AN13016

OM-SE051ARD hardware overview

Rev. 1.2 — 7 December 2020 Application note

Document information

Information	**Content**
Keywords	OM-SE051ARD, EdgeLock SE051
Abstract	This document describes the OM-SE051ARD development kit and details how to use its jumpers to configure the different communication options with the EdgeLock SE051 security IC.

Revision history

Revision history

Revision number	Date	Description
1.0	2020-10-19	First release
1.1	2020-11-27	Minor fix applied in Section 1.
1.2	2020-12-07	Updated to latest template and fixed broken links

1 Overview

The EdgeLock SE05x product family offers enhanced Common Criteria EAL 6+ based security, for unprecedented protection against the latest attack scenarios. This ready-to-use family of secure elements for IoT devices provides a root of trust at the IC level and supports the increasing demand for easy-to-design and scalable IoT security.

The EdgeLock SE05x uses I^{2}C as communication interface and its commands are wrapped using the Smartcard T=1 over I²C (T=1oI2C) protocol. In addition, the EdgeLock SE05x supports the following interfaces, as shown in Figure 1:

- I^{2}C interface in slave mode with date rates up to 3.4 Mbps .
- I^{2}C interface in master mode with date rates up to 400 Khz.
- ISO/IEC 14443 T=CL protocol.

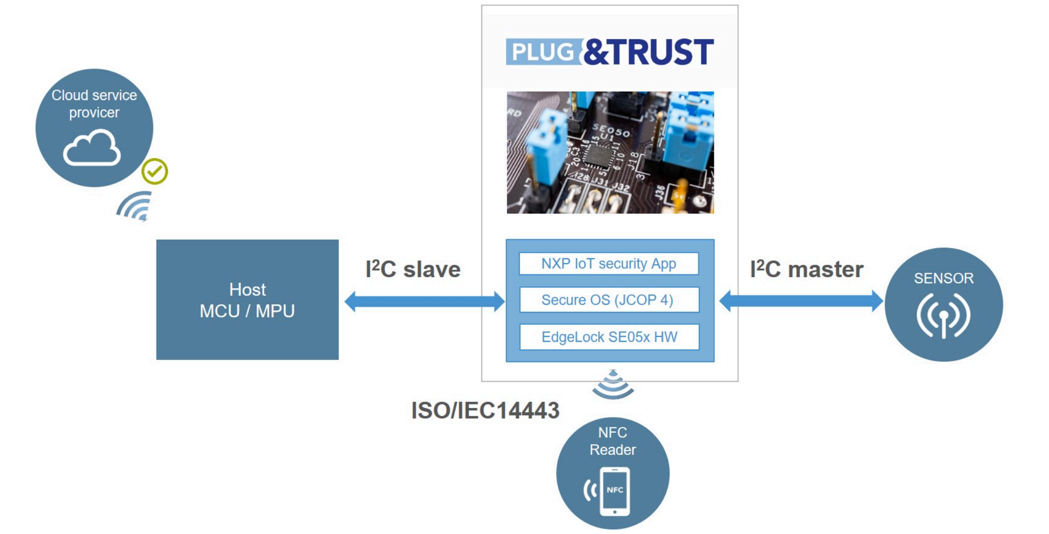

Figure 1. EdgeLock SE05x interface overview

Note: *Only the I^{2}C slave interface is mandatory. The I^{2}C master and ISO/IEC 14443 interfaces are optional.*

The OM-SE051ARD is the development kit for the EdgeLock SE051 security IC and comes soldered with the part `SE051C2HQ1/Z01XD`. Table 1 list the ordering details of OM-SE051ARD development kit.

Table 1. OM-SE051ARD development kit ordering details

Part number	12NC	Content	Picture
OM-SE051ARD	935399187598	SE051 Arduino® compatible development kit	

Note: *The OM-SE051ARD board has the same schematic and layout as the OM-SE051ARD board.*

2 Headers and connectors

The OM-SE051ARD is designed with several headers and connectors that allow you to interface with EdgeLock SE051. The OM-SE051ARD is equipped with:

- **Arduino-R3 header:** It allows you to easily attach it to any NXP MCU/MPU development board with Arduino compatible headers such as many Kinetis, LPC and i.MX MCU boards. The Arduino-R3 female connectors come soldered in the OM-SE051ARD.
- **External I^{2}C connector:** It allows you to connect any non-Arduino compatible MCU boards via I^{2}C slave interface. The OM-SE051ARD includes the mounting holes for the External I^{2}C connector.
- **10-pin header:** It allows you to access several pins of the EdgeLock SE051, including the I^{2}C master interface to attach sensors or peripherals to the board. The 10-pin header male connectors come soldered in the OM-SE051ARD.
- **DB15 header:** It allows you to access several pins of the EdgeLock SE051, including the ISO/IEC 14443 or the I^{2}C master interface to attach sensors or peripherals to the board. The OM-SE051ARD includes the mounting holes for the DB15 connector.

Figure 2 shows an overview to OM-SE051ARD headers and connectors together with its corresponding pin description.

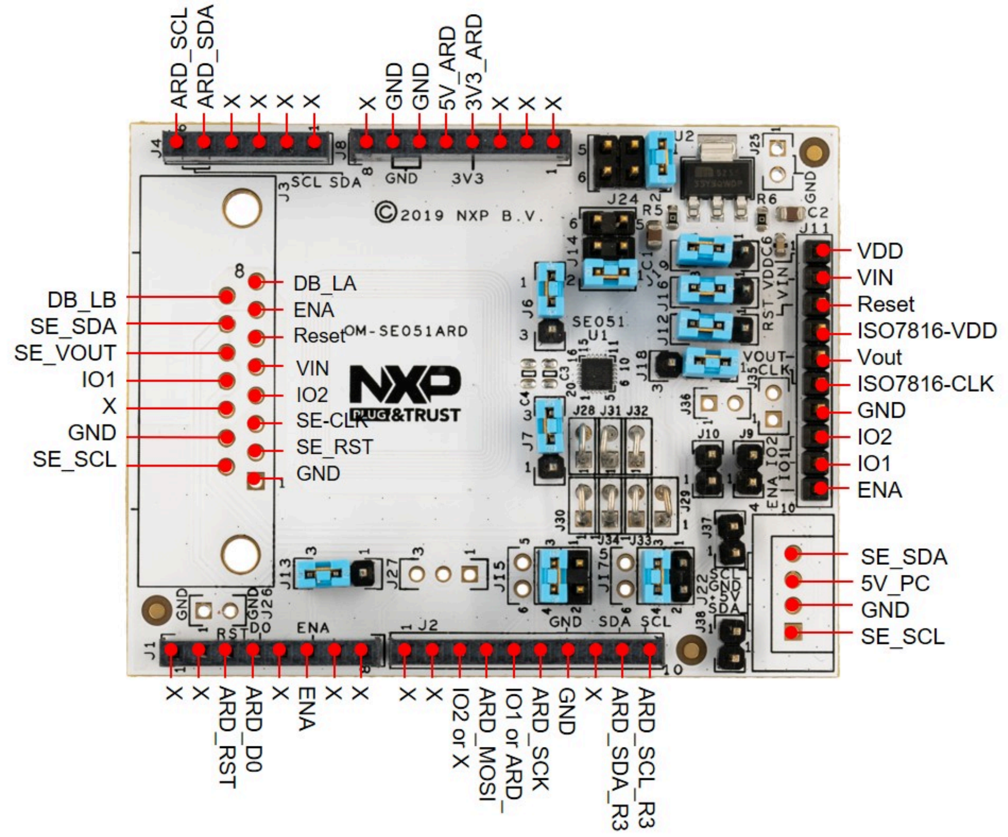

Figure 2. OM-SE051ARD headers and connectors overview

Note: *The OM-SE051ARD schematic is available in SE051ARD-SCH.*

3 Jumpers overview

The OM-SE051ARD board uses individual jumpers to configure settings related with the EdgeLock SE051 interfaces, power supply and power modes. This section provides an overview to the OM-SE051ARD jumpers and its configuration options.

3.1 I^{2}C configuration

The OM-SE051ARD has jumpers that allow you to control the configuration of the I^{2}C slave and master interfaces available in EdgeLock SE051. These jumpers are:

- J9, J10: Configures the I^{2}C master pull up connection.
- J15, J17: Configures the I^{2}C slave connection.
- J37, J38: Configures the I^{2}C slave interface pull up resistor.

Table 2 describes the OM-SE051ARDjumper settings for each I^{2}C setting configuration.

Table 2. Jumpers for I^{2}C configuration

Jumper	Description	Open	1-2	3-4
J9	I^{2}C Master pull up connection	not connected (Default)	3k3 Ohm	n.a.
J10	I^{2}C Master pull up connection	not connected (Default)	3k3 Ohm	n.a.
J15	I^{2}C Slave SDA connection	not connected	Arduino R3 J4:5	Arduino R3 J2:9 (Default)
J17	I^{2}C Slave SCL connection	not connected	Arduino R3 J4:6	Arduino R3 J2:10 (Default)
J18	SE051_IO2 routing	n.a	Routed to J11:9 (Default)	Routed to J2:3
J37	I^{2}C Slave SCL pull up	3k3 Ohm (Default, FastMode)	660 Ohm (HS-Mode)	n.a.
J38	I^{2}C Slave SDA pull up	3k3 Ohm (Default, FastMode)	660 Ohm (HS-Mode)	n.a.

Figure 3 highlights in blue the location of theOM-SE051ARD for I^{2}C settings configuration.

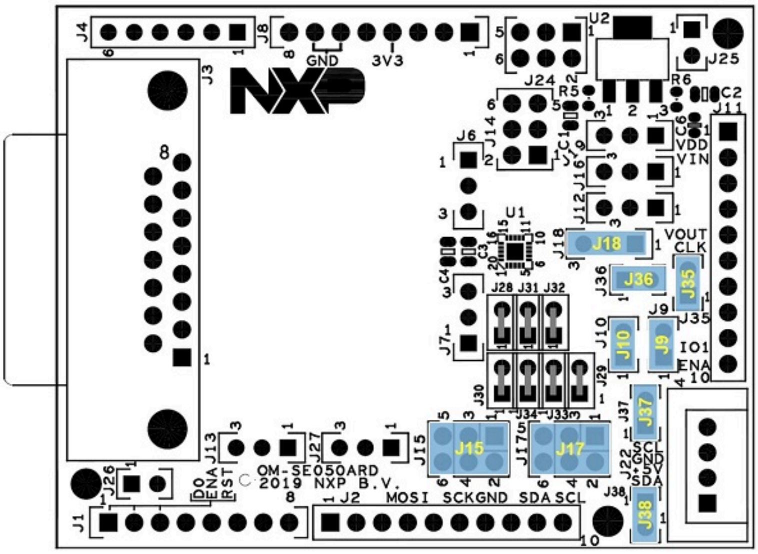

Figure 3. OM-SE051ARD jumpers for I^{2}C settings configuration

3.2 Power supply options

The jumpers that allow you to change the OM-SE051ARD power supply settings are:

- J19: Configures V_{DD} supply voltage options.
- J16: Connfigures SE051_V_{IN} supply options.
- J24: Configures V_{DD} supply voltage options in case the LDO is used.

Table 3 describes the OM-SE051ARDjumper settings for each power supply settings configuration.

Table 3. Jumpers for power supply settings configuration

Jumper	Description	1-2	2-3	3-4	5-6
J16	EdgeLock SE051_V_{in} supply	Supplied by J11:2 pin	Supplied by the V_{DD} (see J19) (Default)	n.a.	n.a.
J19	V_{DD} supply voltage	From LDO	From 3V3_ ARD pin (Default)	n.a.	n.a.
J24	V_{DD} supply voltage (if LDO is used)	From 5V_PC (External I^{2}C connector - Default)	n.a.	From 5V_ DB15 pin	From 5V_ARD pin

Figure 4 shows the power supply unit schematics.

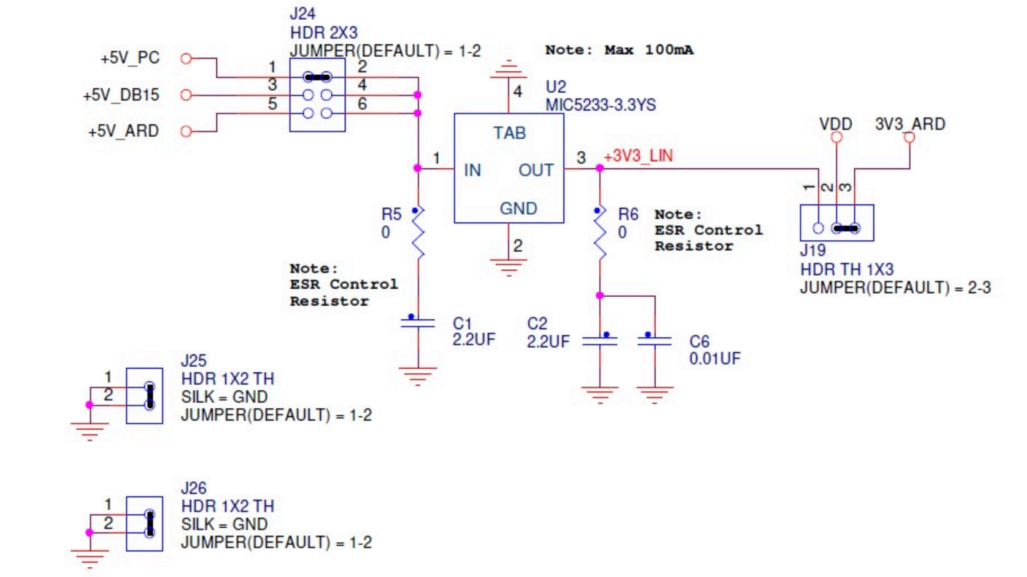

Figure 4. OM-SE051ARD power supply settings

Figure 5 highlights in blue the location of theOM-SE051ARD for power supply settings configuration.

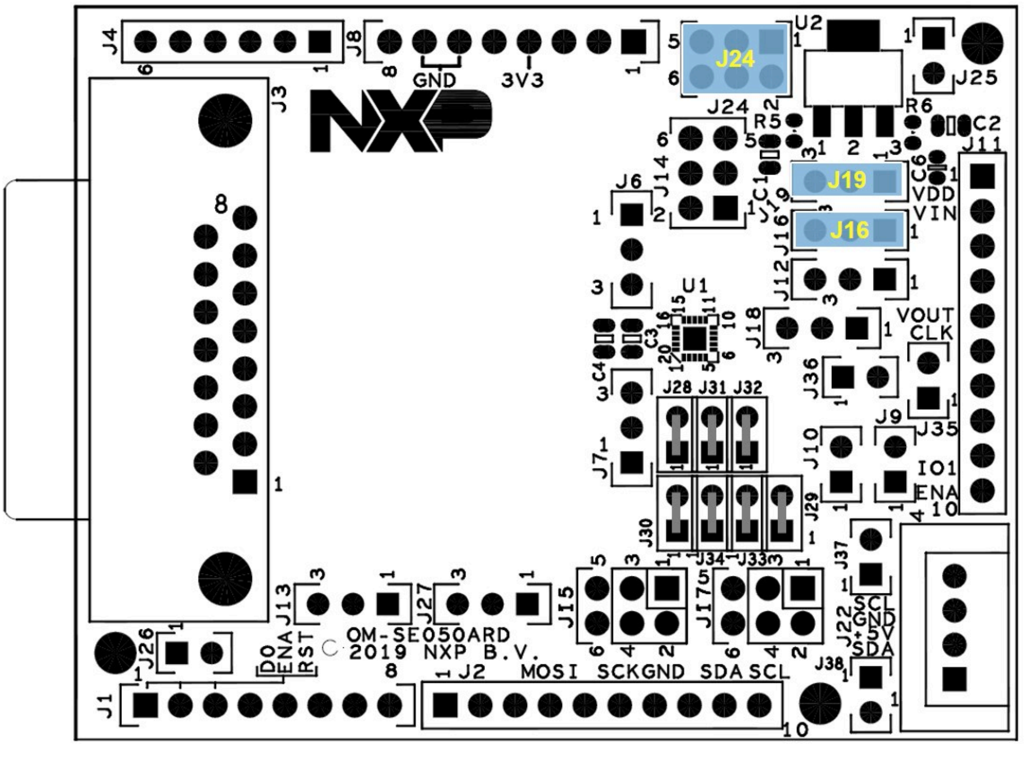

Figure 5. OM-SE051ARD jumpers for power settings configuration

3.3 Deep power-down mode

The deep power-down mode reduces the EdgeLock SE051 power consumption to the minimum. In this mode, only I^{2}C pads stay supplied via V_{in}. The deep power-down mode is enabled by setting the ENA pin to a logic zero. In addition, it is required to supply V_{in} pin and connect V_{out} and V_{cc} pins at the PCB level.

The ENA pin controls an internal switch between V_{out} and V_{in} as shown in Figure 6. Therefore, if V_{out} is connected to V_{cc}, the ENA pin can effectively switch the power on and off to V_{cc}.

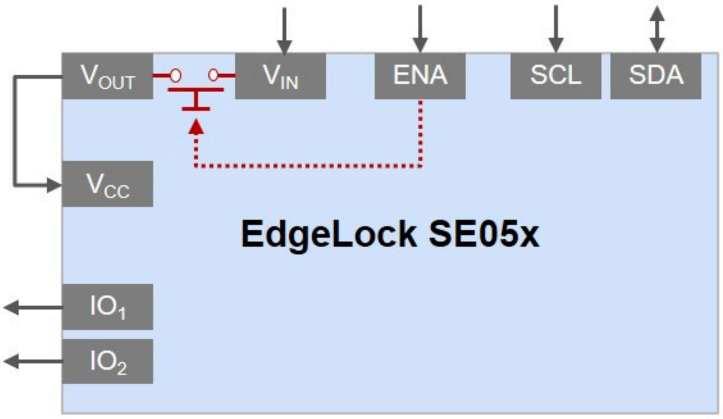

Figure 6. Deep power-down mode diagram

The jumpers J13 and J14 of the OM-SE051ARD allow you to control the EdgeLock SE051 deep power-down mode. To enable the deep power-down mode using the OM-SE051ARD:

- J13: Must be set to position 2-3.
- J14: Must be set to position 3-4.

Table 4 describes the OM-SE051ARD jumper settings for the deep power-down mode configuration

Table 4. Jumpers for deep power-down mode configuration

Jumper	Description	1-2	2-3	3-4	5-6
J13	EdgeLock SE051_ENA pin routing	ENA low. Switch disabled	ENA controlled by Arduino R3 (Default)	n.a.	n.a.
J14	EdgeLock SE051_V_{CC} pin routing	Routed to V_{DD} supply voltage	n.a.	Routed to SE051_V_{out} pin (Default)	Routed to J11:4 pin

Figure 7 highlights in blue the location of jumper J13 and J14.

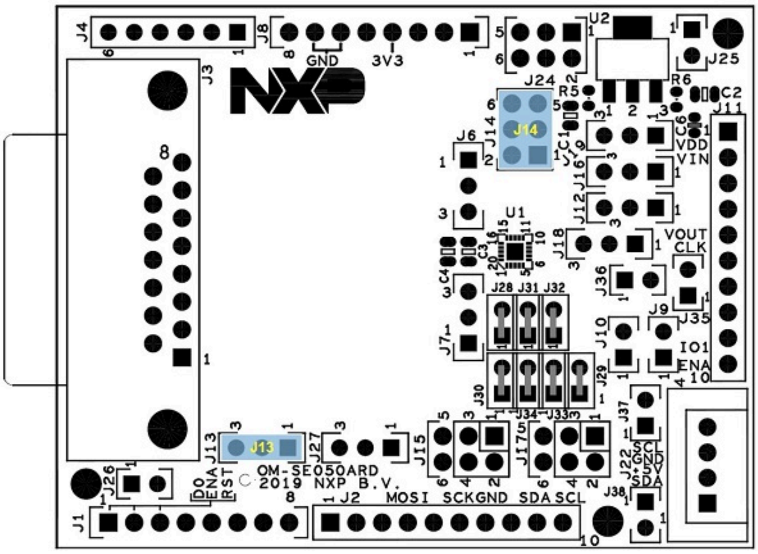

Figure 7. OM-SE051ARD jumper J13 and J14 location

3.4 Reset pin routing

Jumper J12 allows you to control the I^{2}C reset pin routing of the EdgeLock SE051. Table 5 indicates the J12 configuration.

Note: *The EdgeLock SE051 reset pin does not apply for the I^{2}C interface.*

Table 5. Jumpers for reset pin routing configuration

Jumper	Description	Open	1-2	2-3
J12	EdgeLock SE051_RST pin	Not connected	Routed to J11:3 strip pin connector	Routed to Arduino R3 (Default)

Figure 8 highlights in blue the location of Jumper J12.

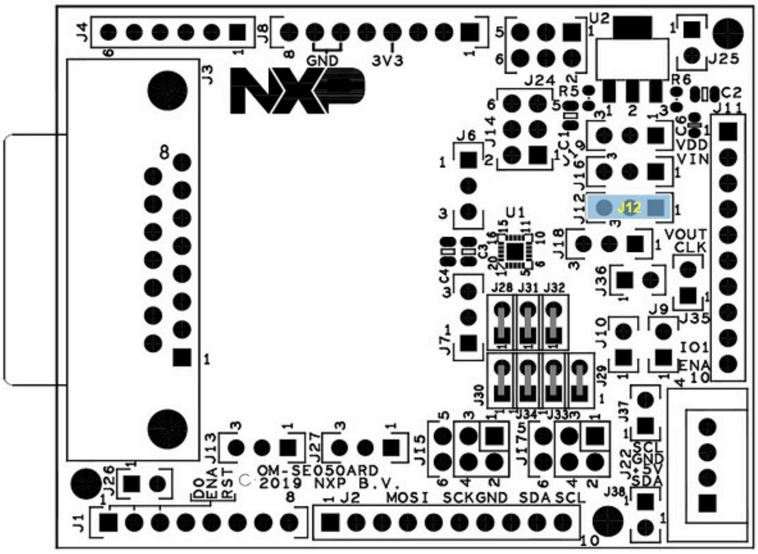

Figure 8. OM-SE051ARD Jumper J12 location

3.5 ISO/IEC14443 contactless interface

Jumper J6 and J7 allow you to control the EdgeLock SE051 contactless interface and allows you to select which antenna shall be used for contactless communication. Table 6 indicates J6 and J7 jumper settings.

Table 6. Jumpers for ISO/IEC14443 contactless interface settings

Jumper position	Description
J6: 2-3 and J7: 1-2	Contactless operation disabled
J6: 1-2 and J7: 2-3	Contactless operation disabled (Default)
J6: 2-3 and J7: 2-3	Contactless operation enabled with OM-SE051ARD internal antenna
J6: 1-2 and J7: 1-2	Contactless operation enabled with external ID1 antenna through DB15 connector

Figure 9 highlights in blue the location of jumpers J6 and J7.

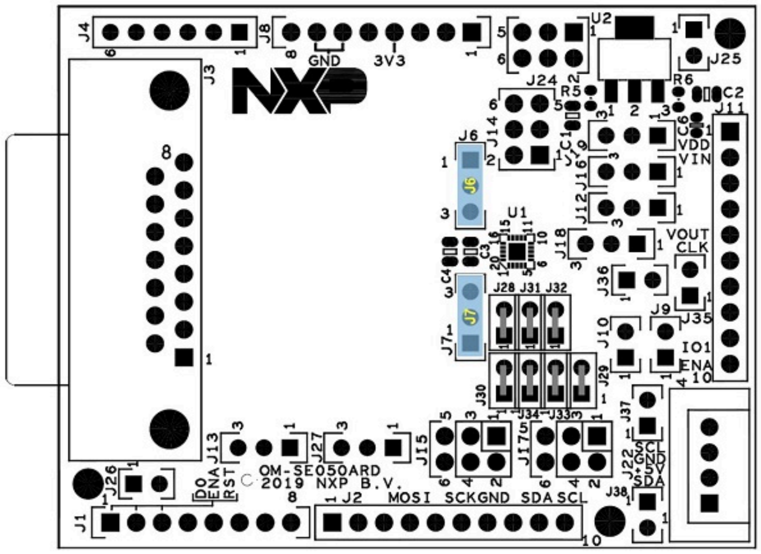

Figure 9. OM-SE051ARD jumper J6 and J7 location

4 OM-SE051ARD board use cases

This section details the jumper settings to configure the differnet interfaces and to enable specific use cases with the OM-SE051ARD board.

4.1 EdgeLock SE051 via Arduino header

This section details the jumper configuration to enable the I^{2}C slave interface in the Arduino header. The related jumpers of the OM-SE051ARD for I^{2}C slave interface configuration are:

- J37 and J38: Configure the pull up resistors of the I^{2}C interface.
- J19: Configures V_{DD} supply voltage options.
- J24: Configures V_{DD} supply voltage options in case the LDO is used.

Table 7. Jumper settings for I^{2}C slave interface configuration

Jumper	Configuration	Comment
J6	Set to 1-2 (Default)	Contactless operation disabled
J7	Set to 2-3 (Default)	Contactless operation disabled
J9, J10	Set to “Open” (Default)	I^{2}C master pull ups disabled
J12	Set to 2-3 (Default)	SE_RST routed to ARD_RST on J1:3
J13	Set to 2-3 (Default)	SE_ENA set to ARD_ENA on J1:6
J14	Set to 3-4 (Default)	SE_V_{OUT} as SE_V_{DD}
J15	Set to 3-4 (Default)	I^{2}C_SDA routed to ARD_SDA_R3 (J2:9)
	Set to 1-2	I^{2}C_SDA routed to ARD_SDA (J4:5)
J16	Set to 2-3	V_{DD} as SE_V_{IN}
J17	Set to 3-4 (Default)	I^{2}C_SCL routed to ARD_SCL_R3 (J2:10)
	Set to 1-2	I^{2}C_SCL routed to ARD_SCL (J4:6)
J19	Set to 2-3 (Default)	SE_V_{DD}=3.3V from Arduino-R3 voltages
	Set to 1-2	SE_V_{DD}=3.3V from LDO.
J24	Set to 1-2 (Default)	No input LDO
	Set to 5-6	5V_ARD to LDO
J25, J26	Do not care	Dummy jumpers
J37, J38	Set to “Open” (Default)	3k3 pull-up resistor for I^{2}C standard mode

Table 7. Jumper settings for I^{2}C slave interface configuration...*continued*

Jumper	Configuration	Comment
	Set to "Closed"	Additional 820 Ohm parallel pull-up resistor for I^{2}C high speed mode

Figure 10 shows the jumper settings to configure the I^{2}C slave in standard mode and 3.3V_ARD supply voltage (no LDO).

In this example, the jumper configuration used in Figure 10 correspond to the values highlighted in bold in Table 7 (J15, J17, J19, J24, J37 and J38).

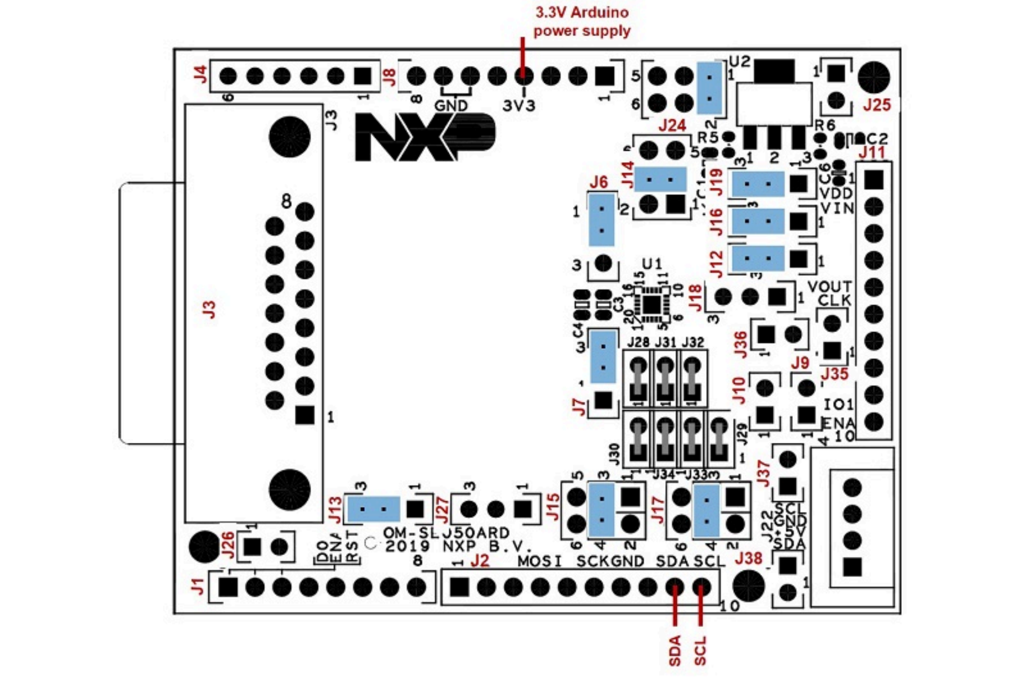

Figure 10. I^{2}C standard mode and 3.3V Arduino power supply

You may modify the I^{2}C mode or power supply settings just changing the jumper settings accordingly as indicated in Table 7.

4.2 SE051 via external I^{2}C connector

Figure 11 shows the jumper settings to configure EdgeLock SE051 communication via external I^{2}C connector:

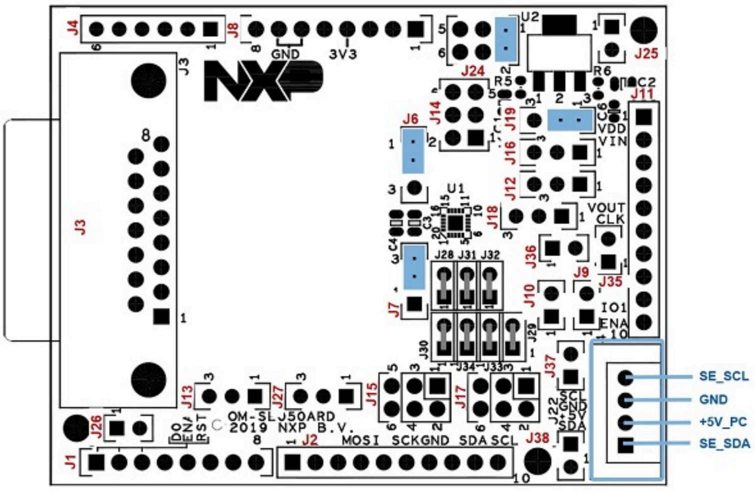

Figure 11. OM-SE051ARD external I^{2}C connector

Table 8 details the jumper settings for this configuration (External I^{2}C connector).

Table 8. OM-SE051ARD external I^{2}C connector

Jumper	Configuration	Comment
J6	Set to 1-2 (Default)	Contactless operation disabled
J7	Set to 2-3 (Default)	Contactless operation disabled
J9, J10	Do not care	
J12	Do not care	
J13	Do not care	
J14	Do not care	
J15	Do not care	
J16	Do not care	
J17	Do not care	
J19	Set to 1-2	3.3V from LDO as SE_V_{DD}
J24	Set to 1-2 (Default)	5V_PC from external MCU board to LDO
J25, J26	Do not care	Dummy jumpers
J37, J38	Set to “Open” (Default)	3k3 pull-up resistor for I^{2}C standard mode

4.3 SE051 in I^{2}C master mode

This section details the jumper configuration to enable the I^{2}C master of the SE051. The I2C master interface can be used to connect a sensor securely. The SE051 guarantees the privacy and the authenticity of the data extracted by sensor. The data collected in the application over the SE051 private sensor can be transferred to the cloud for further treatment and analysis. The Figure 12 shows the SE051 solution block diagram for this use case:

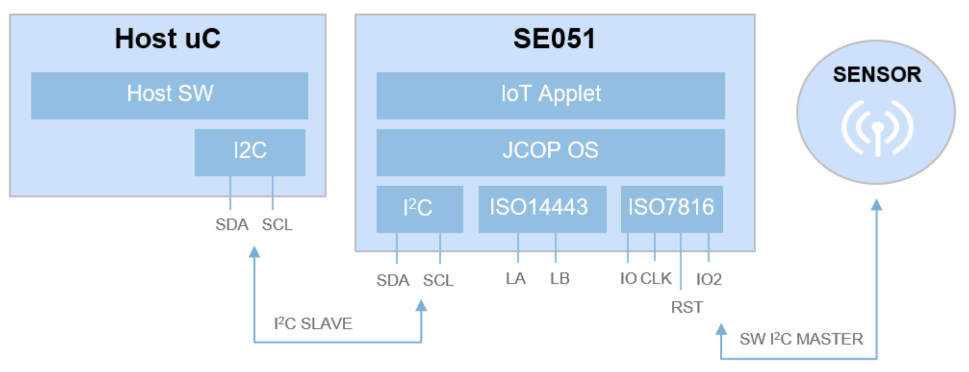

Figure 12. SE051 smart sensor use case block diagram

Figure 13 shows the jumper settings to enable the SE051 I^{2}C master interface.

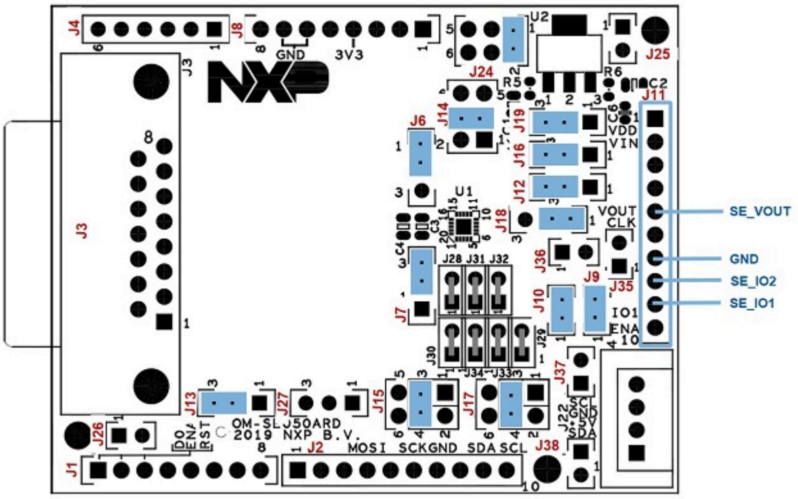

Figure 13. EdgeLock SE051 in I^{2}C master mode

Table 9 details the jumper settings for the configuration of the SE051 I^{2}C master interface.

Table 9. Jumper settings for EdgeLock SE051 in I^{2}C master mode

Jumper	Configuration	Comment
J6	Set to 1-2 (Default)	Contactless operation disabled
J7	Set to 2-3 (Default)	Contactless operation disabled
J9, J10	Set to "Closed"	Set to “Closed” to enable pull-up resistors for I^{2}C master signals SE_IO1 and SE_IO2 *(if IOT sensor board not already provides pull-up resistors)*.
J12	Set to 2-3 (Default)	SE_RST routed to ARD_RST on J1:3

Table 9. Jumper settings for EdgeLock SE051 in I^2C master mode*...continued*

Jumper	Configuration	Comment
J13	Set to 2-3 (Default)	SE_ENA set to ARD_ENA on J1:6
J14	Set to 3-4 (Default)	SE_V_{OUT} as SE_V_{DD}
J15	Set to 3-4 (Default)	I^2C_SDA routed to ARD_SDA_R3 (J2:9)
J16	Set to 2-3	V_{DD} as SE_V_{IN}
J17	Set to 3-4 (Default)	I^2C_SCL routed to ARD_SCL_R3 (J2:10)
J18	Set 1-2 (Default)	SE_IO2 to pin 9 of header J11
J19	Set to 2-3 (Default)	SE_V_{DD}=3.3V from Arduino-R3 voltages
J24	Set to 1-2 (Default)	No input LDO
J25, J26	Do not care	Dummy jumpers
J37, J38	Set to “Open” (Default)	3k3 pull-up resistor for I^2C standard mode

4.4 EdgeLock SE051 via ISO14443 mode

This section details the jumper settings to operate the OM-SE051ARD via the ISO/IEC14443 interface.

Note: *Only the I^2C slave interface is mandatory. The I^2C master and ISO/IEC 14443 interfaces are optional.*

4.4.1 ISO/IECC 144443-A via onboarded antenna

Figure 14 shows the jumper settings to configure the contactless interface via the onboarded antenna in the OM-SE051ARD board.

Note: *The IC selects the active interface on boot up, only one interface will be active. Take care for the interface precedence on IC boot up as described in the datasheet section "startup behavior" as I2C takes precedence over the contactless interface.*

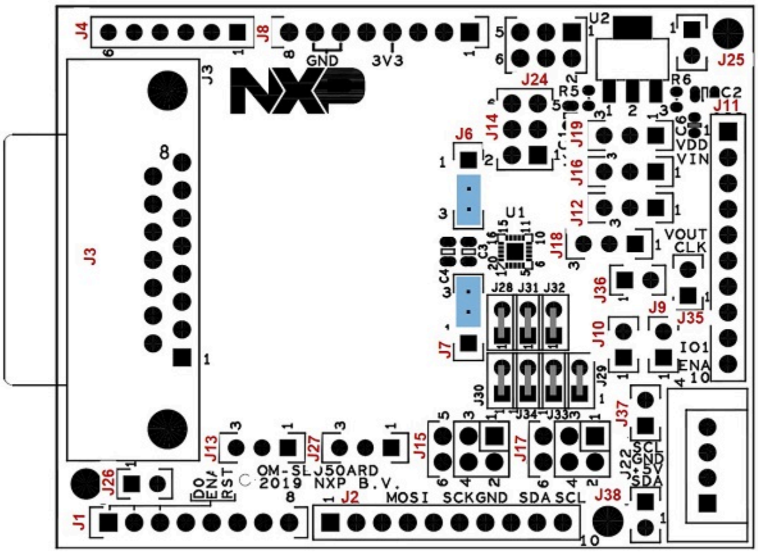

Figure 14. ISO/IEC14443 via onboarded antenna

Table 10 details the jumper settings for this configuration (ISO/IEC14443 via onboarded antenna).

Table 10. ISO/IEC14443 via onboarded antenna

Jumper	Configuration	Comment
J6	Set to 2-3	Contactless operation enabled with onboarded antenna
J7	Set to 2-3	Contactless operation enabled with onboarded antenna

4.4.2 ISO/IECC 144443-A via external antenna

Figure 15 shows the jumper settings to configure the contactless interface via an IN-CLA7816 probe connected through DB15 connector.

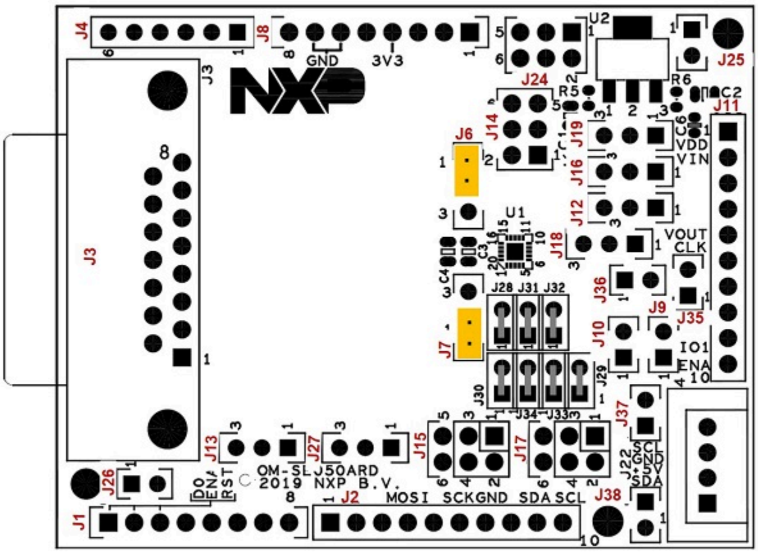

Figure 15. ISO/IEC14443 via DB15 connector

Table 11 details the jumper settings for this configuration (ISO/IECC 144443-A via external antenna).

Table 11. ISO/IEC14443 via DB15 connector

Jumper	Configuration	Comment
J6	**Set to 1-2**	**Contactless operation enabled with external ID1 antenna through DB15 connector**
J7	**Set to 1-2**	**Contactless operation enabled with external ID1 antenna through DB15 connector**

4.4.3 ISO/IEC 14443 via DB15 connector

Figure 16 shows an external contactless interface connected to an IN-CLA7816 probe through DB15 connector.

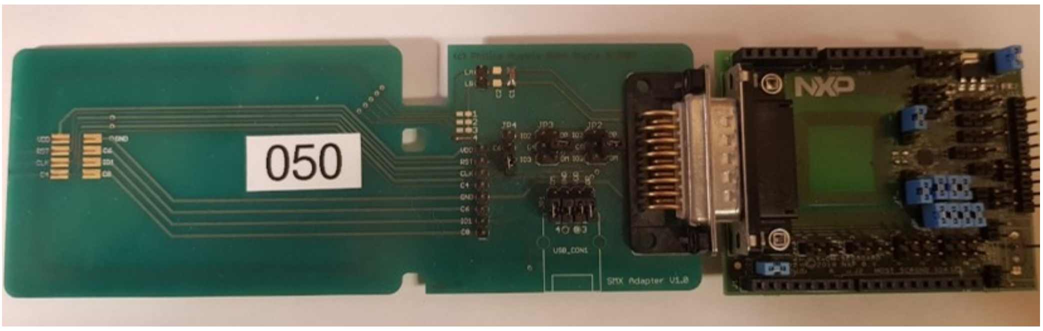

Figure 16. External contactless interface connected to an IN-CLA7816 probe through DB15 connector

5 Legal information

5.1 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.

5.2 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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

5.3 Trademarks

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

Tables

Figures

Contents

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: 7 December 2020