The standard for secure digital services and devices

GlobalPlatform Technology

Next Gen APDU Transport

Version 1.0.0.34

Public Review

April 2025

Document Reference: GPC_SPE_172

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

Tables

Figures

1 INTRODUCTION

More and more devices like mobile devices, wearables, or other IoT (Internet of Things) devices are now using soldered Secure Elements (SEs). This has generated new needs to support physical interfaces such as SPI or I^2C in lieu of the former ISO/IEC 7816 interface.

This specification describes how APDUs (as defined in [7816-3]) may be conveyed over these alternative physical interfaces. It defines a more efficient way to transfer longer payloads and adapt to the specific features of each underlying physical interface (SPI, I^2C, I3C, and ISO/IEC 7816).

A special use case is described to address the data transfer operation taking place during manufacturing (initialization, pre-personalization, personalization) whereby some further optimization in the control flow may be applied to reduce the implementation memory footprint and increase performance.

1.1 Audience

This specification is intended primarily for:

- Device Manufacturers who wish to embed a Secure Element into their solution.
- OS developers who wish to provide support for "Next Gen" APDU transport over various physical interfaces in their products.

It is assumed that the reader is familiar with the ISO/IEC 7816-3 T=1 smart card protocol.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit https://globalplatform.org/specifications/ip-disclaimers/. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
ISO/IEC 7812-1:2017	Identification cards – Identification of issuers – Part 1: Numbering system	[7812-1]
ISO/IEC 7816-3:2006	Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols	[7816-3]
ETSI TS 102 221	Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 17)	[102 221]

Table 1-2: Informative References

Standard / Specification	Description	Ref
Motorola SPI Block Guide	SPI Block Guide v03.06, Motorola Inc. 04 February 2003	[SPI]
NXP I^{2}C manual	UM10204I2C-bus specification and user manual	[I2C]
I3C Basic	Specification for I3C Basic v1.1.1, MIPI Alliance	[I3C]
MIPI I3C DCR Table	MIPI I3C Device Characteristics Register https://www.mipi.org/mipi_i3c_device_characteristics_register	[DCR]
MIPI I3C MID	MIPI Alliance Manufacturer ID Page https://mid.mipi.org	[MID]
BSI-CC-PP-0084	Common Criteria Protection Profile Security IC Platform Protection Profile with Augmentation Packages	[PP-0084]
ISO/IEC 7816-4:2020	Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange	[7816-4]
ISO/IEC 13239	Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures	[ISO 13239]

1.4 Terminology and Definitions

Common terms and definitions are listed in Table 1-3.

For additional terminology specific to SPI, see Table 1-4.

For additional terminology specific to I^{2}C, see Table 1-5.

For additional terminology specific to I3C, see Table 1-6.

For additional terminology specific to ISO/IEC 7816, see Table 1-7.

Table 1-3: Common – Terminology and Definitions

Term	Meaning
Assertion	Act of setting a signal from its inactive state to its active state.
Block	Smallest data unit that can be exchanged by the Data Link Layer. Used to convey application data and/or transmission control data.
Block Waiting Time (BWT)	Maximum delay between the last character of the command block received by the TARGET and the first character of the next response block transmitted by the TARGET. It represents the maximum time the TARGET may take to send its response. It is used to detect cases where the TARGET does not respond or takes too long to respond. The TARGET shall send a Waiting Time Extension (WTX) signal if it wishes more time to process a command and build the corresponding response.
Communication Interface Parameters (CIP)	String of bytes returned by the TARGET providing parameter values that the CTLR shall use to align with the TARGET's protocol and communication capabilities.

Term	Meaning
CTLR	Controller device that initiates and actively controls the communication with one or multiple TARGET(s).
Cyclic Redundancy Check (CRC)	2-byte block error detection code (see [ISO 13239] for more information).
Data Link Layer	Protocol layer that manages the reliable point-to-point transfer of data over a physical interface. It provides data flow control and error correction. It ensures that the incoming data is neither missing nor corrupted nor received in the incorrect order.
De-assertion	Act of setting a signal from its active state to its inactive state
Default Maximum Clock Frequency (DMCF)	Maximum clock frequency that shall be used by the CTLR when the CIP hasn't been received yet.
Epilogue Field	Last part of a Data Link Layer block, containing an error detection code computed over preceding block parts.
Information Block (I-Block)	Used to convey information for use by the application layer.
Information Field	Second part of a Data Link Layer block, containing application information for an I-Block or non-application information for an S-Block.
Information Field Size of the CTLR (IFSD)	Maximum size of the Information field of blocks that can be received by the CTLR (or sent by TARGET); above this limit, chaining shall be used.
Information Field Size of the TARGET (IFSC)	Maximum size of the Information field of blocks that can be received by the TARGET (or sent by the CTLR); above this limit, chaining shall be used.
Node Address Byte (NAD)	Byte indicating the source and the destination of a Data Link Layer block.
Polling Time (POT)	Time interval between two polling requests made by the CTLR. This time interval shall be chosen by the CTLR based on the performance of the TARGET. The chosen value shall not be lower than the Minimum Polling Time (MPOT) communicated by the TARGET in the CIP.
Power Saving Timeout (PST)	Time after which the TARGET may enter Power Saving Mode (if the TARGET implements the optional Power Saving Policy described in this document).
Power Wake-Up Time (PWT)	Minimum time for which the CTLR shall wait after having powered on the TARGET (i.e. after the “VCC Valid” state has been reached) before initiating communications with the TARGET.
Prologue Field	First part of a Data Link Layer block, composed of three fields: NAD, PCB, and LEN.
Protocol Control Byte (PCB)	Byte indicating the type of Data Link Layer block and conveys transmission control information.
Receive-Ready Block (R-Block)	Used to convey a positive or negative acknowledgement.
Secure Element (SE)	A tamper-resistant secure hardware component that is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any form factor, such as embedded or integrated SE, SIM/UICC, smart card, smart microSD, etc.

Term	Meaning
Serial Clock Line (SCL)	Line that synchronizes the output of data bits from the CTLR to the sampling of bits by the TARGET. One bit of data is transferred in each clock cycle.
Supervisory Block (S-Block)	Used to exchange control information between the CTLR and the TARGET.
Tamper-resistant secure hardware	Hardware designed to isolate and protect embedded software and data by implementing appropriate security measures. The hardware and embedded software meet the requirements of the latest Security IC Platform Protection Profile ([PP-0084]) including resistance to physical tampering scenarios described in that Protection Profile.
TARGET	Passive target device that communicates with a CTLR.

Common terms and definitions are listed in Table 1-3 above.

Additional terms and definitions relating to the SPI physical interface are listed in the following table.

Table 1-4: SPI – Terminology and Definitions

Term	Meaning
Clock Phase (CPHA)	Bit indicating when the sampling of data over the SPI CITO / COTI lines shall occur.
Clock Polarity (CPOL)	Bit indicating whether the clock shall be inverted or not.
Controller In / Target Out line (CITO line)	Line used by the TARGET to send data to the CTLR.
Controller Out / Target In line (COTI line)	Line used by the CTLR to send data to the TARGET.
Default Wake-Up Time (DWUT)	Wake-Up Time that shall be used by the CTLR when the CIP hasn't been received yet.
Filling Byte	Byte value '00' or 'FF' sent by the CTLR or TARGET as meaningless data, i.e. while meaningful data is conveyed on one line (COTI or CITO), meaningless data is conveyed on the other line.
Fragment	Piece of data exchanged during an SPI access (Length <= TAL).
Polling Byte	Byte value '00' or 'FF' sent by the CTLR for the purpose of polling the TARGET, to detect that the TARGET is ready either to receive or to send data.
Serial Peripheral Interface (SPI)	Widespread 4(+)-wire physical serial interface allowing the connection of ICs.
SPI Access	Transfer of data over the COTI / CITO line, triggered by the CTLR, consisting of TS line assertion, data transfer, and TS line de-assertion.
SPI Interrupt line (SPI-IRQ)	Line asserted by the TARGET to inform the CTLR that a response is ready to be sent.

Term	Meaning
Target Access Length (TAL)	2-byte length of the data that can be handled by the TARGET in one single SPI controller access. It is required by the CTLR for data flow control purposes when sending data to and receiving data from the TARGET.
Target Guard Time (TGT)	Time for which the CTLR shall wait between two SPI accesses.
Target Select (TS)	Line used by the CTLR to select the TARGET it wishes to exchange data with.
Wake-Up Time (WUT)	Time taken by the TARGET to leave Power Saving Mode and get ready to receive data.

Common terms and definitions are listed in Table 1-3 above.

Additional terms and definitions relating to the I^{2}C physical interface are listed in the following table.

Table 1-5: I^{2}C – Terminology and Definitions

Term	Meaning
Idle Byte	Byte value 'FF' that may be sent by the TARGET to indicate that it is currently busy or that no more data is available to be sent.
Inter Integrated Circuit bus (I^{2}C)	Widespread bi-directional 2-wire physical serial interface allowing the connection of ICs.
R/W Guard Time (RWGT)	Time for which the CTLR shall wait before initiating an I^{2}C write operation after an I^{2}C read operation, and vice versa. **Note:** RWGT does not apply between two read operations.
Serial Data Line (SDA)	I^{2}C data line allowing data to be transferred in both directions between a CTLR and a TARGET.

Common terms and definitions are listed in Table 1-3 above.

Additional terms and definitions relating to the I3C physical interface are listed in the following table.

Table 1-6: I3C – Terminology and Definitions

Term	Meaning
Frame	An I3C frame consists of a START condition (S), followed by one or more transfers, and a STOP condition (P).
Improved Inter Integrated Circuit bus (I3C)	The I3C interface is intended to improve upon the features of the I^{2}C interface, preserving backward compatibility.
In-Band Interrupt	A method whereby a TARGET emits its Address into the arbitrated Address header on the I3C Bus to notify the CTLR of an interrupt.
Message	An I3C message consists of a START condition (S) or repeated START condition (Sr), followed by one or more transfers. An I3C message ends at a STOP condition (P) or repeated START condition (Sr).
R/W Guard Time (RWGT)	See Table 1-5.
Serial Data Line (SDA)	See Table 1-5.

Common terms and definitions are listed in Table 1-3 above.

Additional terms and definitions relating to ISO/IEC 7816 are listed in the following table.

Table 1-7: ISO/IEC 7816 – Terminology and Definitions

Term	Meaning
Answer To Reset (ATR)	Data structure conveying information about the communication parameters proposed by the SE together with the SE's nature and state.

1.5 Abbreviations and Notations

Table 1-8: Abbreviations & Notations

Abbreviation	Context	Meaning
ACK	I^2C	Acknowledge
APDU		Application Protocol Data Unit
ATR	ISO/IEC 7816	Answer To Reset
BCR	I3C	Bus Characteristics Register
BGT	ISO/IEC 7816	Block Guard Time
BWI	ISO/IEC 7816	Block Waiting Time Integer
BWT		Block Waiting Time
CGT	ISO/IEC 7816	Character Guard Time
CIP		Communication Interface Parameters
CITO	SPI	Controller In / Target Out
CLK		Clock line through which CTLR provides the clock signal to TARGET
COTI	SPI	Controller Out / Target In
CPHA	SPI	Clock Phase
CPOL	SPI	Clock Polarity
CRC		Cyclic Redundancy Check
CTLR		Controller Device
CWI	ISO/IEC 7816	Character Waiting Time Integer
CWT	ISO/IEC 7816	Character Waiting Time
D	ISO/IEC 7816	Baud Rate Adjustment Integer
DAD		Destination Address
DBWT		Default Block Waiting Time
DMCF		Default Maximum Clock Frequency
DMPOT		Default Minimum Polling Time
DMRL	I3C	Default Maximum Read Length
DMWL	I3C	Default Maximum Write Length
DPWT		Default Power Wake-Up Time
DRWGT	I^2C	Default R/W Guard Time
DTAL	SPI	Default Target Access Length
DTGT		Default TARGET Guard Time
DWUT	SPI	Default Wake-Up Time
EDC		Error Detection Code

Abbreviation	Context	Meaning
etu	ISO/IEC 7816	Elementary Time Unit
F	ISO/IEC 7816	Clock Rate Conversion Integer
f	ISO/IEC 7816	Frequency value of clock signal provided to the TARGET by the CTLR
FM	I^{2}C	Fast Mode
GT	ISO/IEC 7816	Guard Time
I^{2}C	I^{2}C	Inter Integrated Circuit bus
I3C	I3C	Improved Inter Integrated Circuit bus
IBI	I3C	In-Band Interrupt
I-Block		Information Block
IFS		Information Field Size
IFSC		Information Field Size of the TARGET
IFSD		Information Field Size of the CTLR
IRQ		Interrupt Request
LEN		Length field of a Data Link Layer block
LSB		Least Significant Byte
lsb		Least Significant Bit
MCF		Maximum Clock Frequency
MDB	I3C	Mandatory Data Byte
MPOT		Minimum Polling Time
MRL	I3C	Maximum Read Length
MSB		Most Significant Byte
msb		Most Significant Bit
MWL	I3C	Maximum Write Length
NACK	I^{2}C	Not Acknowledge
NAD		Node Address Byte
P	I3C	Stop Condition
PCB		Protocol Control Byte
POT		Polling Time
PST		Power Saving Timeout
PWT		Power Wake-Up Time
R/W	I^{2}C	Read/Write
R-Block		Receive-Ready Block
RWGT	I^{2}C	R/W Guard Time
S	I3C	Start Condition

Abbreviation	Context	Meaning
SAD		Source Address
S-Block		Supervisory Block
SCL		Serial Clock Line (a.k.a. SCKL or SCLK)
SDA	I^2C	Serial Data Line
SDR	I3C	Single Data Rate
SE		Secure Element
SPI	SPI	Serial Peripheral Interface
SPI-IRQ	SPI	SPI Interrupt line
Sr	I3C	Repeated Start Condition
T	I3C	Transition Bit
TAL	SPI	Target Access Length
TARGET		Target Device
T-bit	I3C	Transition Bit
TGT	SPI	Target Guard Time
TS	SPI	Target Select line
WTX		Waiting Time Extension
WUT	SPI	Wake-Up Time

1.6 Revision History

GlobalPlatform technical documents numbered *n*.0 are major releases. Those numbered *n*.1, *n*.2, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n*.1, *n.n*.2, etc., are maintenance releases that incorporate errata and clarifications; all non-trivial changes are indicated, often with revision marks.

Table 1-9: Revision History

Date	Version	Description
Jan 2020	1.0	Public Release as *APDU Transport over SPI / I2C*
Jul 2023	1.0.0.9	Committee Review
Nov 2024	1.0.0.27	Member Review • Support for ISO/IEC 7816 and I3C physical interfaces is added. • For SPI, support for TAL='0000' is added to allow the TARGET to indicate that it does not support fragmented SPI access. • DTAL is changed from 16 to 32 to allow readout of the CIP without fragmentation of the SPI access. • Default parameter values for SPI and I^2C timing parameters are updated. • Restrictions about I^2C repeated start conditions are removed. • Explanations about the Node Address Byte were refined and extended. • Optimizations for production environments are provided in an informative annex. • Clarifications for the Activation Sequence (SPI/I^2C) explain that Default Parameter Values are only expected to be used in order to retrieve the CIP from the TARGET, if better parameter values are not already known by the CTLR. • New terminology is introduced to use the terms “Controller” (CTLR) and “Target” (TARGET). The term “Hosting Device” (HD) is replaced by CTLR and SE by TARGET. Related terms are updated accordingly: SEAL, SEGT, MOSI, MISO => TAL, TGT, COTI, CITO.
Apr 2025	v1.0.0.34	Public Review • Added Terminology and Definitions for I3C. • Added Abbreviations and Notations for I3C. • Introduced DMRL/DMWL. • Added to section 3.4.3 an explanation of how CTLRs can identify TARGETs on the I3C bus that support the T=1' protocol.
TBD	1.1	Public Release as *Next Gen APDU Transport*

2 OVERVIEW

This document specifies how to transport APDUs between a Controller Device (CTLR) and a Target Device (TARGET) using serial physical interfaces based on [SPI], [I2C], [7816-3], or [I3C], which are very commonly used in the industry for connecting electronic components.

Section 3 describes the Physical Layer that shall be implemented to access the physical interface.

Section 4 describes the Data Link Layer (implemented over the Physical Layer) that shall be used to transport APDU commands and responses.

Section 5 describes the conditions under which the TARGET may enter Power Saving Mode.

3 PHYSICAL INTERFACES

3.1 SPI Interface

3.1.1 Description

The Serial Peripheral Interface (SPI) described in [SPI] is a synchronous Serial Data Link that offers full-duplex communication. In this specification however, the SPI interface is only used for half-duplex communication where the CTLR and TARGET send data alternately.

Although multiple TARGETs may be present, each one using its own individual Target Select line (TS), this specification only describes the communication between one single CTLR and one single TARGET.

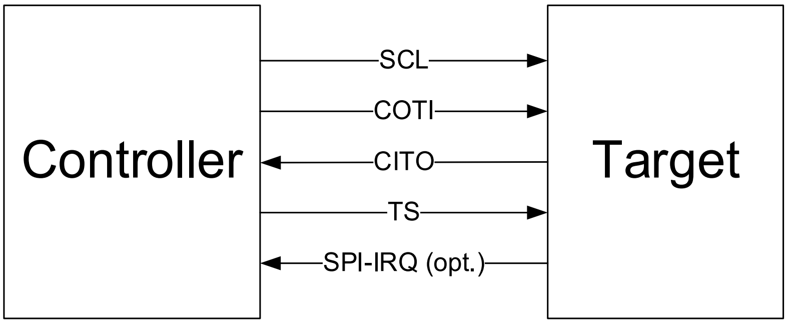
3.1.2 Physical Layer

The SPI bus specifies four mandatory physical signals/lines:

SCL line:	Serial Clock (output from CTLR)
COTI line:	Controller Out / Target In (output from CTLR)
CITO line:	Controller In / Target Out (output from TARGET)
TS line:	Target Select (active low, output from CTLR)

An optional SPI-IRQ physical line may be used.

Figure 3-1: SPI – Simplified Schematics



When present, the SPI-IRQ line may be used by the TARGET to notify the CTLR that it is ready to send data, which is needed because only the CTLR may initiate the communication. If the SPI-IRQ line is not available, the CTLR may instead poll the TARGET for incoming data. See section 3.1.5 for more details.

3.1.2.1 Signal Conventions

The SPI communication shall use the “mode 0” configuration as described below:

- The SPI Clock Polarity bit (CPOL) shall be 0 (non-inverted clock), meaning that the idle state of the clock is low and that trigger is initiated at a rising clock signal (Active-high clocks selected).
- The SPI Clock Phase bit (CPHA) shall be 0, meaning that the sampling of data occurs at a rising clock signal of the SCL signal. The data signals are set at chip selection and falling clock signals.
- The SCL frequency shall not exceed the Maximum Clock Frequency (MCF) defined by the Communication Interface Parameters (CIP – see section 4.3). If the CTLR doesn’t know which MCF to use (e.g. CIP not retrieved yet), the Default Maximum Clock Frequency (DMCF) defined in section 3.1.7 shall be used.
- The number of bits transmitted via COTI or CITO signal during a single SPI access shall be a multiple of eight.
- The Most Significant Bit (msb) shall be sent first.

3.1.2.2 Transmission of Data

Only the CTLR may initiate the transmission of data and it shall select the TARGET before it can exchange data with it, i.e. the CTLR shall pull down the TS line and provide a proper clock signal on the SCL line.

When the CTLR needs to send data to the TARGET, it shall provide it on the COTI line and **may** ignore the data received on the CITO line. Conversely, when the CTLR needs to receive data from the TARGET, it shall provide Filling Bytes on the COTI line and read the data received on the CITO line.

When the TARGET needs to send data to the CTLR, it shall provide it on the CITO line and **may** ignore the data received on the COTI line. Conversely, when the TARGET needs to receive data from the CTLR, it shall provide Filling Bytes on the CITO line and read the data received on the COTI line.

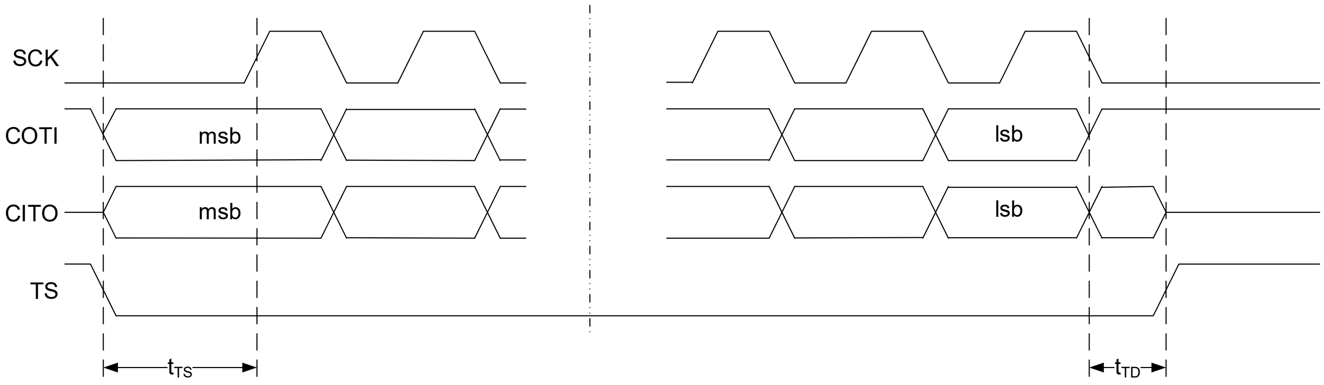
The CTLR and TARGET shall use the same pre-agreed Filling Byte value (i.e. either '00' or 'FF').

Once all data have been exchanged as expected, the CTLR shall stop the clock signal and de-select the TARGET.

The rules above are illustrated in Figure 3-2 where:

- "msb" shows the position of the most significant bit of the first byte of the transmitted data.
- "lsb" shows the position of the least significant bit of the last byte.
- "t_{TS}" is the minimum time for which the CTLR shall wait after the assertion of the TS line before starting the clock signal and transmitting the first bit of data. Its value remains out of scope of this specification.
- "t_{TD}" is the minimum time for which the CTLR shall wait after the transmission of the last bit of data before de-asserting the TS line (i.e. deselecting the TARGET). Its value remains out of scope of this specification.

Figure 3-2: SPI – Data Transmission

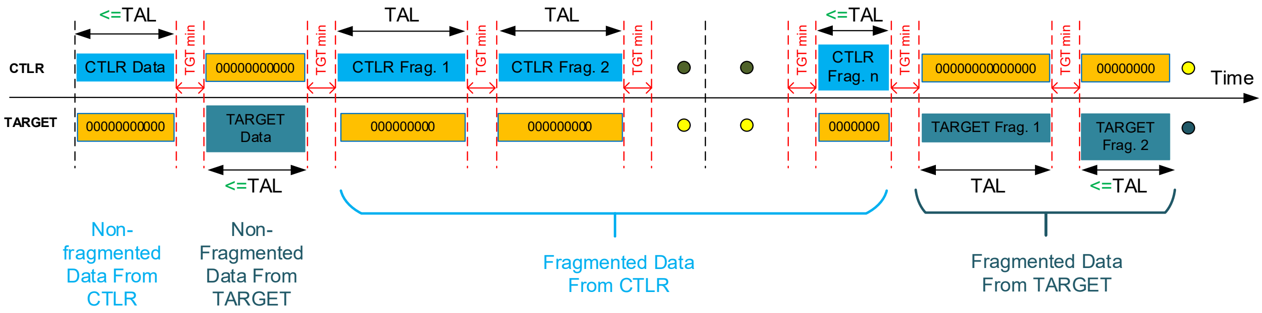


3.1.2.3 Data Fragmentation / SPI Fragments

The SPI bus is used to convey Data Link Layer blocks for which a data flow control is defined (see section 4). However, a first level of data flow control is implemented at the Physical Layer through the exchange of so-called SPI fragments. A block of data may be split in multiple SPI fragments. The fragmentation of data will depend on the size of the data that needs to be exchanged and the Target Access Length (TAL).

When the CTLR needs to transfer data to or from the TARGET and the length of such data exceeds TAL bytes, the CTLR shall fragment and exchange data so that the number of bytes conveyed during each SPI access does not exceed a maximum of TAL bytes (in each direction). The CTLR should maximize the number of bytes transferred per SPI access to minimize the number of SPI accesses. In addition, the CTLR shall pause for a duration of Target Guard Time (TGT) between two consecutive SPI accesses. This process is illustrated in Figure 3-3.

Figure 3-3: SPI – Physical-Layer Fragmentation with Respect to TAL Size



TARGETs may support this mechanism of SPI fragmentation. A TARGET indicates the level of support for SPI fragmentation in the CIP (see section 4.3.3).

3.1.2.4 Half Duplex Usage

Although the SPI bus allows full-duplex mode operation, this specification does not use such capabilities and the meaningful information is only communicated by the Data Link Layer in half-duplex mode (see section 4), meaning that CTLR and TARGET are only expected to send Data Link Layer blocks alternately.

3.1.3 Activation Sequence

After having powered on the TARGET, the CTLR shall wait for the duration of Power Wake-Up Time (PWT) before initiating any communication with the TARGET. Also, before attempting to send data to the TARGET, the CTLR shall ensure that the TARGET is ready to receive data, following the procedure described in section 3.1.4.

Once the TARGET is ready to receive data, the CTLR may retrieve the CIP (see section 4.3). If the CIP has never been retrieved and the CTLR is not aware of the communication parameter values that may be used, the CTLR shall use the default values (e.g. Default PWT, Default TAL, etc.) defined in section 3.1.7 in order to retrieve the CIP. Otherwise, it may use the parameter values already known (i.e. obtained in a proprietary way) or previously read from the CIP.

The CTLR shall adapt its behavior according to the parameters specified by the CIP.

3.1.4 Detecting TARGET Ready to Receive Data

The TARGET may decide to enter Power Saving Mode in order to save battery, in which case it would not be able to receive data. The conditions under which a TARGET implementation may enter Power Saving Mode are described in section 5.

When the CTLR wishes to send data and assumes that the TARGET has entered Power Saving Mode, it shall first make sure the TARGET is ready to receive data. To do so, the CTLR shall apply a so-called wake-up procedure.

Two wake-up procedures are described hereafter; however, this specification acknowledges the fact that it may not be possible to implement these procedures in some environments. Therefore, proprietary wake-up procedures (known to both CTLR and TARGET) are permitted.

- Wake-Up Procedure 1 (a.k.a. TS-WUT-SCL):

  The CTLR shall assert the TS line and wait for the duration of WUT (or DWUT) before applying the clock signal (SCL) and sending data.

  In this procedure, the TS line is used as an interrupt line to wake up the TARGET and waiting WUT provides the TARGET with enough time to wake up and get ready to receive data. For best performance, the CTLR should start sending data immediately after WUT. However, it may safely wait longer; keeping the TS line asserted prevents the TARGET from going back to Power Saving Mode.

- Wake-Up Procedure 2 (a.k.a. PB-WUT):

  The CTLR shall send one Polling Byte (using the procedure described in section 3.1.2.2, i.e. which ends by de-asserting the TS line) and then wait for the duration of WUT (or DWUT) before sending any data. When the TARGET detects that it is deselected for the first time since wake up, it shall discard any data previously received on the COTI line.

  In this procedure, waiting for the duration of WUT provides the TARGET with enough time to wake up and get ready to receive data. However, to prevent the TARGET going back to Power Saving Mode (see section 5), the CTLR shall not wait longer than PST (if PST is a valid timeout value).

  In addition, when the TARGET expects a new Data Link Layer block (see section 4) and instead receives a Polling Byte, the TARGET shall simply discard this Polling Byte and wait for further incoming data. This behavior is required to handle the case where the CTLR would incorrectly assess the TARGET as being in Power Saving Mode and unnecessarily apply the wake-up procedure.

In support of the above procedures, a Wake-Up Time (WUT) is defined as part of the CIP (see section 4.3.3) and a Default WUT (DWUT) is defined in section 3.1.7. The WUT found in the CIP may be ignored or used with another meaning if a proprietary wake-up procedure is implemented.

3.1.5 Detecting TARGET Ready to Send Data

To detect that the TARGET is ready to send data and initiate the retrieval of such data, the CTLR Physical Layer shall use one of the mechanisms described in the following sections. As such mechanisms correspond to different hardware architectures, the choice of using one or the other is implicit (i.e. the CTLR implicitly knows which one to use).

3.1.5.1 Polling Mechanism

When the CTLR and TARGET are designed to use the polling mechanism, the CTLR shall poll the TARGET for available data. To do so, it shall first decide a Polling Time (POT) that shall be greater than the MPOT communicated by the CIP. Then, when expecting some response data, the CTLR shall poll the TARGET as follows:

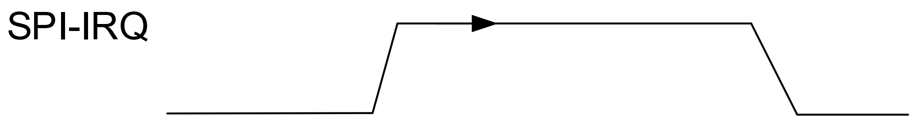
- The CTLR shall assert the TS line, apply the clock on the SCL line, and send one Polling Byte to try receive a first meaningful byte from the TARGET (i.e. valid first byte of a Data Link Layer block).
- If a Polling Byte is received from the TARGET, the CTLR shall de-assert the TS line, wait for the duration of POT, and then try to send a Polling Byte again. The CTLR shall repeat this procedure until it receives a meaningful byte from the TARGET (see below) or until the CTLR’s Data Link Layer determines that a timeout has occurred.

  Note: In this procedure, the CTLR and TARGET shall use the same Polling Byte value (either '00' or 'FF').
- If a meaningful byte is received from the TARGET, the CTLR may carry on receiving remaining block data immediately or may de-assert the TS line and then apply the procedure described in section 3.1.2.2 to receive remaining block data.

3.1.5.2 Interrupt Mechanism

When the CTLR and TARGET are designed to use the interrupt mechanism, the dedicated SPI-IRQ line shall be asserted by the TARGET when response data is available. A Level-Sensitive mechanism shall be implemented where the interrupt shall be triggered by setting the SPI-IRQ line to an active high voltage level. The TARGET shall clear the interrupt as soon as the TS line is asserted by the CTLR.

Figure 3-4: SPI – Level-Sensitive Interrupt Mechanism



To prevent communication errors:

- The TARGET shall only assert the SPI-IRQ line when consistent data are actually ready for sending, that is, when TAL bytes of meaningful data or the end of or a complete Data Link Layer block shorter than TAL bytes is ready for sending.
- The CTLR shall not try to send new command data if the SPI-IRQ line is asserted.

3.1.6 Receiving Data from TARGET

Because receiving data from the TARGET can only be initiated and driven by the CTLR, the CTLR needs to know the size of data that shall be retrieved from the TARGET. This problem is solved by the fact that, when the CTLR detects that the TARGET is ready to send data (see section 3.1.5), the CTLR is then expected to receive a Data Link Layer block (see section 4) from the TARGET and from the prologue field of that block, the CTLR may learn how much data shall be received.

Note: When the polling mechanism described in section 3.1.5.1 is used to detect that the TARGET is ready to send data, the first valid byte returned by the TARGET (i.e. different from '00' and 'FF') indicates the end of the polling procedure and is the first byte of the Data Link Layer block the TARGET intends to send. When the interrupt mechanism is used, the CTLR has not received any byte yet and shall retrieve the entire Data Link Layer block.

Note: Data transfer and communication performance may be optimized by having the CTLR always immediately retrieve not just the prologue field of a Data Link Layer block but rather a common short block size (e.g. 6 bytes). If the CTLR tries to retrieve more data than is made available by the TARGET, the CTLR should only receive additional Filling Bytes (common behavior in SPI implementations), and if the CTLR received an incomplete block it may retrieve the missing data using additional SPI accesses.

3.1.7 Default Parameter Values

The following table defines SPI parameter values that shall be used by default.

Table 3-1: SPI – Default Parameter Values

Parameter	Description	Unit	Value
DPWT	Default Power Wake-Up Time	ms	25
DMCF	Default Maximum Clock Frequency	kHz	1000
DMPOT	Default Minimum Polling Time	µs	1000
DTGT	Default Target Guard Time	µs	200
DWUT	Default Wake-Up Time	µs	4000
DTAL	Default TAL	byte	32

The CTLR shall instead use the parameter values specified by the CIP (see section 4.3) once the CIP has been retrieved from the TARGET or if the CTLR already knows such values.

3.2 I²C Interface

3.2.1 Description

The Inter Integrated Circuit (I²C) bus described in [I2C] allows establishing half-duplex communications between one or several CTLR(s) and one or several TARGET(s). Although multiple controllers may be present, this specification only describes communications involving a single CTLR.

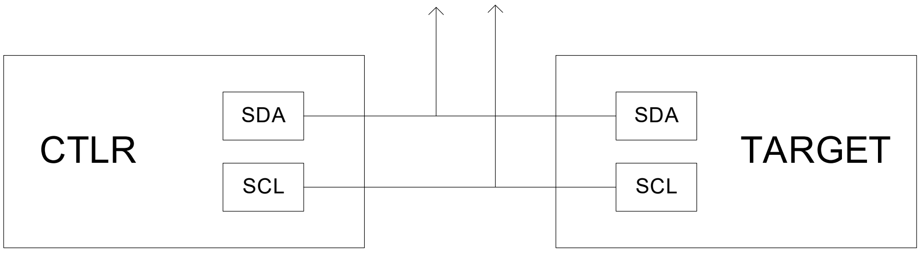
3.2.2 Physical Layer

The I²C bus comprises two signal lines:

- Serial Clock Line (SCL)
- Serial Data Line (SDA)

An optional I²C-IRQ physical line may be used.

Figure 3-5: I²C – Simplified Schematics



Only the following options of I²C are used:

- Support of 7-bit Addressing only
- Single-Controller / Multi-Target configuration
- Maximum Clock Frequency (specified in CIP; see section 4.3.4)
    - 400 kHz for Fast Mode
    - 1000 kHz for Fast Mode Plus
    - 3400 kHz for HS Mode

If the TARGET supports Clock Stretching, then the CTLR shall support it.

When present, the I²C-IRQ line may be used by the TARGET to notify the CTLR that it is ready to send data, which is needed because only the CTLR may initiate the communication. If the I²C-IRQ line is not available, the CTLR may instead poll the TARGET for incoming data. See section 3.2.6 for more details.

3.2.3 Activation Sequence

After having powered on the TARGET, the CTLR shall wait for the duration of Power Wake-Up Time (PWT) before initiating any communication with the TARGET. Also, before attempting to send data to the TARGET, the CTLR shall ensure that the TARGET is ready to receive data following the procedure described in section 3.2.4.

Once the TARGET is ready to receive data, the CTLR may retrieve the CIP (see section 4.3). If the CIP has never been retrieved and the CTLR is not aware of the communication parameter values that may be used, the CTLR shall use the default values (e.g. Default PWT) defined in section 3.2.8 in order to retrieve the CIP. Otherwise, it may use parameter values already known (i.e. obtained in a proprietary way) or previously read from the CIP.

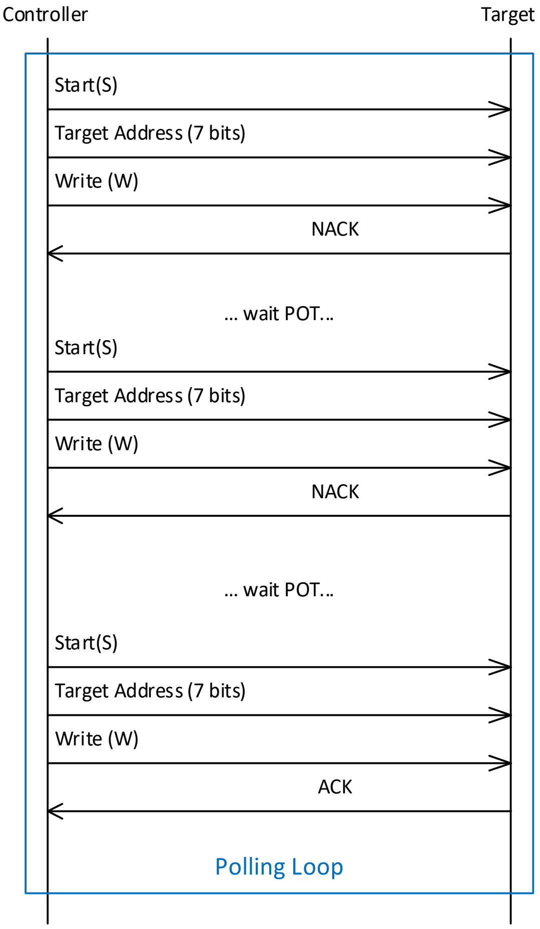
The CTLR shall adapt its behavior according to the parameters specified by the CIP.

3.2.4 Detecting TARGET Ready to Receive Data

The TARGET may decide to enter Power Saving Mode in order to save battery, in which case it would not be able to receive data. The conditions under which a TARGET implementation may enter such a Power Saving Mode are described in section 5.

When the CTLR wishes to send data and assumes that the TARGET has entered Power Saving Mode, it shall first make sure the TARGET is ready to receive data. To do so, the CTLR shall poll the TARGET by sending an I^{2}C write request (i.e. start condition + 7-bit address + 1-bit write request) to the TARGET at a period of time defined by POT, (see Figure 3-6). The TARGET shall reject the I^{2}C write request by sending a NACK if it is not ready to receive data from the CTLR. The polling time (POT) used by the CTLR shall be greater than the MPOT communicated by the CIP.

Figure 3-6: I^{2}C – CTLR Detecting TARGET Ready to Receive Data



3.2.5 Sending Data to TARGET

When the TARGET is in RECEIVING state, it is idle and waiting for a Data Link Layer block from the CTLR. In RECEIVING state, the TARGET shall:

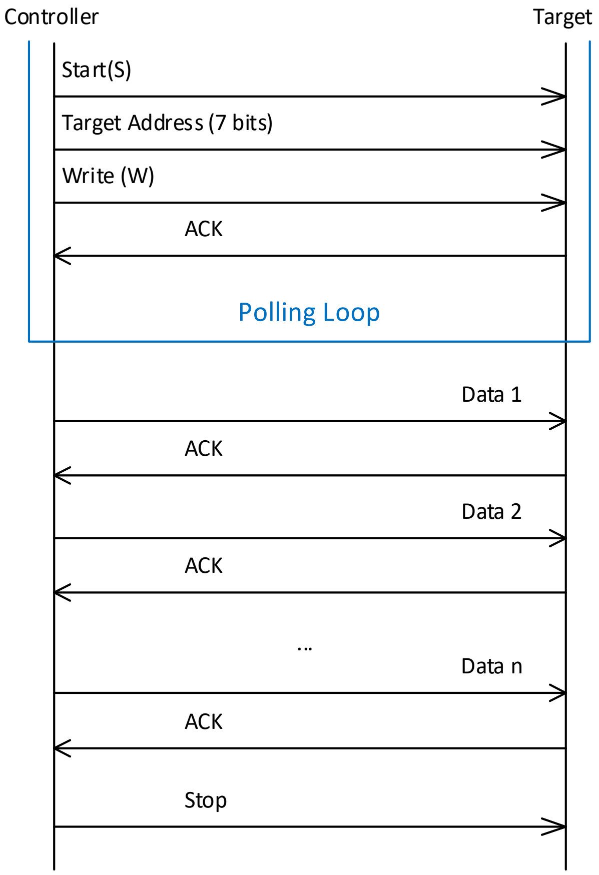
- Acknowledge (ACK) any I²C write request from CTLR (matching the I²C address of the TARGET)

The CTLR shall follow the sequence below to send an I²C message to the TARGET:

1) Send I²C start condition
2) Send the I²C address of the TARGET with the R/W bit low (Write to TARGET)
3) Send data (i.e. Data Link Layer block)
4) Send I²C stop condition

This is illustrated in Figure 3-7. The CTLR shall send a complete Data Link Layer block in one I²C message; however, it may abort the message transmission anytime by sending an I²C stop condition. The CTLR shall wait for the duration of RWGT (Read Write Guard Time) before initiating any new I²C read request.

Figure 3-7: I²C – CTLR Sends Data to TARGET



3.2.6 Detecting TARGET Ready to Send Data

When the CTLR has finished sending an I^2C message (i.e. the TARGET has received the I^2C stop condition), the TARGET shall switch from RECEIVING state to PROCESSING state. In PROCESSING state, the TARGET is busy processing the command sent by the CTLR and shall:

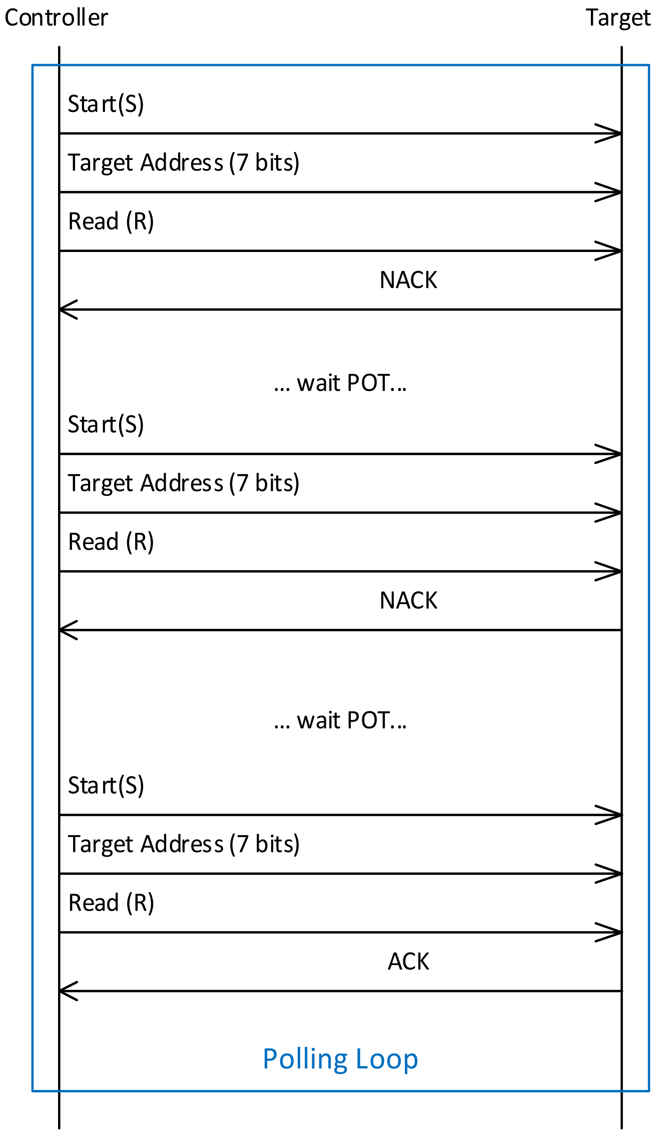
- Reject (NACK) any I^2C write request from CTLR
- Reject (NACK) any I^2C read request from CTLR

To detect that the TARGET is ready to send data and initiate the retrieval of such data, the CTLR's Physical Layer shall use one of the mechanisms described in the following sections. As such mechanisms correspond to different hardware architectures, the choice of using one or the other is implicit (i.e. the CTLR implicitly knows which one to use).

3.2.6.1 Polling Mechanism

The CTLR shall periodically poll the TARGET for response data by sending an I^{2}C read request (i.e. start condition + 7-bit address + 1-bit read request) to the TARGET (see Figure 3-8) and shall retry later (after a duration of POT) if the TARGET rejects (NACK) the I^{2}C read request (to indicate it is busy). The polling time (POT) used by the CTLR shall be greater than the MPOT communicated by the CIP.

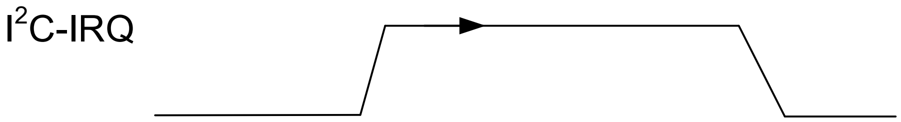
Figure 3-8: I^{2}C – CTLR Polling TARGET for Response Data



3.2.6.2 Interrupt Mechanism

When the CTLR and TARGET are designed to use the interrupt mechanism, the dedicated I²C-IRQ line shall be asserted by the TARGET when response data is available, i.e. when switching to the SENDING state (see section 3.2.7). A Level-Sensitive mechanism shall be implemented where the interrupt shall be triggered by setting the I²C-IRQ line to an active high voltage level. After switching to SENDING state, the TARGET shall clear the interrupt as soon as an I²C read request is received from the CTLR.

Figure 3-9: I²C – Level-Sensitive Interrupt Mechanism



To prevent communication errors the CTLR shall not try to send any new I²C write request (for the same I²C address) as long as the I²C-IRQ line is asserted.

3.2.7 Receiving Data from TARGET

When the TARGET has finished processing the Data Link Layer command block sent by the CTLR and it is ready to send a Data Link Layer response block, the TARGET shall switch from PROCESSING to SENDING state. In SENDING state, the TARGET shall:

- Acknowledge (ACK) any I²C read request from the CTLR (matching the I²C address of the TARGET)

The CTLR shall follow the sequence below to receive an I²C message from the TARGET:

1) Send I²C start condition
2) Send the I²C address of the TARGET with the R/W bit high (Read from TARGET)
3) Receive data
4) Send I²C stop condition

The CTLR may read the response bytes using a single I²C message or multiple I²C messages. This is illustrated in Figure 3-10 and Figure 3-11. If the data is received using multiple I²C messages, the CTLR may have to apply the polling procedure again if the TARGET rejects (NACK) an I²C read request. The CTLR shall wait for the duration of RWGT (Read Write Guard Time) before initiating any new I²C write requests.

The TARGET shall remain in SENDING state until all response bytes have been read by the CTLR or until the CTLR sends a new I²C write request (see section 3.2.5). As the CTLR may safely expect to receive a Data Link Layer block (see section 4) from the TARGET, the CTLR may determine from the prologue field of that block how much data shall be received. If the CTLR attempts to read more data than was made available by the TARGET, the TARGET shall answer with Idle Bytes (see Table 1-5) to indicate it has no more data to send.

Figure 3-10: I²C – CTLR Receives Data from TARGET using a Single I²C Message

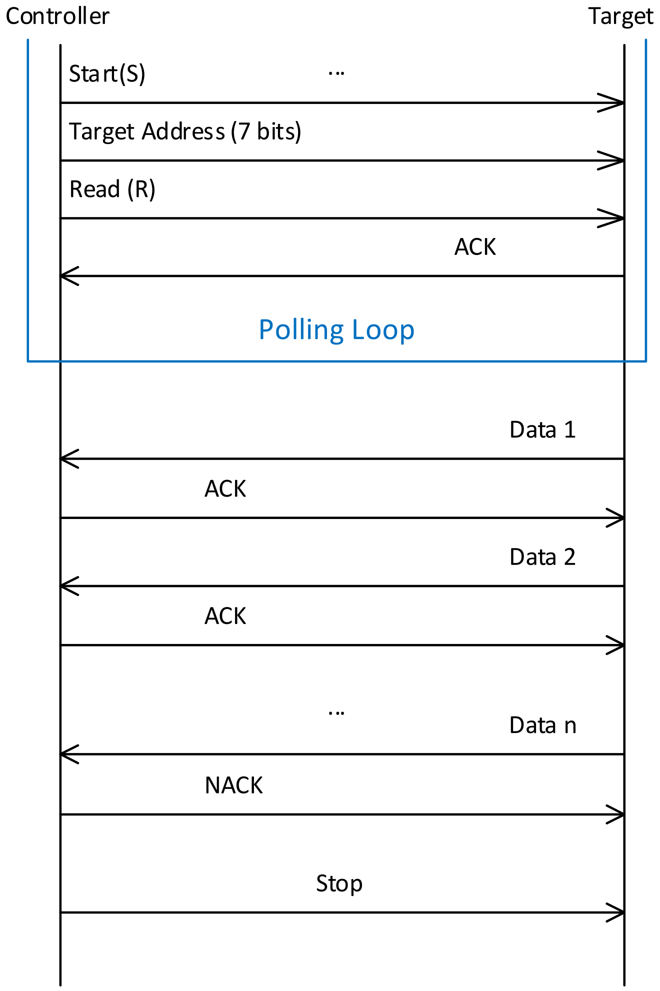
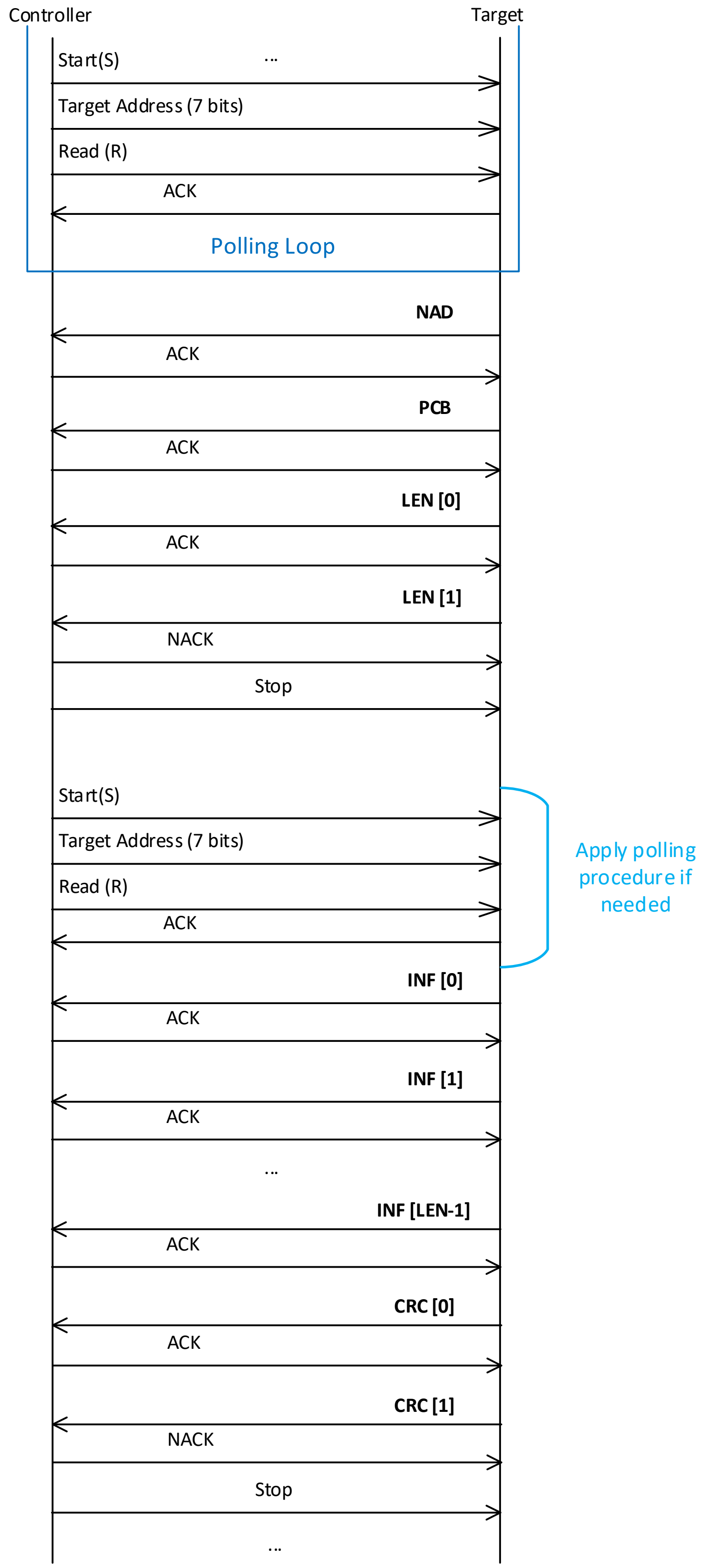


Figure 3-11: I²C – CTLR Receives Data from TARGET using Multiple I²C Messages



3.2.8 Default Parameter Values

The following table defines I²C parameter values that shall be used by default.

Table 3-2: I²C – Default Parameter Values

Parameter	Description	Unit	Value
DPWT	Default Power Wake-Up Time	ms	25
DMCF	Default Maximum Clock Frequency	kHz	400
DMPOT	Default Minimum Polling Time	µs	1000
DRWGT	Default R/W Guard Time	µs	300

Note: The CTLR shall instead use the parameter values (or ranges) specified by the CIP (see section 4.3) once the CIP has been retrieved from the TARGET.

3.3 ISO/IEC 7816 Interface

3.3.1 Description

The interface defined in ISO/IEC 7816 is an asynchronous Serial Data Link that offers half-duplex communication. The CTLR initiates the communication by sending a signal on the RESET pin; the TARGET responds by sending the ATR, a string of informative data for the CTLR to adjust communication parameters, if needed. The CTLR then sends data to the TARGET and keeps the interface active to wait for response data from the TARGET. The TARGET sends response data after processing the command.

The sections below provide a basic summary of the ISO/IEC 7816 physical interface when used in the context of T=1'. Please refer to [7816-3] for more information.

3.3.2 Physical Layer

The ISO/IEC 7816 interface comprises at least five physical lines:

- VCC: Supply power
- RST: Reset signal
- CLK: Clock signal
- GND: Ground (Reference voltage)
- I/O: Input/Output for serial data communication

The SPU line (Standard or Proprietary Use) is out of scope in this document.

Only the CTLR may initiate the transmission of data. It shall follow the Card operation procedure described in [7816-3].

3.3.3 Activation Sequence

3.3.3.1 Activation and Cold Reset

The activation and cold reset processes are described in [7816-3] section 6.2.1. The CTLR receives the ATR from the TARGET that contains supported transmission parameters and Data Link Layer protocols.

In contrast to SPI/I^{2}C physical layers, there is no need to retrieve the CIP (see section 4.3) as all communication parameters are available in the ATR.

3.3.3.2 Warm Reset

The warm reset process is described in [7816-3] section 6.2.3.

Its purpose is to allow the CTLR to select different communication and protocol parameters than the ones defined in the initial ATR at any time after the cold reset has been performed.

3.3.3.3 Class Selection

The nominal supply voltage (class) shall be agreed upon during the class selection process described in sections 5.1.3 and 6.2.4 of [7816-3] and section 5.4 of [102 221].

The goal is to have the CTLR select a power voltage that is compatible with the TARGET.

3.3.3.4 Selection of Transmission Parameters and Protocol

All transmission parameters and protocol information are provided by the TARGET through the ATR mechanism that is defined in the ISO/IEC 7816 specification, sections 8 and 9.

Note: An additional value for the Type T in TD_i within the range [5-13] shall be defined for T=1' through an LS with ISO. The goal being to indicate to the CTLR that the T=1' protocol defined in section 4 is part of the protocols supported by the TARGET. This also allows the TARGET to specify parameters that are specific to this protocol.

3.3.4 Detecting TARGET Ready to Receive Data

Initiation of communication as defined in [7816-3] section 6 covers all the mechanisms needed to detect that the TARGET is ready to receive data.

3.3.5 Detecting TARGET Ready to Send Data

When the CTLR has finished sending a TPDU, the TARGET is busy processing the command sent by the CTLR and, if more time than BWT is required to build the response data, it sends a WTX S-Block to the CTLR. The CTLR silently waits until the response is sent by the TARGET or until the waiting time exceeds BWT and no WTX has been received.

In contrast to SPI/I^{2}C physical layers, neither a polling nor an interrupt mechanism is required.

3.3.6 Default Parameter Values

Default parameter values are defined in [7816-3]. Such default values allow the CTLR to set up the communication to retrieve the ATR information.

Those default values are typically extended by the parameters found in the ATR and if needed modified through the PPS mechanism where the CTLR proposes some alternate communication parameters.

3.4 I3C Interface

3.4.1 Description

The Improved Inter Integrated Circuit (I3C) bus described in [I3C] allows establishing half-duplex communications between one or several CTLR(s) and one or several TARGET(s). Although multiple controllers may be present, this specification describes communications involving a single CTLR and multiple TARGETS. Scenarios with multiple CTLRs are out of scope of this document.

A CTLR shall remain the Active Controller until it has received all expected response data from all managed TARGETs. TARGETs shall only send data in the context of answering a command received from the CTLR.

An I3C bus may mix I3C Targets and I^{2}C legacy Targets under the conditions described in section 3.4.9.

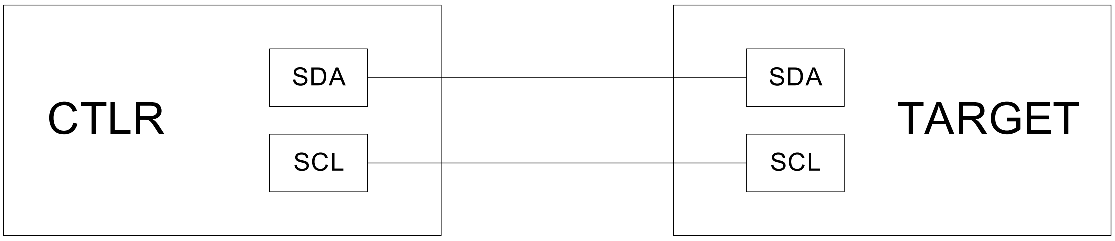
Note: There may be other Controllers and Targets present on the I3C bus, not compliant to this specification, possibly using a different or no link layer protocol for data transfers. This kind of deployment is out of scope.

3.4.2 Physical Layer

The I3C bus comprises two signal lines:

- Serial Clock Line (SCL)
- Serial Data Line (SDA)

Figure 3-12: I3C – Simplified Schematics



The following I3C options and mechanisms shall be used:

- SDR mode (Single Data Rate)

  This I3C mode supports specific built-in Broadcast Messages and Direct Messages, which are used to enable new features, in contrast to the I^{2}C protocol that only defines read and write transfers.

  - I3C private read or write transfers are used to convey Data Link Layer blocks, defined in this specification.
  - Built-in commands defined in [I3C] are used by the CTLR e.g. to discover the communication parameters of the TARGET and assign dynamic addresses to the I3C Targets during the I3C Initialization, described in [I3C].
- In-Band Interrupt requests

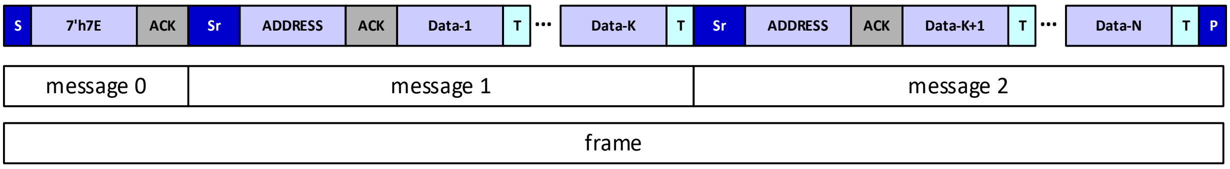
3.4.2.1 I3C concepts

In alignment with [I3C], any exchange on the I3C bus (i.e. between CTLR and TARGET(s)) is considered a “transfer”. Such transfers consist of 9-bit words grouped to “messages” and “frames”.

An I3C message consists of a START condition (S) or repeated START condition (Sr), followed by one or more transfers. An I3C message ends at a STOP condition (P) or repeated START condition (Sr).

An I3C frame consists of a START condition (S), followed by one or more transfers, and a STOP condition (P).

Figure 3-13: I3C – Data Transfers



3.4.3 Activation Sequence

The I3C bus initialization, as defined in [I3C], shall be completed before the CTLR starts any T=1' communication with the TARGET. Before attempting to send data to the TARGET, the CTLR shall ensure that the TARGET is ready to receive data following the procedure described in section 3.4.4.

TARGETs compliant to this specification shall have their DCR value set to 188 ('BC'). This value is allocated by MIPI for the "eSE" category (see [DCR]). The CTLR identifies TARGETs compliant to this specification using the Provisioned ID that can be retrieved using the GETPID CCC defined in [I3C]. The Provisioned ID shall use Vendor Fixed Values for bits 0 to 31. This is indicated by setting bit 32 of the Provisioned ID to ‘0’. It is assumed that values of the Provisioned ID of TARGETs compliant to this specification are known by the CTLR.

The TARGET transitions to RECEIVING state, when it is ready to receive data. At this stage, the CTLR may retrieve the CIP (see section 4.3). If the CTLR is not aware of the communication parameter values that may be used, the CTLR shall use the default values (e.g. Default MPOT) defined in section 3.4.8 in order to retrieve the CIP. Otherwise, it may use parameter values already known or previously read from the CIP.

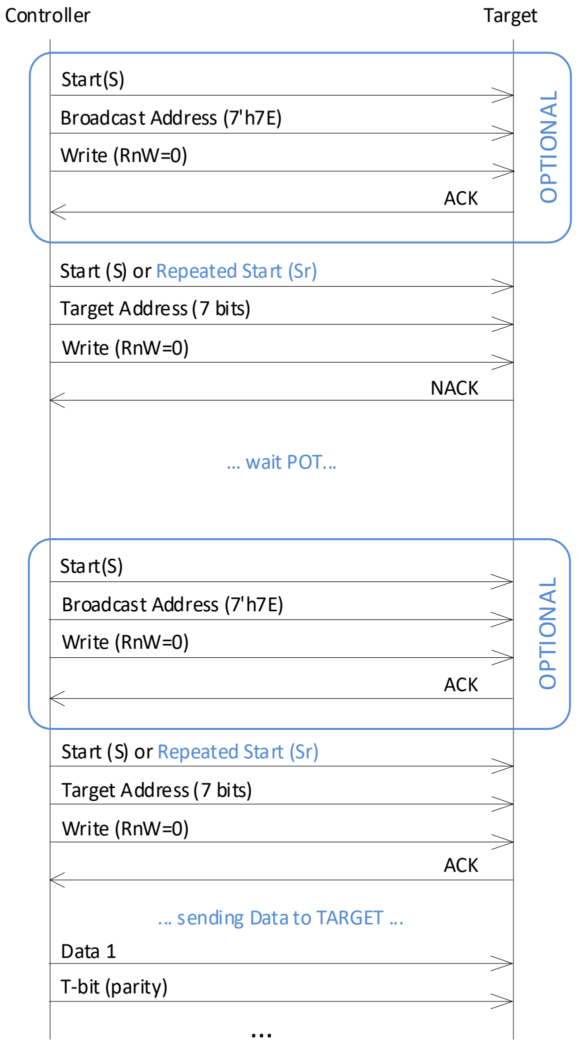
The CTLR shall adapt its behavior according to the parameters specified by the CIP.

3.4.4 Detecting TARGET Ready to Receive Data

The TARGET may decide to enter Power Saving Mode to save battery, in which case it would not be able to receive data. The conditions under which a TARGET implementation may enter such a Power Saving Mode are described in section 5.

When the CTLR wishes to send data and assumes that the TARGET has entered Power Saving Mode, the CTLR shall still attempt to send data to the TARGET at a period of time defined by POT, as described in Figure 3-14. The CTLR assumes that this attempt to send data causes the TARGET to wake up. If the TARGET is not ready to receive data from the CTLR, it shall reject the I3C write request by sending a NACK. The polling time (POT) used by the CTLR shall be greater than the MPOT communicated by the CIP. If the TARGET is offline (e.g. in deep sleep), the NACK is done passively by not pulling SDA low after the address has been emitted.

Figure 3-14: I3C – CTLR Detecting TARGET Ready to Receive Data



3.4.5 Sending Data to TARGET

When the TARGET is in RECEIVING state, it is idle and waiting for a Data Link Layer block from the CTLR. In RECEIVING state, the TARGET shall:

- Acknowledge (ACK) any I3C write request from CTLR (matching the I3C address of the TARGET)

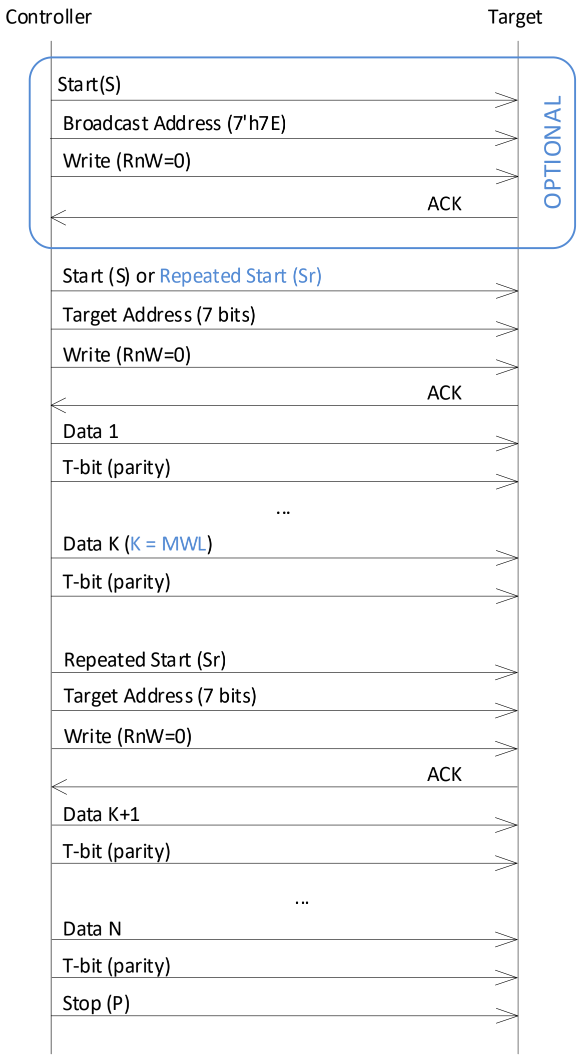
The CTLR shall follow the sequence below to send an I3C frame to the TARGET:

0) OPTIONAL: See [I3C] section 5.1.2.2.3 for details.
    a. Send I3C start condition.
    b. Send I3C Broadcast Address (7'h7E + R/W bit low).
    c. Receive ACK from TARGET.
1) Send I3C start condition or repeated start condition (if optional step 0 was performed or coming from step 3).
2) Send the I3C address of the TARGET with the R/W bit low (Write to TARGET) and receive ACK from the TARGET. If the TARGET sends a NACK, the CTLR should retry from step 1).
3) Send a complete message (i.e. all or part of a Data Link Layer block) up to Maximum Write Length (MWL). Repeat from step 1) if there is more data to send.
4) Send I3C stop condition.

This sequence performs a private write operation, as described in [I3C]. The CTLR shall send a complete Data Link Layer block using a single I3C frame, as illustrated in Figure 3-15. However, it may abort the frame transmission anytime by sending an I3C stop condition. The CTLR shall wait for the duration of RWGT (Read Write Guard Time) before initiating any new I3C read request.

> **Note:** During a private write operation, the T-bit is interpreted as a parity bit. It is automatically handled at the I3C peripheral level, and the TARGET will follow the rules described in [I3C] if the received parity bit doesn't match. The TARGET shall ignore subsequent bytes until STOP condition and respond with an R-Block with error indication, i.e.: "CRC error" (see error handling described in section 4.1).

Figure 3-15: I3C – CTLR Sends a Data Link Layer Block to the TARGET



3.4.6 Detecting TARGET Ready to Send Data

When the CTLR has finished sending an I3C frame (i.e. the TARGET has received the I3C stop condition), the TARGET shall switch from RECEIVING state to PROCESSING state. In PROCESSING state, the TARGET is busy processing the command sent by the CTLR and shall:

- Reject (NACK) any I3C write request from CTLR
- Reject (NACK) any I3C read request from CTLR

To detect that the TARGET is ready to send data and to initiate the retrieval of such data, the CTLR shall use the I3C In-Band Interrupt (IBI) mechanism to receive Data Transfer Request from the TARGET.

To send a Data Transfer Request, the TARGET shall request an In-Band Interrupt (IBI) to the CTLR.

To allow for IBI requests, for each I3C frame the CTLR should:

1) Send I3C start condition.
2) Send I3C Broadcast Address (7'h7E + R/W bit low). (See [I3C] section 5.1.2.2.3 for details.)
3) Receive ACK from TARGET.

As described in [I3C], if there is no activity on the bus for more than 1µs (i.e. Bus Available Condition in [I3C]), a TARGET may alternatively issue a start condition request. In this case, the CTLR would complete the start condition and the TARGET would be able to request an IBI.

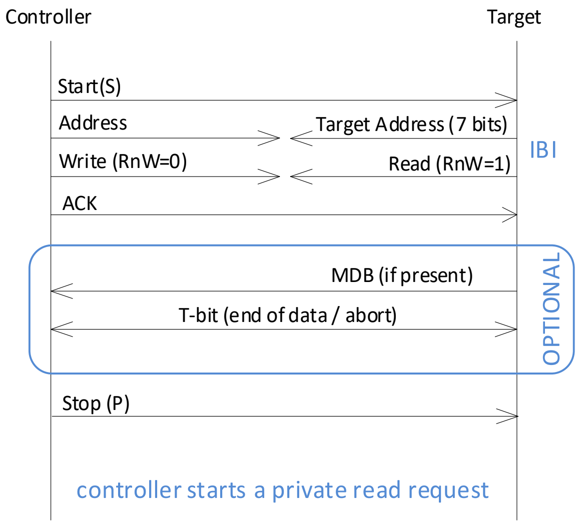
When detecting an IBI request, the CTLR may either:

- NACK the request, in which case the TARGET shall retry later; or
- ACK the request.
  - If the TARGET is capable of sending the Mandatory Data Byte (MDB) to the CTLR, as indicated in the capabilities of the TARGET (BCR[2]; see [I3C] section 5.1.1.2.1), it shall send the value 0xB0 (which is vendor reserved and complies with the MDB category of Pending Read Notification). In this case the Data Transfer Request is equivalent to an [I3C] Pending Read Notification.
  - Else the CTLR shall not expect the TARGET to send an MDB.
  - In both cases, the CTLR shall initiate a private read request and the TARGET shall be ready to transmit the data.

Note 1: As described in [I3C], the TARGET can request an IBI by leveraging the concept of arbitrable address headers. Any address header (following a start condition) can be subject to arbitration, meaning both the CTLR and one (or more) TARGET may attempt to drive an address on the I3C bus using the SDA line. When using the IBI mechanism, the I3C frame initiated by the CTLR begins with a start condition followed by the broadcast address (0x7E<<1). This broadcast address is arbitrable, which means any TARGET on the I3C bus has a chance to request an IBI by transmitting its own address (with R/W bit set to read) at the same time the broadcast address is being transmitted by the CTLR.

Note 2: According to [I3C] section 5.1.6.2.2, the use of IBIs with an MDB by a TARGET to indicate a Pending Read Notification might need to be enabled by the CTLR. In the scope of this specification, IBIs with an MDB to indicate a Pending Read Notification are implicitly enabled for all TARGETs capable of sending the MDB.

Figure 3-16: I3C – TARGET Signaling Pending Data followed by Read by CTLR



3.4.7 Receiving Data from TARGET

When the TARGET has finished processing the Data Link Layer command block sent by the CTLR and it is ready to send a Data Link Layer response block, the TARGET shall switch from PROCESSING to SENDING state. In SENDING state, the TARGET shall:

- Acknowledge (ACK) any I3C read request from the CTLR (matching the I3C address of the TARGET) if it is ready to send data, or otherwise NACK the I3C read request from the CTLR.

The CTLR shall follow the sequence below to receive an I3C frame from the TARGET:

0) Manage the IBI request, as described in section 3.4.6.

1) Send I3C repeated start condition.

2) Send the I3C address of the TARGET with the R/W bit high (Read from TARGET). If the TARGET sends a NACK, the CTLR should retry from step 1). The CTLR may wait for the duration of RWGT (Read Write Guard Time) before retrying from step 1).

3) Receive a complete message with a length up to Maximum Read Length (MRL). Repeat from step 1) if there is more data to receive.

4) Send I3C stop condition.

This sequence performs a private read operation, as described in [I3C]. The CTLR may read the response bytes using a single I3C frame or multiple I3C frames, as illustrated in Figure 3-17 and Figure 3-18. The CTLR shall wait for the duration of RWGT (Read Write Guard Time) before initiating any new I3C write requests.

> **Note:** During a private read operation, both CTLR and TARGET can influence the T-bit. The TARGET signals the end of data by setting the T-bit to 0 whereas the CTLR may abort the private read operation by setting the T-bit to 0.

The TARGET shall remain in SENDING state until all response bytes have been read by the CTLR or until the CTLR sends a new I3C write request (see section 3.4.5), e.g. because the CTLR detected an error. In this latter case, the TARGET shall discard any unsent bytes and switch to RECEIVING state.

The TARGET shall signal the end of data in the T-bit, after the last byte of a Data Link Layer block is transferred.

As the CTLR may safely expect to receive a Data Link Layer block (see section 4) from the TARGET, the CTLR may determine from the prologue field of that block how much data shall be received.

Figure 3-17: I3C – Example: CTLR Receives Data Link Layer Block from TARGET Using Single I3C Frame

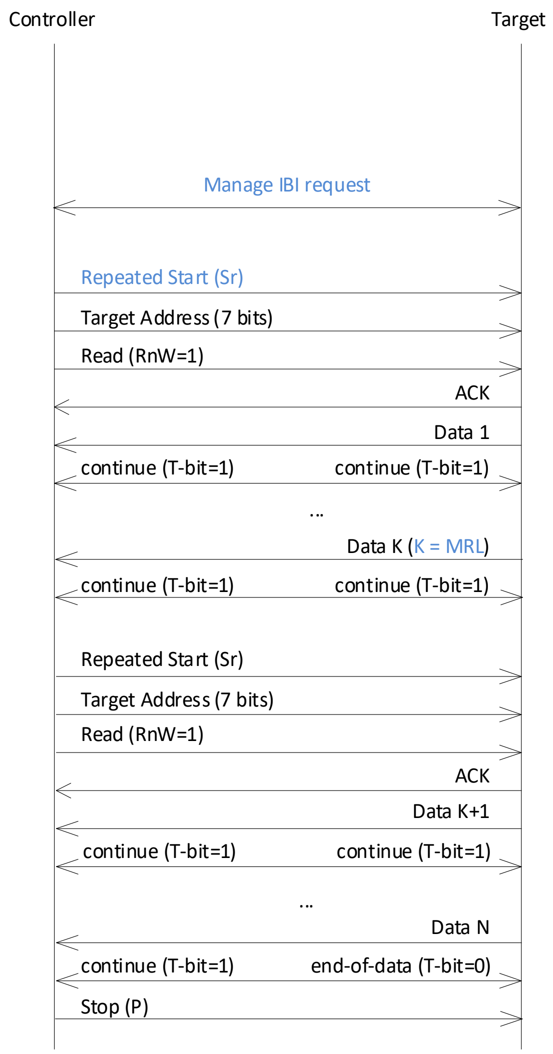
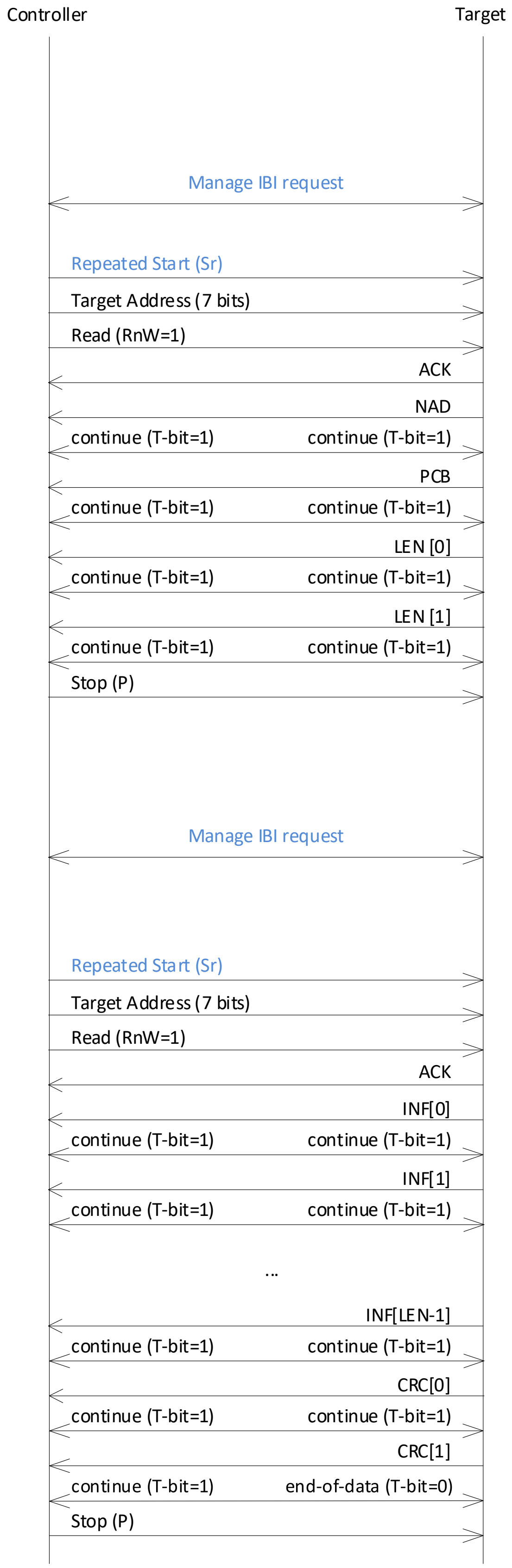


Figure 3-18: I3C – Example: CTLR Receives Data Link Layer block from TARGET Using Multiple I3C Frames



3.4.8 Default Parameter Values

The following table defines I3C parameter values that shall be used by default.

Table 3-3: I3C – Default Parameter Values

Parameter	Description	Unit	Value
DMPOT	Default Minimum Polling Time	µs	1000
DRWGT	Default R/W Guard Time	µs	300
DMRL	Default Maximum Read Length	bytes	64
DMWL	Default Maximum Write Length	bytes	64

Note: Once the CIP (see section 4.3) has been retrieved from the TARGET, the CTLR shall instead use the parameter values (or ranges) specified by the CIP.

Note: DMRL/DMWL apply when no negotiation for MRL/MWL takes place as described in [I3C] and if MRL/MWL are not pre-known.

3.4.9 Compatibility with Legacy I²C Targets

A legacy I²C TARGET may operate on an I3C bus only under the following conditions:

- The I²C TARGET supports Fast mode (Fm) or Fast mode + (Fm+), i.e. 400kHz or 1MHz clock frequency.
- The I²C TARGET does not use clock stretching.
- The static address and legacy virtual register (containing the operating I²C mode) of the I²C TARGET are known in advance by the I3C CTLR (i.e., before power-up).

4 Data Link Layer

The Data Link Layer uses one of the Physical Layers described in section 3 to transfer blocks of data between the CTLR and the TARGET. Such blocks may only be sent alternately by the CTLR and TARGET (i.e. half-duplex communication) and may convey application data or transmission control data. The protocol that shall be implemented by the Data Link Layer is very similar to the T=1 protocol described in [7816-3] and therefore is simply called T=1'.

For a physical layer allowing multiple TARGETs on the same bus, such as I3C, a CTLR shall maintain a Data Link Layer context for each TARGET.

4.1 T=1' Protocol

The T=1' protocol builds upon the T=1 protocol described in [7816-3] with the following differences:

- The general block structure is the same except for the LEN field of the prologue, which is coded on 2 bytes.
- Additional rules are defined for the value of the NAD field.
- 2-byte CRC is retained as the unique EDC algorithm that shall be used.
- The S(IFS xxx) block may contain a value coded on 1 or 2 bytes.
- Additional S-Blocks are defined (see details in section 4.2.2).
- A default IFSC value of 8 is defined and shall be used by the CTLR if it doesn't know IFSC. This default value is large enough for the CTLR to send an S(CIP request) block, which the CTLR may want to do in order to discover a more suitable IFSC value.
- A default IFSD value of 64 is defined and shall be used by the TARGET if it doesn't know IFSD. This default value is compatible with the maximum CIP length. The CTLR may send an S(IFS request) block to declare a more suitable IFSD value for the remainder of the communication.
- No assumption is made about the presence or absence of a physical reset mechanism (e.g. cold or warm reset). Only a software reset is defined, which may be requested using new S(SWR xxx) blocks. Situations where a physical mechanism could be needed and used remain out of scope of this specification.

More explanations are given throughout section 4.2.

The rules for error free operation described in [7816-3] section 11.6.2.3 and the example scenarios described in [7816-3] Annex A.2 still apply. The error handling rules described in [7816-3] section 11.6.3 and the example scenarios described in [7816-3] Annex A.3 still apply. Notice however that when [7816-3] suggests performing a “warm reset”, the T=1' protocol should try to exchange S(SWR xxx) blocks instead (see section 4.2.2).

4.2 Block Format

The general block structure used by the T=1' protocol is the same as the one described in [7816-3] for the T=1 protocol; however, the LEN field is coded on 2 bytes as shown in Table 4-1.

Table 4-1: Block Format

Prologue Field (mandatory)			Information Field (optional)	Epilogue Field (mandatory)
NAD (1 byte)	PCB (1 byte)	LEN (2 byte)	INF (LEN bytes)	CRC (2 bytes)

The LEN and CRC fields shall have their Most Significant Byte sent first (i.e. big-endian order).

For example, a block transporting a 14-byte APDU command (including Le field) and having a CRC value of 0x42EB would be coded as indicated in Table 4-2. (**Note:** NAD and PCB values may vary, and CRC value vary accordingly.)

Table 4-2: Example Block Format

NAD	PCB	LEN[0]	LEN[1]	INF	CRC[0]	CRC[1]
'29'	'40'	'00'	'0E'	'00A40400 08 A000000151000000 00'	'42'	'EB'

4.2.1 Node Address Byte (NAD) Field Format

For configurations where both the CTLR and the TARGET implement logical connections, the T=1' protocol amends the original T=1 protocol by re-using bit 8 and bit 4 of the NAD byte and generalizing the interpretation of the DAD and SAD values, as further explained below.

Table 4-3: NAD Format

b8	b7	b6	b5	b4	b3	b2	b1	Description
0				0				invalid
0				1				Block from CTLR to TARGET
1				0				Block from TARGET to CTLR
1				1				invalid
	x	x	x					DAD (bits b7-b6-b5)
					x	x	x	SAD (bits b3-b2-b1)

Bit 8 and bit 4 shall be used together to specify the direction of the transmitted block, either from a CTLR to a TARGET or from a TARGET to a CTLR. A NAD Byte with both b4 and b8 set to 0 or both set to 1 is invalid (error handling described in [7816-3] section 11.6.3 applies).

The DAD value (bits b7-b6-b5) and SAD value (bits b3-b2-b1) shall be used together to encode a logical connection number. Blocks in which the NAD byte contains the same pair of DAD and SAD values shall be associated with the same logical connection. As a consequence, incoming blocks (from CTLR to TARGET) and outgoing blocks (from TARGET to CTLR) associated with the same logical connection shall have their DAD and SAD values swapped.

The following concerns are left out of scope and might be further defined by users of this specification:

- How the DAD and SAD values are combined to form a logical connection number. In particular, although the names DAD and SAD are kept in this specification, they might not pertain to so-called destination and source addresses.
- How logical connections are created and interpreted by communicating devices.

If the TARGET is not aware of the logical connection associated with an incoming block (e.g. because such a logical connection hasn't been created), then in order to build the NAD byte of an outgoing block the TARGET should simply re-use and swap the DAD and SAD values of the last incoming block.

For configurations where the TARGET does not implement logical connections, in order to build the NAD byte of an outgoing block the TARGET should simply swap the first and last 4 bits (nibbles) of the NAD byte of the last incoming block. Implementing such a behavior remains compatible with generic rules (where logical connections are supported) and still allows the CTLR using logical connections if so desired.

For configurations where neither the CTLR nor the TARGET implements logical connections, this specification recommends using the following NAD byte values:

- From CTLR to TARGET: '29' (DAD=010b, SAD=001b)
- From TARGET to CTLR: '92' (DAD=001b, SAD=010b)

4.2.2 Protocol Control Byte (PCB) Field Format

The PCB field defines the type of the block and includes transmission control data.

The T=1' protocol introduces the following new block types:

- S(CIP request): Requests the TARGET to return the CIP.
- S(CIP response): Answers an S(CIP request) block containing the CIP (see section 4.3).
- S(RELEASE request): Releases the TARGET, i.e. the CTLR indicates that it doesn't mind the TARGET going to Power Saving Mode at that time. See section 5 for more details.
- S(RELEASE response): Acknowledges an S(RELEASE request) block.
- S(SWR request): Requests the TARGET to perform a software reset of the communication interface. When sending this request, the CTLR also resets the N(S) bit and discards any block chaining information. The exact interpretation of this request by the TARGET is out of scope.
- S(SWR response): Acknowledges an S(SWR request) block after software reset.

The encoding of the PCB field is described in Table 4-4.

Table 4-4: Protocol Control Byte (PCB)

Type	Sub-Type	b8	b7	b6	b5	b4	b3	b2	b1
I-Block	Application Data	0	N(S)	M-bit	0	0	0	0	0
R-Block	Error-free acknowledgement	1	0	0	N(R)	0	0	0	0
	CRC error	1	0	0	N(R)	0	0	0	1
	Other error	1	0	0	N(R)	0	0	1	0
S-Block	RESYNCH request	1	1	0	0	0	0	0	0
	RESYNCH response	1	1	1	0	0	0	0	0
	IFS request	1	1	0	0	0	0	0	1
	IFS response	1	1	1	0	0	0	0	1
	ABORT request	1	1	0	0	0	0	1	0
	ABORT response	1	1	1	0	0	0	1	0
	WTX request	1	1	0	0	0	0	1	1
	WTX response	1	1	1	0	0	0	1	1
	CIP request	1	1	0	0	0	1	0	0
	CIP response	1	1	1	0	0	1	0	0
	RELEASE request	1	1	0	0	0	1	1	0
	RELEASE response	1	1	1	0	0	1	1	0
	SWR request	1	1	0	0	1	1	1	1
	SWR response	1	1	1	0	1	1	1	1
	Reserved for future use	1	1	x	1	0	x	x	x
	Reserved for proprietary use	1	1	x	1	1	x	x	x

4.2.3 Length (LEN) Field Format

The LEN field encodes the length of the INF field of the block.

The following values shall be considered as invalid by the receiver:

- Values exceeding the current IFS value of the receiver (i.e. IFSC for TARGET, IFSD for CTLR)
- Values beyond '0FF9' (4089) (see explanations in section 4.2.5)

4.2.4 Information (INF) Field Format

The content of the INF field depends on the block type.

Table 4-5: Information (INF) Field Format

Type	Sub-Type	Information Field Usage
I-Block	Application Data	Application Data
R-Block	Error-free acknowledgement	Not Present
	CRC error	Not Present
	Other error	Not Present
S-Block	RESYNCH request	Not Present
	RESYNCH response	Not Present
	IFS request	1- or 2-byte IFS value (see explanations below)
	IFS response	Same INF field as preceding S(IFS request)
	ABORT request	Not Present
	ABORT response	Not Present
	WTX request	1-byte integer value multiplier of BWT
	WTX response	Same INF field as preceding S(WTX request)
	CIP request	Not Present
	CIP response	Communication Interface Parameters (see section 4.3)
	SWR request	Not Present
	SWR response	Not Present
	RELEASE request	Not Present
	RELEASE response	Not Present

For the INF field of an S(IFS request) block:

- A value from '01' to 'FE' shall be coded on 1 byte.
- A value from '00FF' to '0FF9' (4089) shall be coded on 2 bytes (MSB first).
- Values beyond '0FF9' (4089) are invalid (see details in section 4.2.5).

4.2.5 Epilogue Field Format

The Epilogue field conveys the Error Detection Code of the block.

In this version of the specification, a 2-byte CRC shall be used. Note that such a CRC can only efficiently protect (2^15 - 1) bits (including itself) from 1, 2, and 3 bits corruption. For this reason, the size of INF fields in this protocol is limited to a maximum value of '0FF9' (4089) bytes.

4.3 Communication Interface Parameters

The CIP contains the communication interface parameters (i.e. both Physical Layer and Data Link Layer parameters) that the CTLR shall use to communicate with the TARGET, as well as Historical Bytes.

To retrieve the CIP, the CTLR shall send an S(CIP request) block (see section 4.2) and receive an S(CIP response) block containing the CIP structure described in the following sections. This procedure may be used anytime (although rather expected to be used upon power on or after a software reset).

In the following sections, all numerical values are encoded as unsigned integers.

4.3.1 CIP – Common Structure

This section describes the common structure of the CIP, irrespective of the Physical Layer that is used.

Table 4-6: CIP – Common Structure

Name	Length	Description
PVER	1	Protocol Version This version of the specification defines version '01' of the protocol.
Length of IIN	1	Length of Issuer Identification Number (0 or 3 or 4)
IIN	Var.	(Optional) Issuer Identification Number (according to [7812-1], BCD encoded) registered by and identifying the SE OS Developer
PLID	1	Physical Layer ID: '00' for ISO/IEC 7816, '01' for SPI, '02' for I^{2}C, and '03' for I3C
Length of PLP	1	Length of Physical Layer Parameters
PLP	Var.	Physical Layer Parameters Either data describing the SPI Physical Layer, as defined in Table 4-8, or data describing the I^{2}C Physical Layer, as defined in Table 4-9
Length of DLLP	1	Length of Data Link Layer Parameters
DLLP	Var.	Data Link Layer Parameters: see Table 4-7
Length of HB	1	Length of Historical Bytes (Max. 32 bytes)
HB	Var.	Historical Bytes

When the Physical Interface is the ISO/IEC 7816 interface (Physical Layer ID = '00'), no Physical Layer Parameters, no Data Link Layer Parameters and no Historical Bytes shall be present (i.e. the corresponding length bytes shall be set to 0), as all the necessary parameters are already sent automatically by the TARGET within the ATR (following the reset signal sent by the CTLR on the RST line).

In this version of the protocol, the overall length of the CIP structure shall not be greater than 64 bytes.

Note: This requirement is compatible with the default IFSD value defined in section 4.1.

4.3.2 CIP – Specific Parameters for Data Link Layer

This section describes the parameters provided by the CIP for the Data Link Layer.

Note: This section does not apply when the underlying Physical Layer is the ISO/IEC 7816 interface.

Table 4-7: CIP – Specific Parameters for Data Link Layer

Name	Length	Description
BWT	2	Block Waiting Time (in ms)
IFSC	2	Maximum Information Field Size of the TARGET (in bytes) (i.e. initial value)

If the CIP has never been retrieved and the CTLR is not aware of the BWT that may be used, the CTLR shall use a default BWT value (DBWT) of 300ms.

Note: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), CTLR implementations shall accept more data (not described in the table above) to be present at the end of Data Link Layer Parameters and ignore such data.

4.3.3 CIP – Specific Parameters for SPI Physical Layer

This section describes the parameters provided by the CIP when the SPI Physical Layer is used.

Table 4-8: CIP – Specific Data for SPI Physical Layer

Name	Length	Description
Configuration	1	RFU
PWT	1	Power Wake-Up Time (in ms; see section 3.1.3)
MCF	2	Maximum Clock Frequency (in kHz; see section 3.1.2.1)
PST	1	Power Saving Timeout (in ms; see section 5)
MPOT	1	Minimum Polling Time (multiple of 100µs; see Note 2 below)
TGT	2	Target Guard Time (in µs; see section 3.1.2.3)
TAL	2	Maximum Target Access Length (in bytes; see Note 3 below)
WUT	2	Wake-Up Time (in µs; see section 3.1.4)

Note 1: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), CTLR implementations shall accept more data (not described in the table above) to be present at the end of Physical Layer Parameters and ignore such data.

Note 2: See section 3.1.5. If the Polling Mechanism is **not** used, MPOT shall be set to '00'.

Note 3: See section 3.1.2.3. The TARGET may indicate the maximum access length with the TAL or may set the TAL to specific values to indicate the level of support for fragmented SPI accesses:

- A TAL of 'FFFF' indicates that the TARGET does not require fragmentation. The CTLR may send or receive entire Data Link Layer blocks with a single SPI access. But the TARGET still supports fragmentation. The CTLR may decide (due to constraints on its side) to split the transfer of Data Link Layer blocks into multiple SPI fragments.
- A TAL of '0000' indicates that the TARGET does not support fragmentation. The CTLR shall transfer Data Link Layer blocks in a single SPI access. In this case the overall length of the CIP shall not be greater than DTAL (see section 3.1.7).
- Any other value indicates the maximum TAL of the TARGET and that the TARGET supports SPI fragmentation.

4.3.4 CIP – Specific Parameters for I²C Physical Layer

This section describes the parameters provided by the CIP when the I²C Physical Layer is used.

Table 4-9: CIP – Specific Parameters for I²C Physical Layer

Name	Length	Description
Configuration	1	RFU
PWT	1	Power Wake-Up Time (in ms; see section 3.2.3)
MCF	2	Maximum Clock Frequency (in kHz; see section 3.2.2)
PST	1	Power Saving Timeout (in ms; see section 5)
MPOT	1	Minimum Polling Time (multiple of 100μs; see sections 3.2.4 and 3.2.6)
RWGT	2	R/W Guard Time (in μs; see sections 3.2.5 and 3.2.6.2)

Note: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), CTLR implementations shall accept more data (not described in the table above) to be present at the end of Physical Layer Parameters and shall ignore such data.

4.3.5 CIP – Specific Parameters for I3C Physical Layer

This section describes the parameters provided by the CIP when the I3C Physical Layer is used.

Table 4-10: CIP – Specific Parameters for I3C Physical Layer

Name	Length	Description
Configuration	1	RFU
PST	1	Power Saving Timeout (in ms; see section 5)
MPOT	1	Minimum Polling Time (multiple of 100μs; see section 3.4.4)
RWGT	2	R/W Guard Time (in μs; see section 3.4.5)

Note: Some communication parameters used by the I3C physical layer do not appear in the CIP as they are already discovered by the CTLR as described in [I3C]. E.g., dynamic I3C addresses, maximum read/write length, data rate limitation (if any), etc.

5 Power Saving Policy

The TARGET may decide to enter Power Saving Mode in order to save battery. The conditions under which a TARGET implementation would enter such a mode usually depend on high-level applicative use cases defining requirements regarding performance, availability, battery saving, etc. As it might be impossible to capture a set of such conditions that would fit all use cases, this specification acknowledges the fact that a particular TARGET implementation may decide to enter Power Saving Mode according to proprietary policies. Nevertheless, this document specifies the following interoperable policy for the TARGET:

- The TARGET may only enter Power Saving Mode:
  - On receipt of an S(RELEASE request) block (see section 4.2.2) and after returning the corresponding S(RELEASE response) block, or
  - After a timeout if the CTLR didn't send any new Data Link Layer block after any of the following events:
    - Completion of boot (upon Power-On)
    - TARGET returned an R-block or S-block (including S(SWR response)).
    - TARGET returned an I-block completing the sending of an APDU response (or last APDU response of a chain if APDU chaining is used).

  While this policy guarantees that the TARGET will only enter Power Saving Mode when one of the above conditions is satisfied, the TARGET may choose not to do so (i.e. even if above conditions are satisfied) for other proprietary reasons.

  Notice that if a timeout applies (see below), the CTLR may choose to send an S(RELEASE request) block before the timeout is reached, i.e. providing the TARGET with an earlier opportunity to enter Power Saving Mode.

- The TARGET shall indicate the applicable Power Saving Timeout value (PST) as part of the CIP (see section 4.3).
  - If the timeout value is set to '00', the TARGET indicates that it may enter Power Saving Mode according to a proprietary policy. It is assumed that the CTLR implementation is aware of and can adapt its behavior to such a proprietary policy.
  - If the timeout value is set to 'FF', the TARGET indicates that it doesn't use this timeout value and therefore may only enter Power Saving Mode on receipt of an S(RELEASE request) block.
  - Any other value (from '01' to 'FE') shall be understood as a valid timeout value. Note that the CTLR should apply some margin when measuring timeouts.

Upon power-on, if the CTLR expects the TARGET to implement the above interoperable policy and is not aware of the applicable timeout value (e.g. CIP not retrieved yet), it shall assume that the TARGET may have already entered Power Saving Mode.

It is assumed that, if the TARGET implements a proprietary Power Saving Policy (or only partially behaves according to the above interoperable policy), the CTLR would have enough knowledge of such a proprietary policy to adapt its own behavior.

Notice that it is assumed that entering or exiting the Power Saving Mode has no effect on the communication parameters of the Data Link Layer (e.g. N(S) bit, M bit, N(R) bit).

Note: [7816-3] was initially written for smart cards, which do not fundamentally need to have a built-in power saving mechanism as they are typically powered only during the course of a transaction and usually do not need to be kept powered on for a longer period of time. The situation is different in embedded use cases for which every possible means to save energy from the CTLR may need to be put in place. The CTLR has the freedom to switch off the power applied to the TARGET at any time, the ISO/IEC 7816 interface is designed to allow immediate start-up of the TARGET whenever the CTLR wishes to start communicating with the TARGET again.

Annex A OPTIMIZATIONS FOR PRODUCTION ENVIRONMENTS (INFORMATIVE)

A few simplifications of the T=1' protocol may be considered for usage in production environments where higher security and reliability assumptions can be made, leading to higher performances and a reduced binary code size. This section describes a variant of the T=1' protocol, called the T=1* protocol, which may include a number of optimizations for usage within such environments.

The T=1* protocol may include all or part of the following changes compared to the T=1' protocol:

- The Chaining Mechanism described in [7816-3] section 11.6.2.2 is not supported. In particular,
  - The M-bit of I-blocks shall always be set to 0.
  - The S(ABORT xxx) blocks are not supported.
- IFSC and IFSD values are known to the CTLR and TARGET and will not change, hence there is no need to notify IFSC or IFSD changes. In particular,
  - The S(IFS xxx) blocks are not supported.
- Optimal communication parameters are already known to the CTLR and TARGET, hence CIP retrieval by the CTLR is not supported. In particular,
  - The S(CIP xxx) blocks are not supported.
- The production process only requires usage of a single communication interface, hence there is no need for the CTLR to “release” the TARGET. In particular,
  - The S(RELEASE xxx) blocks are not supported.
- The TARGET does not implement any Power Saving Mode, hence allowing for optimizations of the Physical Interface (e.g. no or simplified Wake-Up procedure).

It is assumed that the CTLR and TARGET know in advance which of the above optimizations are implemented.