Safe Wireless Communication Solution for Driver Machine Interface for Train Control Systems

Jesper Grønbæk, Tatiana K. Madsen, Hans Peter Schwefel
Institute of Electronic Systems, Aalborg University
Neils Jernes Vej 12, 9220 Aalborg Øst, Denmark,
e-mail: ljg, tatiana, hps @es.aau.dk

Abstract— This paper presents a design for safe wireless communication solution to be used for data transmission to and from a Driver Machine Interface that is a part of a train control system. Introduction of a wireless interface can significantly simplify the maintenance operations of a DMI since no physical detaching and cabling of the component is required. However, since wireless support is becoming a part of the DMI, it shall exhibits the same safety characteristics as DMI. It implies challenges in the design of the wireless communication protocol stack and requires a special-purpose Safety Layer. The paper presents a proposed network architecture, together with the description of the protocols, where the special attention is on wireless security, session control and fault management. The initial measurement results are presented.

I. INTRODUCTION AND MOTIVATION

Wireless technology is expected to impact to a great extend industrial control and monitoring. Elimination of wires as the physical layer to carry data is often referred to as cable replacement. Cable replacement has clear advantages in installation and maintenance cost reduction, and ease of installation. However, error characteristics of wireless links and communication latency makes this task nontrivial. Although we are witnessing fast deployment of wireless networks, their applicability in industrial environments has been limited so far. The emphasis in developing wireless networks is on speed and coverage. In the context of industrial control and monitoring applications, the throughput requirements are much more relaxed but the operating conditions are harsher [1]. On the contrary, the requirements for reliability, adaptability, and safety play the main role.

Many industrial applications require high safety level. Examples of such applications are aircraft and vehicle systems. In these examples, a system typically contains a distributed network with multiple vendor software and hardware and potentially multiple communication interfaces. The design of safety-critical systems is becoming increasingly complex. Many industries are in the process of setting, or have already set, specific standards for the development, testing and certification of safety critical equipment. In order to design a safe system the possible hazards should be identified and it should be determined how to remove the hazards or to reduce the associated risk to the acceptable level. The IEC 61508 standard [2] introduces four integrity levels. An integrity level indicates a criticality level of a system based on the severity of a potential catastrophe and the probability of its occurrence. Speaking about safety, one should clear understand the difference between the terms safety, reliability, availability and security. Reliability concerns with making a system failure free; a safe system may fail as long as it fails in a safe way. Safety applies to avoiding conditions that can cause physical harm to humans or damage to or loss of equipment or property. Availability is defined as the proportion of time a system is in a functioning state. Non-functioning system is, of course, very safe, but useless. Availability, reliability and safety may imply conflicting requirements, and a system can not be designed maximizing them all. Additionally, security should be considered for many safety-critical applications, since malicious attacks can jeopardize system safety. However, in each particular case catastrophic consequences of different attacks, such as denial-of-service attacks, tampering attacks, or the need for authentication and confidentiality, should be analyzed separately.

In the evolution of industrial control applications we see growing usage of wireless communication. As wireless interfaces are becoming a part of system, there is a need to address network architecture design from the safety perspective to meet the requirements of system safety.

In this paper we present one particular example where wireless communication is applied to ease the operational procedure and to reduce maintenance cost in safety-critical environment. This example comes from railway systems and is connected with the development of safe Driver Machine Interface (DMI). The DMI displays information from the onboard train control system to the driver. The development of a DMI that can be classified at Safety Integrity Level 2 is the goal of the European project SAFEDMI (Safe Driver Machine Interface for ERTMS Automatic Train Control) [3]. Besides the development of a DMI architecture at a higher safety integrity level than currently available equipment, SAFEDMI project aims at providing the design for wireless support for maintenance operations. The proposed wireless communication solution should exhibit SIL2 characteristics as well.

The paper is organized as follows. Section II introduces the system under consideration and summarizes the system requirements. An overview of COTS wireless technologies and the discussion on their suitability in the considered scenarios is presented in Section III. Section IV elaborates on the proposed solution including wireless link security mechanisms. The measurement results of IPsec performance in the SAFEDMI
scenario are given. Concluding remarks are presented in section V.

II. SYSTEM DESCRIPTION AND REQUIREMENTS

Railway automatic train control (ATC) systems are based both on trackside and on-board systems. The increasing level of train traffic is now demanding an increasing safety level, at least Safety Integrity Level 2. Currently, all communication links of on-board equipment are wired. However, for some operations, such as software upload and data download for diagnostic purposes to and from Driver Machine Interface (DMI), it is highly desirable to introduce a wireless interface. DMI component is a part of the on-board ATC. Its main functions are the acquisition of driver’s commands and the display of those information that support the train driving. The introduction of wireless communication interface in DMI component will allow very quick DMI configuration and SW/firmware upgrade, avoiding mechanical operations. In fact a more traditional approach usually requires to extract the DMI itself from the driver desk, open some DMI panel to access an internal communication interface, proceed with the configuration/upgrade, close the DMI, and restore it into the driver desk. Wireless technologies obviously supply a faster way for maintainability.

![Fig. 1. Scenarios for wireless communication with the DMI.](image)

The usage of SAFEDMI’s wireless interface is envisioned for the following two operations: maintenance, resulting in file uploads to DMI, and diagnostic, resulting in downloading of smaller portions of data from DMI periodically or by a request. Data download and file upload for configuration can be performed in the following three scenarios (Fig. 1):

- **Short-range wireless domain**: The train is stationary at a maintenance site where a dedicated wireless network infrastructure may be established to enable communication with the remote centre. The maintenance site may be a train depot, a train station or a test track.
- **Long-range wireless domain**: The train is stationary or moving outside the maintenance site for example at an open railway track. Special requirements for long-range wireless network systems may be required. In the open track environment dedicated wireless equipment may not be available, i.e. existing wireless long-range infrastructure networks would preferably be used as a link between the train and the remote center to minimize establishment costs.

- **On-board wireless domain**: Independent on the train location an on-board operator may make use of mobile equipment like a laptop to connect to the DMI. This scenario could imply the use of the same dedicated wireless technology as in scenario I for the connection.

The focus in the proposed design is on the maintenance operation in scenarios I and III. However, with little or no extension the same solution for wireless communication can be applied for scenario II.

A number of functional and non-functional requirements for wireless communication solution have been identified [4]. The wireless requirements can be classified in several groups:

- **Availability and performance**: Wireless interface shall be available for software uploading and data download. A maintenance operation shall be completed in 5 min. Additionally, direct connection using cables with SAFEDMI shall be available for use when the wireless interface is unavailable (e.g. due to interference, spectrum jamming or instantaneous bad channel conditions).

- **Open communication system**: since a wireless communication link presents an open system, the wireless interface shall be compliant according to the CENELEC standard EN 50 159-2 [5].

- **Integrity verification**: file uploading shall be compliant according to the SIL2.

- **Safety**: Wireless transmission shall not affect other safety-critical transmissions. Additionally, separation of safety-related and other functions in SAFEDMI shall be done.

- **Authentication**: requirements on the characteristics of an authentication mechanism have been added to the list of the requirements, e.g. defences against DoS attacks and making brute-force login attempts less likely.

- **Operation separation**: only one operation can be performed at a time.

III. COTS WIRELESS TECHNOLOGIES AND PROTOCOLS

The motivation for using COTS components (Components of the shelf) is that they will reduce overall system development costs and involve less development time. As alternative to COTS, in-house developed products are not available to the general public and, thus, using in-house devices the risk of malicious attacks can be somewhat reduced. The goal of the SAFEDMI project is to show the feasibility of usage of wireless links (cable replacement) in scenarios connected with SW upload and download of data for diagnostic. For this purpose, we are choosing one (or more) of the currently available technologies and protocols for wireless communication.
While making a choice of a COTS wireless technology, several factors should be taken into account, such as achievable data rates, coverage, licensed/ non-licensed spectrum and sustainability to interference in the later case; usage of forward error correction (FEC) codes; embedded security mechanisms and availability on the market. Data rates gives an indication if a technology can potentially fulfill performance requirements of SAFEDMI scenarios. Coverage parameter shows to what extent a technology can be applied in scenarios: short-range and long-range scenarios. High interference level or high level of congestion among different users of a shared wireless medium can lead to degradation of performance and increase data upload/ download time and, in worst case, it can lead to non-availability of wireless interface. Error correcting codes are used to overcome or reduce the impact of channel errors. However, these codes cannot provide a perfect protection and some amount of residual errors pass through undetected. This can be a serious issue that can potentially affect the safety level of a designed system. Additionally, a wireless medium is an insecure communication channel and some of the technologies incorporate security mechanisms, typically link security. Furthermore, for our development we would like to choose a mature technology that is commonly available on the market.

Some of the currently widely deployed and used wireless technologies are presented in Table I. Depending on their coverage range, their suitability for different scenarios is shown. The applicability of the presented technology will largely depends also on their ability to provide sufficient data rates. The performance requirement states that the operation (maintenance or diagnostic operation) shall be completed in 5 min. Typically a software upload will consists of approx. 20 files 2 MB each, and the size of downloaded data for diagnostic purposes can vary from 20 byte to 400 byte. Considering introduced protocol overhead, packet fragmentation and possible retransmissions on lower layers, the efficient link layer throughput of approx. 1-2 Mbps is required for maintenance operation and about 10-50 Kbps for diagnostic. Basically, it is only WLAN IEEE 802.11 and possibly WiMAX that can live up to the high data rate requirement for maintenance operation. The maximum data rate of WLAN 802.11 a and g is 54 Mbps, nd for 802.11b it is 11 Mbps. Mobile WiMAX (IEEE 802.16e) is planned to support data rates up to 500 kbps. Therefore, software uploading is only commenced at maintenance sites where a sufficient short range/high bandwidth wireless infrastructure is established.

Speaking about on board and short range scenarios, we should note that both Bluetooth and ZigBee have been created having in mind energy-efficiency of communication and they are optimized to minimize energy consumption. Energy-efficiency plays an important role when a device possesses unchangeable batteries or if it should operate for days or months without recharging. This is not the case in the SAFEDMI context where sessions are considered to be of limited duration and where there is a possibility to use constant power supply. This indicates that Bluetooth and ZigBee are suitable for occasional or periodic transmission of small portions of data, as in diagnostic operation. WLAN 802.11 is suitable for the maintenance operation. Additionally, WLAN 802.11 presents another advantage by providing a cost-efficient and well known solution of establishing a wireless infrastructure consisting of multiple access points.

A major problem with using unlicensed frequency bands such as 802.11x is obviously the interference on and shared access of the wireless medium. If these aspects become dominant blocking the desired services, switching to another communication interface can solve this problem. Multiple wireless interfaces will increase system cost, but can help to improve system availability greatly. It can be recommended to use a simple option enabling an Ethernet interface to DMI.

There exists a specially developed solutions, such as GSM-R (GSM-Railway) [12] for railway communication. It is based on GSM technology and is a part of the European Rail Traffic Management System (ERTMS) standard. GSM-R is deployed along the railway lines and gives the excellent coverage for trains even in the rural areas and in the tunnels. However, the capacity of GSM-R is limited, and already now it carries a substantial amount of traffic, that is expected to increase even more in the future. Therefore, this kind of technologies has not been excluded from Table I.

The technologies presented in this section are typically specifying physical and data link layers. While the choice of data link layer is dictated by a choice of a particular wireless technology, the proper higher layers protocols should be selected for the SAFEDMI architecture. Typically used COTS protocol suit TCP/IP is designed keeping in mind unreliability of transmission medium: packets can get lost or corrupted. Mechanisms such as acknowledged transmissions and redundancy checks can solve this problem. However, while they are efficient against accidental transmission errors, they can not provide protection against malicious attacks. This is a task of cryptographically based security. Security mechanisms can be implemented at different layers of the protocol stack. Examples are IP security (IPsec), Secure Shell (SSH), Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols. In our work we have limited our considerations to IPsec. The detailed discussion on IPsec and it’s role in the overall design is provided in the next section.

IV. PROPOSED WIRELESS COMMUNICATION SOLUTION

The challenge in designing the protocol stack to be applied in SAFEDMI scenarios is to achieve the high safety level, while guaranteeing availability and performance and keeping

<table>
<thead>
<tr>
<th>Scenario</th>
<th>On board operator</th>
<th>Short range</th>
<th>Long range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance</td>
<td>WLAN 802.11 [8]</td>
<td>WLAN 802.11</td>
<td>WiMAX [9]</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>ZigBee [6], Bluetooth [7], WLAN 802.11</td>
<td>Bluetooth, WLAN 802.11</td>
<td>WiMAX, GPRS [10], UMTS [11]</td>
</tr>
</tbody>
</table>

TABLE I

APPLICABILITY OF WIRELESS TECHNOLOGIES IN DIFFERENT SCENARIOS
the solution simple. We follow the traditional layered approach of computer networks. Off-the-shelf protocol components will be used to facilitate the development and deployment processes. However, the generally used protocol suites for data delivery over a network, such as TCP/IP or RTP/UDP/IP, do not address safety issues. There is a need for an inclusion in the protocol stack a special-purpose layer that we refer to as Safety Layer (SL). The purpose of SL is to guarantee connection establishment, data transfer and connection release that fulfill safety requirements for wireless communication stated in [4].

The wireless communication links are classified as open communication systems according to the CENELEC standard [5]. In order to achieve a required safety level, a proper defences against malicious attacks and measures to avoid e.g. packet re-sequence should be applied. These protection mechanisms are known to be resource-consuming. Therefore, in order to fulfill the requirement on the separation of safety-related and other functions in DMI component, we propose to divide a DMI system into two subsystems: one sub-system is a DMI itself and a second sub-system is a Bridge device that is connected to DMI via Ethernet (Fig. 1 and Fig. 2).

A. Wireless Link Security

A common trend evolving networking systems like Next Generation Networks (NGNs) is to move from proprietary solutions to IP-based services, protocols and equipment [2]. This improves system interoperability and reduces cost. A COTS solution to security in IP networks is IPsec. IPsec is a set of open standards developed by the IETF and documented in RFC 2401 and related RFCs [28]. IPsec is a mandatory part of IPv6 and it is optional for use with IPv4. It provides encryption and authentication at the network layer to protect IP packets between IPsec compliant devices independent of the overlaying applications. A strength of IPsec framework is its versatility to fit a large variety of security requirements and deployment scenarios. However, this versatility is also argues to be the greatest weakness of IPsec [15]. For instance known attacks to IPsec solutions are based on wrong configuration and implementation issues [14]. In the SAFEDMI wireless design the IPsec versatility is not offered to end-users. Instead a secure IPsec configuration is a central part of the design. This is possible as the use case scenarios are pre-defined and not expected to change in the given communication system architecture.
Supplying a proper configuration for IPsec is an issue of required security features and the associated risks of attack occurrences and consequences. This is further related to the resources required to enable the security functionality. Table II contains the configuration chosen to provide a secure wireless channel between the DC and the BD.

Different IPsec configuration policies enable negotiation of used security functions between hosts with different capabilities. However, in this setup all hosts are controlled and the desired state-of-the-art security functions are made available.

To quantify the resource impact of adding the described security functions basic performance analysis has been conducted. The aim is to examine the performance impacts of adding the suggested security solution.

**Test setup**

The test environment is depicted in Figure 3. The DMI and BD are mediocre x86 based PC systems corresponding to embedded systems with limited performance capabilities. To consider a worst case analysis the bottleneck system is the BD itself. It has fewest resources while it must execute cryptographic algorithms in the communication toward the DC. The DC must perform the same functions but is however assumed to be a powerful systems with capabilities exceeding the BD. Thus, focus is on considering the end-to-end performance characteristics between the DMI and DC considering resource consumption of the BD.

**Baseline performance**

The baseline performance of the systems has been established without IPsec enabled. In the BD a static route has been defined that forwards packets from one interface to the other. Only wired links are used to establish performance measurements without considering the unreliable conditions of a wireless link.

An FTP connection is established between the DMI and the DC. Next a 40 MB file with random bits is uploaded from the DC to the DMI in 100 attempts. The transfer time consumed in each attempt is used to calculate a mean goodput. The baseline performance results are shown in Table III. In this case the mean goodput is restricted by the bandwidth of the 100 MBit ethernet links. Notice, the BD CPU is busy forwarding packets but not fully utilized.

**IPsec performance**

The same measurement approach has been used with the IPsec functions enabled. The results for varying key sizes of the AES encryption algorithm are also depicted in Table III. Clearly, a significant performance impact in the goodput is seen from the added IPsec functions. The BD CPU is fully utilized and is thereby likely to be the bottleneck component. Despite the fact that goodput performance is reduced to $\frac{1}{3}$ with IPsec in the given setup, this may not be a significant issue compared to the actual performance requirements as described in section III. However, more BD throughput may be required if additional data overhead for integrity and error correction functions are added on layer 3 or above. A solution to performance problems is in this case to increase the BD performance. As hardware accelerated security functions are emerging in cost-efficient processing solutions[17], employing IPsec may be associated with a low cost.

Finally, quantifying encryption security for different key sizes is difficult. In relation to NSA [16] AES key sizes $\geq 192$ are considered sufficient to provide 'TOP SECRET'-level security. However, from the achieved results the performance impact of doubling the key size from 128 to 256 is not dramatic in this setup.

**B. Key Management**

Secret keys need to be established for encryption, origin and integrity check functions. The IPsec open standards do not specify how keys are established. RFC 4306 specifies IKEv2 which is a protocol for Internet Key Exchange referring to

---

### Table II

**IPsec Configuration Used for the LOWSL Safe Communication.**

<table>
<thead>
<tr>
<th>Requirements</th>
<th>IPsec Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP</strong></td>
<td>IPv4</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>ESP using AES-CBC to provide strong standardized encryption.</td>
</tr>
<tr>
<td>Protection against data insertion, re-sequencing, corruption, masquerade, deletion</td>
<td>Data integrity and origin checks are provided in ESP with HMAC using the cryptographic hash function SHA-2.</td>
</tr>
<tr>
<td>Repetition/replay protection</td>
<td>ESP with packet sequence numbering.</td>
</tr>
<tr>
<td>Host-to-host security</td>
<td>Transport mode where original IP headers are maintained. This mode is designed for host-to-host solutions leading to less overhead compared to tunnel mode which is typically used between routing devices.</td>
</tr>
</tbody>
</table>

### Table III

**Communication Performance Characteristics with and without IPsec.**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Mean goodput</th>
<th>BD CPU utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>No IPsec</td>
<td>11.1 MiB/s ($\sigma = 0.0041$) $\approx 75%$</td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>2.57 MiB/s ($\sigma = 0.00028$) $\approx 100%$</td>
<td></td>
</tr>
<tr>
<td>128bits key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>2.50 MiB/s ($\sigma = 0.0001$) $\approx 100%$</td>
<td></td>
</tr>
<tr>
<td>192bits key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>2.36 MiB/s ($\sigma = 0.00035$) $\approx 100%$</td>
<td></td>
</tr>
<tr>
<td>256bits key</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPsec: For HMAC-SHA-2 a constant key size of 256bits is used.**
IPsec and session key establishment over unsecure network paths. The concept of session keys is referring to temporary short term keys that are only used throughout the lifetime of a session. In SAFEDMI a session is defined from a DC establishes a connection to a DMI, performs some operations and until it closes the connection. Thus, a session may have a duration from a few minutes to a couple of hours. The session key \( k_{s} \) is a common secret known by the two communicating peers. Using Diffie-Helman key exchange such keys can be created safely by the two peers in their exchange of public keying material in an unprotected channel [18]. Session keys do not provide authentication of peers. For this purpose Long Term (LT) keys are needed. LT-keys are only used in an initial authentication process protecting them from exposure in the unprotected channel. In SAFEDMI LT-keys are required to be protected in hardware. This provides increased key protection even if an attacker would get physical access to a secure device. As a design choice LT-keys are stored in the DC and DMI respectively. However, the secure channel is created between the BD and DC. Thus, the BD must include the DMI in the authentication process. This collocated key approach requires a modification to IKEv2. A similar method is used in 3GPP cellular systems. Here, a mobile phone is still authenticated in relation to its home network even when it operates in a visited network.

Following different common approaches to provide LT-keys are discussed in relation to the SAFEDMI solution.

- **Pre-shared (symmetric) keys**: Such keys are simple to setup for small systems with a small amount of nodes. However, a unique key-pair is needed for each association between two devices. With multiple trains (DMIs) and multiple portable and remote DCs this becomes unmanageable. In addition, solutions to securely protect user defined keys in hardware may be difficult to establish.

- **Asymmetric keys**: Using asymmetric keys a peer, e.g. the DC, can use the shared public key of the other peer, the DMI, to encrypt information only the designated DMI can decrypt using its private key. Similarly the DMI can encrypt information only the DC can decrypt. Providing hardware solutions for such an authentication method is widely available today. In PC systems mainboard manufacturers implement Trusted Platform Modules (TPM) chips. Such chips are at production created with an asymmetric key pair. The private key cannot be read outside the chip itself leaving it well protected.

- **Third party trust**: Asymmetric keys themselves do not ease key management. Peers still need to be pre-configured with each others public keys. To improve this situation a trusted third party may be introduced. A trusted third party can sign public keys of peers. Thus a DMI or a DC may dynamically retrieve public keys from each other and use the trusted third party signed value to establish a trust in, and authenticate, each other. Thus, DMIs and DCs do not need to know each other in advance. This eases key management significantly.

For more information on IKEv2 and key management see [18].

Simple performance measurements of IKEv2 key establishment have been performed in the setup described in Figure 3 (without collocated authentication). The aim is to quantify the secure session establishment delay introduced by IKEv2 and the DH-key establishment process. The algorithm of DH uses keying material \( DH_{seed} \). A \( DH_{seed} \) size of 1024 bits is considered to provide high security. Using this configuration to generate 256 bits symmetric session keys, the duration of key establishment is approximately 3 seconds where around 12 messages are exchanged. The delay in session establishment is clearly bound to increase for high latency channels like in UMTS. However, the delay measured in seconds should be seen in relation to a session duration of several minutes. Thus the establishment of session keys is expected to have a limited impact in relation to timely requirements.

C. Session Control and Fault Management

The communication flow to and from DMI should not affect the safety of the system. Therefore, one of the important component of the HighSL is Session control mechanism that manages end-to-end session. It’s tasks are to ensure that connection is established, maintained and closed gracefully in case of faults. Session control uses information from performance monitoring component to handle predictions of bad wireless conditions. This is needed for several reasons:

- to avoid too many errors to be corrected in higher layers;
- to make it possible to inform users/system administrators when problems occur in the wireless environment.

Examples are notification about high level of noise or interference making communication impossible or intrusion detection.

Verification of data integrity is conducted at the application layer. However, to guarantee the successful completion of this operation, residual bit errors should not exceed a predefined threshold (depending on the type of codes used). Therefore, a performance monitoring component should provide estimation of the residual Bit Error Rate (BER) to the session control and the later will close the session and switch off the wireless interface in case BER exceeds the threshold . There exists several methods for an estimation of the current wireless channel BER. One class of methods compute BER using pilot symbols. Pilot symbols represent a predefined sequence of symbols, which are known at the transmitter and receiver side. However, the transmission of the pilot symbols introduces overhead. Additionally, BER is computed over a small amount of the total bits that are transmitted and, therefore, can lead to an inaccurate estimation. Other approaches are based on the modelling the channel with all the effects that cause the disturbance of the wireless channel. But it is questionable if estimation of the exact quality of the signal of the wireless channel is possible at all, since each model has its limitations. A possible approach is to provide worst case BER estimation based on other performance metrics available, such as...
packet error rate and signal strength, and as a function of the modulation schemes used. Currently, we are evaluating different approaches for performance monitoring in terms of their applicability in SAFEDMI scenarios.

V. CONCLUSIONS

This paper presents one particular example of a cable replacement by a wireless link in a safe-critical system. It is shown that in order for the wireless interface to exhibit high safety characteristics, it is necessary to introduce a special-purpose Safety Layer in the COTS protocol stack. The applicability of different wireless technologies, such as WLAN 802.11, and different COTS protocols, such as IPsec, for the considered scenarios is discussed.

VI. ACKNOWLEDGEMENTS

This work has been undertaken as part of the SAFEDMI project which is funded by the European Commission (contract 031413).

REFERENCES

[17] VIA Technologies, Inc. VIA C7-D Datasheet