiality and/or the integrity of the intended TOE is violated.

T.Staff-Collusion: An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment. The target is to steal assets during the shipment/delivery process to gain access to TOE data.

3.3 Organisational Security Policies

P.Reception-Control: The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the received delivery can be identified and destroyed.

P.Product-Transport: Technical and organisational measures ensure the correct labelling of the intended delivery. A controlled internal shipment and/or the external delivery is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.

3.4 Assumptions

A.Item-Identification: For the processing of NXP material the client shall provide information which can be uniquely identify the delivered packages.

4 Security Objectives

The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organisational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorised people. The site enforces two or three levels of access control (GREEN, YELLOW, RED area) to sensitive areas of the site. The access control measures ensure that only registered employees and can access restricted areas. Sensitive deliveries are handled in restricted areas only.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (assets). After the alarm is triggered the unauthorised person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Staff-Engagement: All employees who have access to sensitive material and who can interact with deliveries are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job whatever is applicable for this site.

O.Zero-Balance: The site ensures that all sensitive products are separated and traced on a package unit basis. Two employee's acknowledgement during hand over is applied for all shipments. According to the agreed production flow all materials delivered are securely destroyed.

O.Reception-Control: Upon reception of any material an immediate incoming inspection is performed on the packaging with the delivery weight confirmed. The inspection comprises the received amount, their package identification and the assignment of the items to a related internal process.

O.Internal-Shipment: An appropriate internal secure shipment procedure is applied for all deliveries. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of delivery items during internal shipment. For every delivery item, the protection measures against manipulation are defined.

4.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

4.1.1 Mapping of Security Objectives

Table 1. Security Objectives Rationale

Threat and OSP	Security Objective	Note
T.Smart-Theft	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security**	The combination of security measures (physical, technical and organisational) ensure a detection of attacks and allows adequate reaction to prevent or limit damage.
T.Rugged-Theft	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security**	The combination of security measures ensure a detection of attacks and allows adequate reaction to prevent or limit damage.
T.Unauthorised-Staff	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security** **O.Staff-Engagement** **O.Zero-Balance**	Physical access control measures limit the access to sensitive areas to authorised person only.
T.Staff-Collusion	**O.Internal-Monitor** **O.Maintain-Security** **O.Staff-Engagement** **O.Zero-Balance**	Control procedures and personal accountability hinder collusion or allow to identify such attempts.

Threat and OSP	Security Objective	Note
T.Attack-Transport	**O.Internal-Shipment** **O.Reception-Control**	The security measures applied on sensitive data during internal shipment detect modification and prevent disclosure. The security measures applied on physical items during internal shipment allow detection of attempted attacks. The version of the assets of the site can be uniquely identified.
P.Reception-Control	**O.Reception-Control**	The control ensures the correct identification and assignment of all received items.
P.Product-Transport	**O.Internal-Shipment**	The correct destination address, the controlled packing and the tracing of the transport ensure the correct internal shipment.

5 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

6 Security Assurance Requirements

Clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [2].

The Security Assurance Requirements are chosen from the class ALC (Life-cycle support) as defined:

- Development Security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

The Security Assurance Requirements listed above fulfill the requirements of [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017.

6.1 Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the term “TOE” is not applicable in the Site Security Target, the associated processes for the handling of products, or “intended TOEs” are in the scope of this Site Security Target and are described in this document. These processes are subject of the evaluation of the site.

6.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

There is no claim for ALC_CMC compliance. At no time would SIPI interact with NXP material packages remained seal into the destruction tools. A CM system is employed to guarantee the traceability and identification of shipment numbers and content controlled by NXP shipping sites. Appropriate administration procedures are provided in order to maintain the integrity and confidentiality of the deliveries.

6.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

There is no claim for ALC_CMC compliance. At no time would SIPI interact with NXP material packages remained seal into the destruction tools. A CM system is employed to guarantee the traceability and identification of shipment numbers and content controlled by NXP shipping sites. Appropriate administration procedures are provided in order to maintain the integrity and confidentiality of the deliveries.

6.1.3 Overview and Refinements regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to

(i) the “development environment”,

(ii) to the “TOE” or “TOE design and implementation”. The component ALC_DVS.2 “Sufficiency of security measures” requires additional evidence for the suitability of the security measures.

The NXP materials delivered to SIPI are never interacted with by SIPI employees.

Based on these requirements the physical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

The SIPI site deals only with the destruction NXP material and has no knowledge of the material being destroyed.

6.1.4 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PP [2] provides a life-cycle description there specific life-cycles steps can be assigned to the tasks at site. This comprises solely for the secure destruction of NXP materials.

The PP [2] does not include any refinements for ALC_LCD. For a site under evaluation the dependencies to other sites must be explained if they are not covered by the obvious deliverables.

6.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [4] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of NXP materials before delivery to SIPI.

Table 2. Rationale for ALC_DVS.2

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to securely destroy NXP material in its environment.	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Staff-Engagement** **O.Internal_Shipment** **O.Zero-Balance**	Physical and structural protection is described by **O.Physical-Access** and **O.Zero-Balance**. The protection is supported by **O.Security-Control**, **O.Alarm-Response**, and **O.Internal_Shipment**. The personnel security measures are provided by **O.Staff-Engagement**.
SAR	**Security Objective**	**Rationale**
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE or TOE related material through the destruction process.	**O.Internal_Shipment** **O.Maintain-Security** **O.Reception_Control**	The combination of security measures described under **O.Maintain-Security** in ALC_DVS.2.1C above are regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous validation is part of the objectives **O.Reception_Control, O.Internal_Shipment**

Table 3. Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to for complete destruction.	**O.Zero-Balance**	The processes used for identification of the NXP materials are covered by **O.Zero-Balance**
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control used for complete destruction.	**O.Zero-Balance**	The site receives NXP materials purely for destruction. The applied production process is controlled according to **O.Zero-Balance**, the finished photomasks are verified according to .

7 Site Summary Specification

7.1 Preconditions Required by the Site

This section shall include justifications for the assumptions included in the SST. These assumptions are relevant for the splicing process since they must be examined during the product evaluation. Especially aspects like the classification of items and the appropriate provision of specifications for the site must be verified by checking appropriate evidence (e.g. the set of specifications provided to the site with a site certificate) during the product evaluation.

Table 4. Justification of Assumptions

Assumption	Justification
A.Item-Identification	For the processing of NXP material the client shall provide information which can be uniquely identify the delivered packages.

7.2 Services of the Site

S.Scrapping: This site provides a scrapping service for other sites having a business relationship with NXP, to hand in defect or rejected security items (e.g. finished, semi-finished, wafers, hard discs containing unencrypted data) which are destroyed according to the defined secure destruction process.

7.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

- **O.Physical-Access**
  The plant is surrounded by a fence. The plant is monitored by different surveillance measures. The building is separated in different access controlled areas. The physical and technical security measures implement a detection layer and a stop layer and ensure sufficient retardation of an attacker to enable appropriate reaction of the security service. The access control ensures that only registered persons can access sensitive areas or related assets.
  Thereby the threats **T.Smart-Theft** and **T.Rugged-Theft** can be prevented. Further on the physical separation of areas restricts access of employees and contractors to authorised areas preventing **T.Unauthorised-Staff**.
- **O.Security-Control**
  The control of the CCTV system, registration of contractors/ visitors, management of the access control system and patrol rounds are performed by trained security personnel. The security personnel are also responsible to follow up alarm messages generated by the surveillance systems.
  This addresses the threats **T.Smart-Theft** and **T.Rugged-Theft**. In addition an internal attacker triggers the security measures implemented by **O.Security-Control**. Therefore also the threat **T.Unauthorised-Staff** is addressed.
- **O.Alarm-Response**
  Based on **O.Physical-Access** attackers require a certain time to overcome the implemented protection layer. The response time of the security personnel and the resistance of the physical security measures match to provide an effective alarm response. The response is determined based on the information provided by the different control systems.
  The threats **T.Smart-Theft**, **T.Rugged-Theft** and **T.Unauthorised-Staff** are address by this security objective.
- **O.Internal-Monitor**
  Regular meetings of the security team are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This includes the assessment of security alarms and associated logs of the physical and logical protection. Changes of the security systems and security procedures are reviewed during management systems review meetings. In addition results of internal audits and assessments are reviewed.
  This addresses **T.Smart-Theft**, **T.Rugged-Theft**, **T.Unauthorised- Staff**, **T.Staff-Collusion**

- **O.Internal_Shipment**

  The security related surveillance is controlled by the secure internal shipping processes, they are reviewed and updated if needed. Logs of the associated systems are reviewed to support the work.
  This objective prevents **T.Smart-Theft**, **T.Rugged-Theft**, **T.Unauthorised-Staff**, and **T.Staff-Collusion**.
- **O.Staff-Engagement**
  All staff working at the site have to sign a non-disclosure agreement if they have access to sensitive items or data. This provides legal liability to protect the assets against disclosure. All employees are trained regarding security measures to support the security awareness.
  This objective prevents the threats **T.Unauthorised-Staff**, **T.Staff-Collusion**
- **O.Zero-Balance**
  Automated tracking within the process flow and the application of a 4-eyes-principle outside the process flow ensures a continuous tracking of sensitive items.
  The threats **T.Unauthorised-Staff**, and **T.Staff-Collusion**
- **O.Reception-Control**
  This objective prevents the threat **T.Attack-Transport** The organisational security policies and **P.Reception-Control** are addressed by the objective.

7.4 Security Assurance Requirements Rationale

The SAR Rationale does not explicitly address the developer action elements defined in [4] because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. This includes the requirement that the procedures are applied as written and explained in the documentation.

7.4.1 ALC_DVS.2

See Section 8.4.3 ALC_DVS.2 of [1].

7.4.2 ALC_LCD.1

See Section 8.4.4 ALC_LCD.1 of [1].

7.5 Assurance Measure Rationale

Some rationales are directly taken over from the template ([1]) others need some refinement because higher assurance requirements are claimed for ALC_CMC and ALC_CMS in this SST.

O.Physical-Access see Section 8.5 of [1].

O.Security-Control see Section 8.5 of [1].

O.Alarm-Response see Section 8.5 of [1].

O.Internal-Monitor see Section 8.5 of [1].

O.Maintain-Security see Section 8.5 of [1].

O.Staff-Engagement see Section 8.5 of [1].

O.Zero-Balance ALC_DVS.2.1C, ALC_LCD.1.1C and ALC_LCD.1.2C requires security measures that are necessary to protect the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Reception-Control ALC_DVS.2.2C: The security documentation shall show that a process is in place to ensure an appropriate level of identification and records to destruction are maintained. Thereby this objective is suitable to meet the Security Assurance Requirement.

7.6 Mapping of the Evaluation Documentation

In the scope of the evaluation no Configuration Management claimed. The specifications and descriptions provided by the client are not part of the configuration management at Sipi Metals Corporation

Table 5. Rationale for ALC_DVS.2

SAR	Aspects	References
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	Fence, access control to the building, surveillance, alarm system, receptionist and guard to prevent access to the building for unauthorised persons.	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]
	Internal storage of products in a strong room	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]
	Organisational measure to enforce security and alarm tracing	SipiDataDest SBNXP NXP SD Policy Secure Destruction Project Management
	Access control inside the building to enforce the production and control by authorised persons only	SipiDataDest SBNXP NXP SD Policy Secure Destruction Project Management

SAR	Aspects	References
	Trustworthiness and tracing of employees	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]
	Destruction of sensitive documents, data, products and other items	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]
ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	The justification is provided in this security target because it shows that all threats are addressed by the measures. In addition the measures are monitored to control the effectiveness.	Section 7

Table 10. Rationale for ALC_LCD.1

SAR	Aspects	References
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.	The intended TOE is developed and maintained according to the Release Manual.	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	The development control of the client NXP Semiconductors provides the necessary control and compliance of the development environment in use.	SipiDataDest SBNXP [7] NXP SD Policy [8] Secure Destruction Project Management [9]

8 Bibliography

[1] Eurosmart. Site Security Target Template, Version 1.0, 21.06.2009.

[2] Eurosmart. Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, 2014.

[3] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[4] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017.

[5] Common Criteria. Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[6] Common Criteria. Supporting Document Guidance, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.

[7] SIPI Security Procedures and Protocols

[8] NXP SD Policy

[9] Secure Destruction Project Management NXP

9 Legal information

9.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

9.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Tables

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 25 June 2020