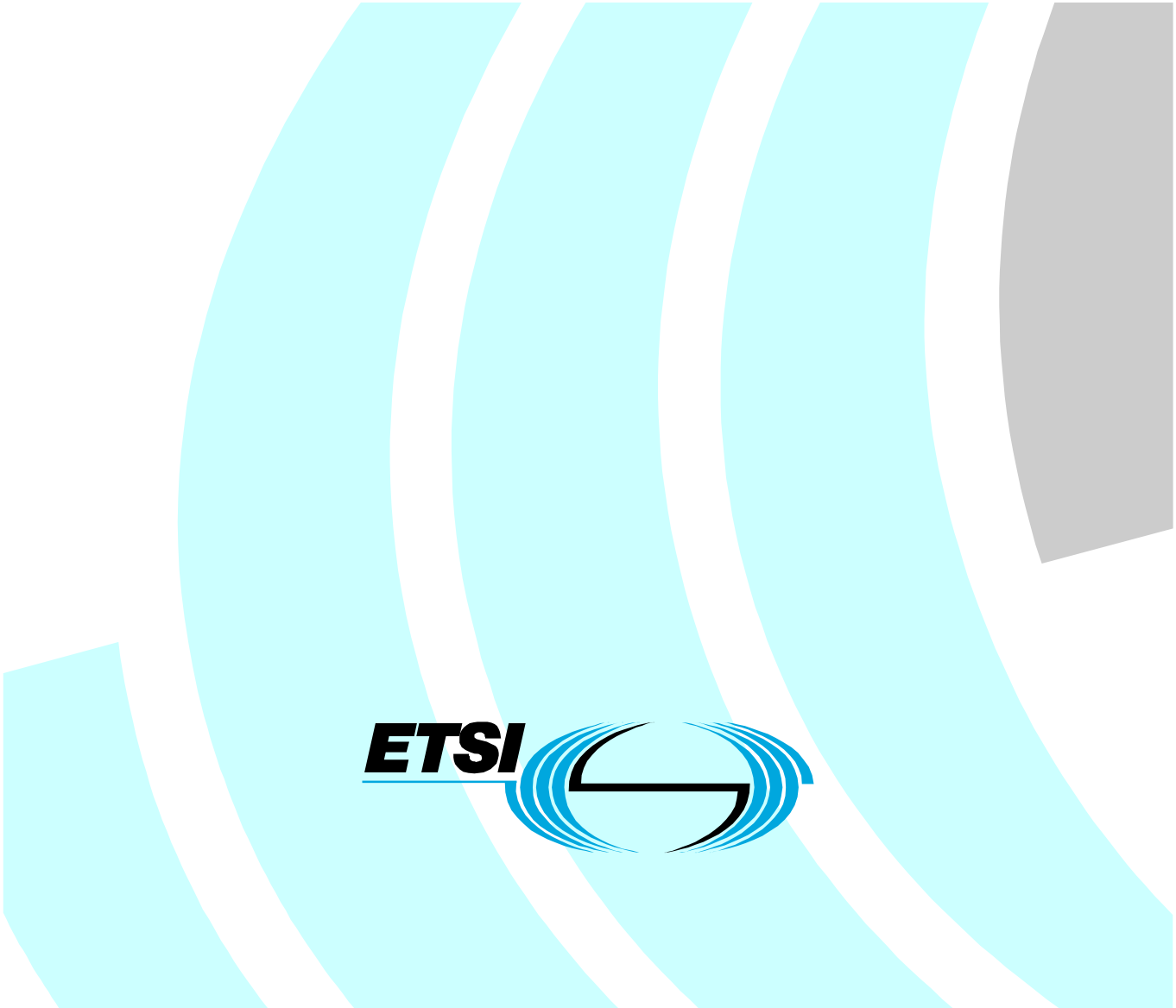
ETSI TR 102 242 V3.0.0 (2003-06)

Technical Report

Smart Cards;
Terminal - card interface;
Considerations on robustness improvements



Reference
DTR/SCP-010287

Keywords
EMC, smart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Smart Card Platform (SCP).

Introduction

Extensive use of the GSM specifications has revealed a potential weakness of the communication interface between card and terminal.

The evaluation has shown that radiated RF bursts could generate significant I/O line voltage drops that could lead to major communication interference.

It was also noticed that the I/O voltage drop did not depend on voltage supply but on RF emission power and the technology used in the card and card reader implementation, thus making the interface more sensitive to RF radiation when operating at the lower voltage classes.

In addition, the present document identifies other potential weaknesses of the currently specified terminal-card interface, lists existing mechanisms and identifies countermeasures and enhancements that may improve the interface robustness.

Some of the identified countermeasures do not require any change in the current standards. These should be applied in Terminals and SIM/UICC silicon design in order to reduce the risk of having interface malfunction especially at low voltage operation.

Other countermeasures have been outlined that would provide further improvement of the operation. They would require changes in the standards that will be studied and proposed in further documents.

1 Scope

The present document describes:

- the failure mechanisms that could potentially generate major operating issues between the terminal and the card;
- the countermeasures that should be applied within the current specifications;
- the enhancements that may further increase the interface robustness.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ISO/IEC 7816-3: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[2] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Answer To Reset (ATR): string of characters sent by the card following a reset sequence

card: smart card, SIM or UICC

clock: clock provided by the terminal to the card

terminal: handset, ME or UE

reader: hardware used to connect the card to the terminal printed circuit board

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ATR	Answer To Reset
CLK	Clock signal provided by the terminal to the card
I/O	bi-directional communication line between the terminal and the card
ME	Mobile Equipment
MF	Master File
PCB	Printed Circuit Board
RST	Reset signal provided by the terminal
T=0, T=1	Communications protocols defined in ISO/IEC 7816 standards
TDMA	Time Division Multiple Access

4 Failure mechanisms and applicable countermeasures

There are basically two main categories. One is the contact problem that can occur between the reader and the card. The card is connected to terminal using a reader with spring contacts. In particular in a mobile application the terminal is subject to vibration and drop, the conformance requirements is that the terminal shall withstand certain vibration and free fall. The mechanical stress is propagated through the mechanics of the terminal to the card reader causing bending and contact problems. Another source for contact problems is dust and wear of the contacts surfaces in general. The card is seldom removed from the reader and depending upon the reader design removing the card may not have a cleaning effect on the contacts. Also the problem with excessive wear on the contact plating due to frequent removal or improper reader design may on a long term cause contact problems.

Another failure mechanism is interference caused by external sources. These problems are seen as increased noise level on the signals between the card and the terminal. The sensitivity or immunity against external interference is depending upon the impedance of the electrical signals and the way the connection has been implemented. The immunity to interference is also depending upon how the interface is operated.

The two categories are described hereafter, together with the already specified or recommended countermeasures.

4.1 Mechanical failures

These failures are considered as momentary disconnection of a contact. The way this happens is of no importance. Contact failures on some contacts will be catastrophic and can not be 'rescued' as is the case with contacts related to the communication and control interface (CLK, RST, I/O).

A contact failure on the power and ground cannot be encountered for except in a situation where the power consumption is very low and there is an energy storage on the card, as an example a capacitor on the card between power and ground. In this case a contact failure on the power and ground may to some extent be covered up for. As a general conclusion contact problems on power and ground signals cannot be covered up.

Contact problems on the communication and control contacts can be covered up so that they do not affect the system or the state of the card. In order to find out what is needed as study of the behaviour of each contact is needed and to identify the state which these signals are in most of the time. The interface has an idle state which it is in when there is no activity on the interface. In a telecom application the idle state may be the state in which the card is in most of the time, which means that a contact problem is more likely to occur in this state. In the analysis the assumption is that only that contact is disconnected from the terminal, other combinations may occur.

4.1.1 RST pin

The Reset signal is in the physical high state except during the start up sequence on the card. In order to prevent uncontrolled reset of the card due to contact problems having a weak pull-up on the card inside would not cause any change in the state of this signal on the card side if the connection on this side is momentarily disconnected. Having a pull-down in the card on this signal inside the card would cause an automatic reset of the card. Once the contact to the terminal is established the reset is pulled high and if the clock is running the card would return the ATR which would cause confusion. Depending upon the implementation in the card if the clock is not running when this failure would occur the ATR may not be transmitted until the clock is started. When the terminal starts the clock it means that a command will be sent. This command will collide with the ATR and the terminal will not get the response to the transmitted command and the ATR sent by the card would be lost. The state of the card would be that the MF is selected as after a normal successful ATR. This would lead to a situation where the ME has different information regarding the current directory, where the pointers are in the card. This will lead to a mismatch in the commands sent to the terminal with respect to the current state of the card.

The outcome of the scenarios is that in order to minimize the impact on contact problems on the reset contact the card should contain a weak pull-up in order not to cause unexpected ATRs to be transmitted upon a contact failure on the RST line.

4.1.2 CLK pin

A connection problem on the CLK contact is a problem when the clock is running. In case the clock is stopped if a resistor is connected to the corresponding level of the clock stop the problem can be covered up for. The card should indicate the relevant preferred clock stop level.

4.1.3 I/O pin

The natural level of the I/O signal is high. Therefore including a weak pull-up in the card on the I/O line would cover up for contact failures during sleep or idle when the I/O line is in its high state.

4.2 Interference from external signals

Due to the nature of the buffer used for the signal generation, not all of the card pins are equally subject to this kind of interference. As a matter of fact, the high impedance nature of the I/O pin at the high logical level makes it more sensitive. Thus, only interference on I/O pin is part of this analysis.

4.2.1 Consequences of interference on the I/O pin

As expressed before, only the "high" level of the I/O can suffer from interference as the signal is asserted through a pull up resistor. A strong interference can generate a parasitic pulse on the I/O that could have different effects depending upon the card state:

- The card is in Idle mode, the clock is running: Depending on the pulse duration, it could be ignored (not long enough to be recognized as a start bit), or processed as a start bit, leading to a communication error (parity error regardless of the convention) followed by a retransmit request from the receiver(s) (both terminal and card could potentially see the pulse).
- The card is in Idle mode, the clock is stopped: If the I/O signal is not clock edge sampled, the card can enter an undefined mode, that could lead to a locked state.
- A communication is on going on the interface: The pulse can corrupt the received byte, leading to communication error. A well designed communication error processing routine should reduce the effect of such case.

4.2.2 Design recommendations to limit interference effect

There are basic design recommendations within the current ISO/IEC 7816-3 [1] and TS 102 221 [2] specifications that exist to limit the identified potential issues that would at least create severe communication problems and in worst case lead to the card becoming mute to the terminal requests.

These could be split in two categories, interference limitation by the terminal design and interference resistance by the card/silicon design.

4.2.2.1 I/O routines and error detection

From previously identified effects of interference on the I/O pin, it could be concluded that communication errors have to be carefully taken into account for the I/O routines design:

- Parity checking and retransmission request in T=0 have to be handled on both sides;
- The terminal and the card could potentially receive unexpected characters and should discard them;
- Even if all care is taken, the terminal and card may not detect all communication corruption, as current parity check do not cover multiple bit value corruption.

The last point is the most critical, as it is highly impossible to protect against it when using T=0 protocol. T=1 protocol implements redundancy checking on blocks (LRC or CRC) and provides a better fault detection. From that aspect, T=1 may then be preferable to increase communication robustness.

However corrupted bytes could still be processed by the card. The terminal should then be tolerant to error messages such as for example 'class not supported' or 'instruction code not recognized'. In this case, the terminal should perform retries rather than consider the card as faulty.

4.2.2.2 Terminal design

The major source of interference is the terminal transmitter section. The emission power cannot obviously be reduced to decrease the interference strength, but experience has proven that the card reader design and position has a major impact on the interference pattern. It is worth noting that a voltage drop to RF interference does not depend on the card power supply voltage: The lower the power supply voltage is, the higher the noise to signal ratio and the more critical the interference are.

The impact of a particular reader design and position on the terminal PCB could then be tested and validated, and if necessary reworked.

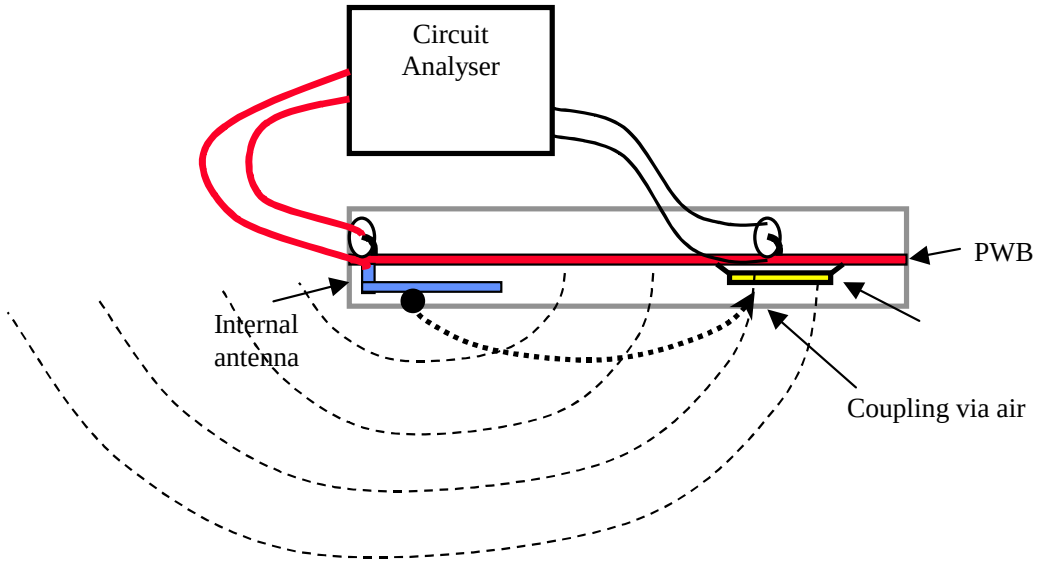
Two tests could be thought. The first test would allow to measure the RF conductivity between the terminal antenna and the card. The second coming at the very end would measure the existing operation margin between normal field RF power and extreme test RF power. This test should anyway be realized to correlate measured RF conductivity with interference problems: The absolute conductivity value is of a limited interest if its effect on interference strength is not known.

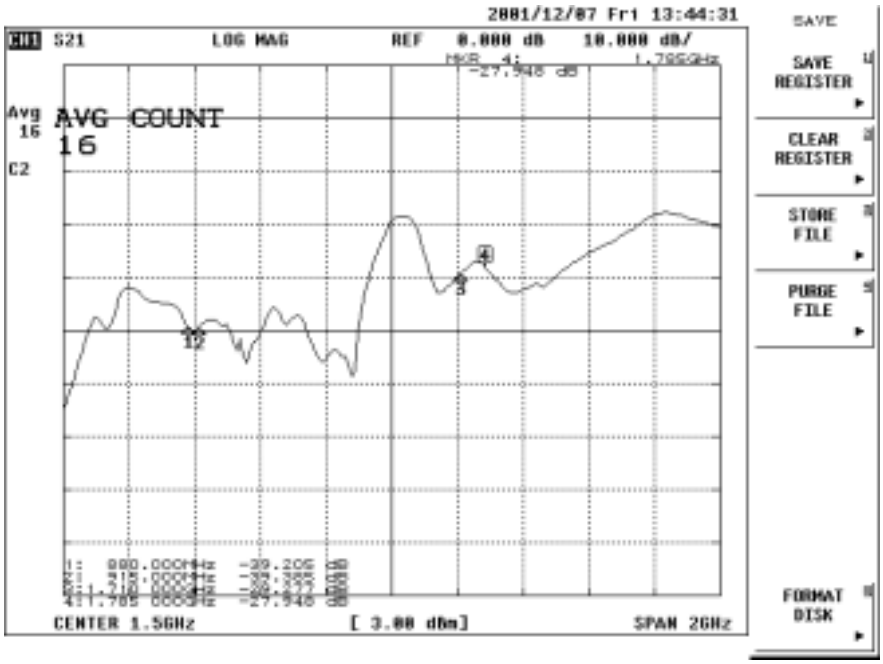
4.2.2.2.1 RF conductivity from transmitter to card

This method is used to identify the critical frequencies that may cause the interference. The purpose of this measurement is to measure the S21 parameter between the terminal PA and the card I/O line. The measured value, attenuation will give an indication of the interference sensitivity of the terminal.

The S21 parameter is measured over the TX band and a frequency response graph is the result. This measurement is repeated with the terminal placed on a non conductive and on a conductive surface, to observe the difference in frequency response. Both the attenuation and the critical frequencies will change when the terminal is placed on a conductive surface.

For the measurement a vector analyzer is required, equipment that can measure the S21 parameter. The measurement equipment output is connected to the terminal antenna and the input is connected to the card I/O line. The measurement equipment scans the specified frequency band, terminal TX bands, and a response graph is produced. It is important that the terminal PA is disconnected from the antenna when the measurement equipment is connected as the PA will have an impact on the measurement result if connected in parallel. The measurement setup as well as obtained graph are described below.

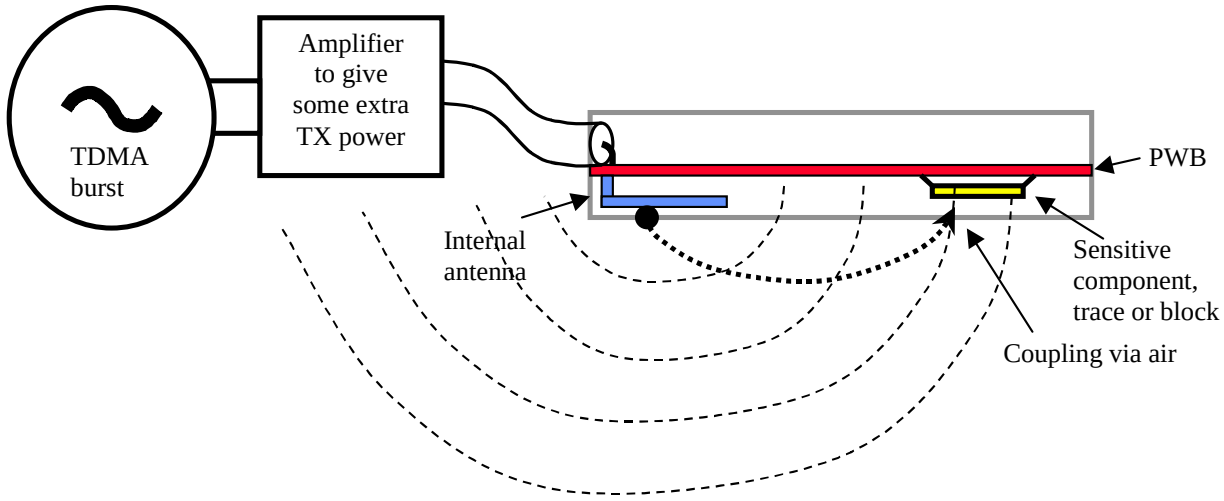




The S21 parameter should be particularly watched for the TX RF frequencies.

4.2.2.2.2 RF power level causing transmission problems

Based on the previous measurements the critical frequencies found are used for this test. The purpose of this test is to figure out at which power level fed to the antenna the interference on the I/O line will cause communication problems. The power is fed from a TDMA source through an amplifier with variable gain. The RF power is fed to the antenna of the terminal and the power level is increased until communication problems are seen when operating the terminal-card interface. The power level is noted. This test is performed with the terminal on a non conductive and a conductive surface, in order to see the impact of the coupling through the conductive surface.



Measurements with this setup shows that there is a difference in interference tolerance between different cards in the same environment. It also shows that it is a difference between environments, i.e. different terminals.

Measurements shows that with proper reader design, location of the reader and interface design RF power levels in excess of +40 dBm, 900 MHz, +37 dBm, 1,8 GHz, are needed in order to cause interference on the terminal-card interface to such an extent that the communication is aborted, the card is reset or rejected. Parity errors may of course occur at lower power levels and it is depending upon the implemented recovery procedures in the terminal this may not be visible to the user.

Correlated with the S21 parameter measurement, this test could give an indication of the conductivity/attenuation values that need to be targeted to insure proper operation, and then decide on further iteration that may be applied to the reader design and position.

4.2.2.3 Card silicon design

An interference occurring when the card is in idle mode may happen that could drop the I/O pin to the low level. If the clock is running, it will be processed as a character, and normal error processing should take place.

However, if the clock is stopped, the falling edge of the I/O pin should be discarded to maintain the card in idle mode.

A design recommendation for the card silicon would be to sample the I/O with the CLK signal.

5 Further improvement to the interface robustness

In the previous section, methods have been listed that increase the interface robustness within the current specifications scope.

Apart from optimizing the reader design and position in the terminal, another possibility to decrease the interference level is to strengthen the I/O logical high signal level. This could be achieved through implementing a lower impedance buffer to assert the high level on the line, and/or through decreasing the I/O signal intrinsic noise sensitivity.

5.1 Decreasing the suggested pull-up resistor value

Current specification recommends a 20k value for the I/O pull-up resistor.

Implementing a lower value will decrease the voltage drop created by the interference, but will also increase the power consumption of the card during communication. This should be done on both sides, that is in the terminal as well as in the card silicon.

5.2 Using a low impedance driver on the high side: Push-pull driver on the I/O line

This would have an even better efficiency than previous solution, as the driving impedance becomes by design far lower than any pull-up resistor. This method requires changes in the standard, and may be applied for all or only selected interface status.

- Push-pull driver active during card idle state: This is where the card is most of the time. Clock should be stopped, and the card expects a wake-up procedure from the terminal. In this state, the terminal asserts the I/O to the high level through a low impedance driver.
- Push-pull driver active during terminal to card communication: This would reduce the risk of communication errors during terminal to card data exchange.
- Push-pull driver active during card to terminal communication: This would reduce the risk of communication errors during card to terminal data exchange.
- Push-pull driver active during card operating state: This is the second most used state. The card is processing a command and the terminal expects a response from the card. In this state, the card asserts the I/O to the high level through a low impedance driver.

The changes to be applied in the standards will have to take into account:

- The buffers protection against bus contention. The potential use of a series resistor to reduce the current during the bus conflict.
- The backward compatibility, and in particular, if necessary the process of selecting the push-pull drivers.

5.3 Using different voltages for bus and card operation

Keeping a "high" operation voltage for the bus intrinsically increases the voltage swing between low and high logical levels, thus increase the noise robustness.

This can be achieved through two methods:

- Introducing an additional power supply line that will be used to reference the interface levels: This needs an additional pad to be defined. The interface voltage shall be used for all interface signals, I/O, RST, CLK.
- Keeping a "high" power supply voltage: The provided power supply voltage may not necessarily be used inside the card silicon, as the trend in card silicon technology is to use voltage regulators to decrease the internal operating voltage and level shifters on the I/O to adapt the internal and external voltages.

A consequence on the terminal design would be to keep a higher voltage for the interface or the card external power supply. In the latter case, the current consumption is not expected to increase as the card internal operating voltage is becoming independent from externally provided voltage.

5.4 Using differential data signals

Another way of increasing noise robustness is to implement a differential I/O bus. This solution is probably the most efficient. Its implementation from the specification side is not more complicated than the push-pull driver, although a second I/O pad is necessary for the D- pin.

From a hardware implementation point of view, it will mean major changes to the current I/O structure realized in the interfaces silicon.

6 Summary of failure mechanisms and countermeasures

The following table summarizes the various failure mechanisms and the identified countermeasures. It also goes through the expected countermeasure efficiency and applicability.

Failure type	Countermeasure	Efficiency	Changes in specifications and standards	Remarks
Contact on RST	Pull-up on RST signal in the card silicon	Good	No	
Contact on CLK	CLK signal pulled to the clock stop preferred level in the card silicon	Good	No	
Contact on I/O	Pull-up on I/O signal in the card silicon	Good	No	Additional coverage by error processing routines
Interference on RST	N/A			
Interference on CLK	N/A			
Interference on I/O	Optimize reader design and position in the terminal	Fair	No	Only a recommendation. Problem may still happen at low voltage classes
	Lower I/O pull-up resistor in the terminal and/or the card silicon.	Fair	No	Increase power dissipation during communication Problem may still happen if reader design not optimized and with low voltage classes
	Keep high "operating voltage" e.g. 3 V or 1,8 V (tbd)	Good	No	Complementary with other improvements. 1,8 V terminals already on the field: if applied, would prevent the usage of lower voltage classes.
	Push-pull buffer on the terminal	Good	Yes (protection for bus contention)	Associated with strong error processing, covers most critical issues.
	Push-pull buffer on both sides	Good	Yes	Covers all issues
	Introduce a separated interface power supply, kept at a "high" level e.g. 3 V (tbd)	Good	Yes	Complementary with other improvements Additional pad necessary Only low current load on the high voltage
	Differential data signals	Very Good	Yes	Covers all issues Additional pad necessary

7 Conclusion

Contact problems on the card pins can be covered by the implementation without changes to the specifications. However, noise immunity of the I/O signal is a real concern. Investigations have proven that careless design could create genuine field issues that may become critical while going to lower voltage classes.

The current interface can be significantly improved from a robustness point of view. Improvements will have an impact on both terminal and card.

None of the identified improvements would cause compatibility problems.

Some of the identified improvements do not require any change in the specification. These should be seen as good design practice, some may show limited effect when lower power supply voltages will be used.

Several steps can be identified to increase the interface robustness.

Step #1: Each of these items can be implemented separately, with no or minor changes to the specifications and standards

- Reducing the interference level becomes an additional design goal for the reader;
- The terminal actively drives the I/O high during card idle state and clock stop mode;
- The card samples its I/O with the CLK;
- Lower pull-up values are used, in the terminal as well as in the card silicon;
- T=1 protocol is preferred: it offers better error detection/correction.

Step #2: These will need significant changes in the standards, thus further discussion:

- The I/O buffer is changed to push-pull: better immunity;
- A separated power supply is provided to the interface: better signal to noise ratio;
- Another bus type is used - e.g. differential - that may facilitate other features implementation.

As a conclusion, it is recommended that Step #1 measures are applied to secure short term operation, and Step #2 solutions are worked on to prepare a safer longer term interface.

History

Document history		
V3.0.0	June 2003	Publication