Simulating and Modelling the Impact of Secure Communication Latency for Closed Loop Control

R.D.Sparrow, A.A.Adekunle, R.J.Berry and R.J.Farnish
The Wolfson Centre for Bulk Solids Handling Technology,
University of Greenwich,Chatham Maritime,
Chatham, Kent ME4 4TB, England, UK
{r.d.sparrow, a.a.adekunle, r.j.berry, r.j.farnish} @gre.ac.uk

***Abstract*—Closed loop control systems have been implemented to conduct a variety of tasks (e.g. manufacturing and automation). Industrial Control System (ICS) have been used to regulate a closed loop process; however, ICS are exposed to the same security vulnerabilities associated with enterprise networks. Cryptography has been deployed to overcome the associated data communication weaknesses between each ICS node through the use of block ciphers; however, the drawback of applying cryptographic algorithms to ICS is the additional communication latency. This paper investigates the relationship between security constructs and latency for closed loop control system with test conducted in a simulated environment. A case scenario is illustrated to demonstrate the impact of the results obtained to a real world context.**

***Index Terms*—closed loop control, real-time systems, computational constraints, security constructs**

I. Introduction

Closed loop control systems are implemented in a variety of sectors to provide feedback from a set process. With closed loop control providing autonomous actions based on feedback from an actuator, this method is suitable for monitoring a continuous process without human intervention. Closed loop control has commonly been identified in Industrial Control Systems (ICS) (e.g. computer aided manufacturing). With devices becoming interconnected, one of the most challenging aspects of ICS is the exposed security vulnerabilities, this is due to the increase of cyber crime and availability of open designs [1].

Increased threats to ICS are also becoming more frequent [2] with statistics reported indicating that cyber attacks against control systems has increased. The System Administration Networking and Security Institute (SANS) survey indicates a minimum of one or two security breaches against ICS has occurred within the past twelve months [3]. Safety of industrial networks is critical as undetected corruption of data packets during transmission can cause damage to equipment, environment and human health [4]. This paper investigates how software based security algorithms using block ciphers impact the overall communication latency of closed loop control systems. A mathematical model is proposed to aid practitioners to predict the effects of security constructs on closed loop control systems without the requirement and cost of implementing an experimentation platform.

The structure of this paper is organised as follows: Section II introduces the terms and phrases discussed in this paper. Section III discusses a system safety case scenario with Section IV reviewing relevant literature. Section V discusses the experimentation procedure with Section VI analysing the results obtained. Section VII introduces the proposed mathematical mode with Section VIII conducting a comparative experiment of the proposed mathematical model against the simulation. Section IX examines the mathematical model as a predictive tool. Section X discusses the impact of the results to the context of the case scenario. Section XI concludes.

II. Preliminary

This section defines the terms used throughout this paper.

- *Real-Time Constraints:* is a computing system whose correct behaviour depends not only on the value of the computation but also on the time at which outputs are produced.
- *Non Real-Time Constraints:* is a computing system whose correct behaviour depends only on the value of the computation.
- *Latency:* The duration taken for data to travel from transmitter to receiver.
- *Confidentiality:* Confidentiality in this paper refers to using encipherment methods in order to thwart an unauthorised entity understanding the content of the payload of the data frames transmitted.
- *Integrity:* In this paper integrity is determining whether data has been altered in transit at the receiving node.
- *Authentication:* The proof that a device on the network is legitimately eligible to communicate with other eligible devices on the same network.
- *AEAD concept:* The Authenticated Encryption with Associated Data (AEAD) concept provides both confidentiality and integrity security data services to transmitted packetised data.

III. System Safety Case Scenario

The following section considers a scenario where a closed loop control system is used to automate a safety critical process. Dust explosions in bulk solids powder handling can result in personal injury or death and loss of plant. The adoption of legislation to mitigate the effects of such events is now widespread and many technical approaches can be applied to ensure plant safety. The scenario uses a suite of these counter-measures commonly found in industry. Figure 1 illustrates, the main components found in many plants (i.e. air mover, powder feeder, pneumatic conveying pipeline and reception vessel).

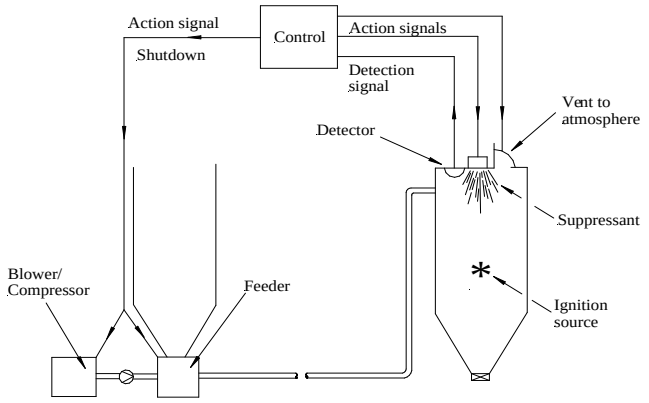

Figure 1. Schematic of a process plant for bulk solids powder handling

Best practice dictates that in the event of a rapid pressure rise being detected (i.e. the initiation of a dust explosion) a range of counter-measures should be activated. The energy released during a dust explosion is such that an over-pressure capable of destroying the plant can develop on average within a tenth of a second (e.g. polyester can attain a maximum explosion pressure of 6.1 bar at a rate of 85 bar/sec) [5] thus the response time for detection and actuation of counter-measures is a critical factor for the safety of staff and the safe operation of the plant.

IV. Literature Review

Section IV introduces literature relevant to the context of this paper with focus on confidentiality, integrity and authentication in closed loop control and methods of modelling utilised. The literature review is sectioned into three parts; firstly the current approaches undertaken by other researchers, secondly the introduction of the AEAD constructs and finally a conclusion of the literature undertaken. Ma et al focus on mechanisms for providing security to real-time systems; the authors propose the Adaptive Risk Control and Security Management concept (ARCSM) [6]. This approach targets current security vulnerabilities for insecure environments without compromising the real-time element of embedded systems. This is achieved by using a two tier feedback control framework on each node on the network. Experimentation conducted by the authors examine the time and energy required by cryptographic constructs and how this influences the operation of the embedded system. The results obtained from their research show that the ARCSM approach is better suited for open loop control with varying run-time performance; however, the security constructs tested in this paper only utilises legacy security constructs, raising questions to how contemporary cryptographic constructs would behave in this context. It is also noted that a high end specification ARM S3C2440 microprocessor was selected for experimentation.

A method to overcoming deception attacks in closed loop control systems is presented by Pang et al using their secure networked predictive control system (SNPCS) [7]. The research conducted by the authors provides confidentiality, integrity and authentication to data by using a software implementation of the Data Encryption Standard (DES), Message Digest version 5 (MD5) and a time-stamp. The Recursive Networked Predictive Control (RNPC) is utilised to compensate for the control system performance from the deception attacks. Experimentation was performed on an internet based control rig with results showing the implemented countermeasure was suitable; however, it is unknown whether this security approach is suited against other attacks vectors. The comparison between the authors method and other software security constructs is not explicitly explained. The implementation of a time-stamped authentication system is also a security vulnerability due to synchronisation of two time zones. An attacker could craft their own packet using the same time-stamp and spoof a legitimate device with the possibility of the packet still passing the authentication procedure.

Gupta et al [8] assesses the performance of data and time sensitive wireless network control systems with the presence of information security. The issues examined by the authors emphasise the security vulnerability of wireless broadcast to transmit data over the internet from the Network Control System (NCS) as the broadcast signal can be detected by anyone within range. This is further exposed as NCS had been designed without consideration of security in mind, allowing for the attacker to compensate the device remotely. A proposed solution by the authors uses security constructs DES and Triple Data Encryption Standard (3DES) operating in the Electronic Code Book (ECB) mode on a closed loop control testbed intelligent space (ispace). Results obtained suggest that the security constructs investigated have a slight impact on the timing of the closed loop control system with overhead of 9% to 18%. The focus of the research conducted by the au tours is for securing NCS traffic over the internet. The security constructs used are no longer standardised due to their known security vulnerabilities and the ECB mode of operation is also susceptible to known plain text attacks.

An approach undertaken by Dhand et al [9] examines the impact of communication delay on real-time distributed control systems. Current problems discussed by the authors focuses on the challenge of minimising delay within a

control loop and how time delays are not always specific to the controller alone but also from transmission and sensor delays. The solution presented in this literature uses the Auto-regressive Integrated Moving Average (ARIMA) to forecast the communication delay a control loop. Experimentation was performed using the national instruments Data Socket Transport Protocol (DSTP) at the application layer, the Transmission Communication Protocol (TCP) for the transport layer and Ethernet for the data link layer. Results had been acquired by using minilab 15 and Simulink. The impact of security constructs on the operation of real-time control networks has been overlooked as the focus of the model is for communication latency.

This paragraph introduces the AEAD concepts with two paradigms being presented; the fixed standardised approach of Counter with cipher block chaining (CCM) and the adjustable and flexible approach of TinyAEAD. CCM is a National Institute of Standards and Technology (NIST) standardised AEAD construct designed to provide integrity and confidentiality using a 128-bit block cipher [10]. The TinyAEAD construct is designed to provide confidentiality and integrity services using block ciphers of varying bit length [11]. This construct can be configured to run at a reduced specified number of block cipher iterations in order to enhance the processing speed of the construct. In addition TinyAEAD provides flexibility and adaptability that can be applied to a broad range of contexts.

Concluding from the literature review undertaken two areas have been identified as areas to conduct further research; firstly the requirement for test with modernised cryptographic constructs is required as the literature uses constructs that are no longer standardised. Secondly a mathematical model is required to predict and disclose the impact of security constructs on closed loop control systems as current models do not take this into consideration.

V. Experimentation Procedure

Section V discusses the experimentation procedure conducted and the apparatus selected. The simulation programme used is Proteus ISIS 8 professional with the Microchip PIC18F45K22 selected as the microcontroller of choice. The Serial Peripheral Interface (SPI) has been selected as the physical medium used to transport the data between microcontrollers. Software security constructs evaluated in this paper focus on variation of the Advanced Encryption Standard (AES) using a 128-bit key. Modes of operation examined were CCM and TinyAEAD. The selected closed loop control approach used is the Proportional-Integral-Derivative (PID).

The experimentation examines latency for a transmitting microcontroller to process and transmit the packet, the duration of the packet to propagate to the receiving microcontroller to process the received packet and perform the feedback action. The metric utilised for measuring the impact software security constructs on latency is measured in milliseconds. All timings are taken from the simulator used.

Packet sizes of 36, 52 and 84 bytes in length were sampled to mimic ICS protocols with SPI divisor of 4 to output the data at the fastest configuration setting. The crystal frequency sampled was 8 MHz to replicate a low frequency micro-controller. Finally it is assumed for this test scenario that the communication medium used to transmit between the microcontrollers uses copper cabling of 100m in length.

VI. Results and Analysis of Experimentation

This section analyses the data obtained from undertaking the experimentation procedure. Table I illustrates the latency for varying packet sizes using an SPI divisor of 4 without security constructs applied. Table I is used as a benchmark as the real-time operation of a closed loop control network without security.

Table I
Total simulated communication latency for a simulated single hop closed loop feedback link without security

Packet size (bytes)	Time (ms)
36 Bytes	180.4
52 Bytes	180.7
84 Bytes	181.7

Data in Figure 2 presents the communication latency generated by software security constructs for a 36 byte packet. The zero on the x-axis reflects the time recorded for no security for a 36 byte packet. It is inferred that the communication latency has increased with longer latency recorded for CCM and TinyAEAD at ten rounds, whilst TinyAEAD at five and three rounds had the smallest impact. TinyAEAD had the least latency overhead of 12% whilst CCM incurred an overhead of 29%.

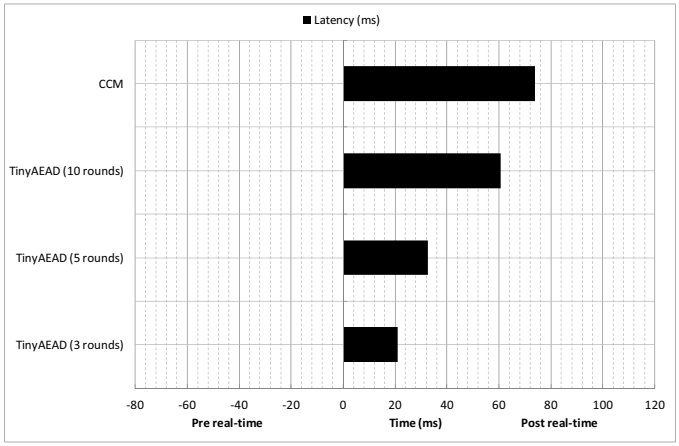

Figure 2. Simulated communication latency for a simulated single hop closed loop feedback link with security (36 byte packet length)

Figure 3 graphs the results using a packet size of 52 bytes. The security constructs examined have shown an increased

in the total communication latency with noticeable difference between TinyAEAD at three rounds and CCM. TinyAEAD at 3 rounds incurred the smallest latency overhead of 25% with CCM incurring the biggest latency overhead of 37%.

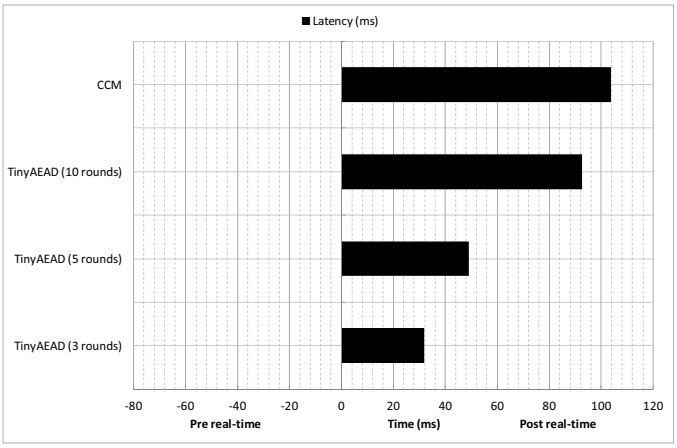

Figure 3. Simulated communication latency for a simulated single hop closed loop feedback link with security (52 byte packet length)

Figure 4 illustrates the impact of software security constructs using an 84 byte packet size. The graphs indicates that CCM and TinyAEAD both running at ten rounds has the biggest increase in the communication latency. TinyAEAD using three rounds has the least communication latency. Tiny AEAD at three rounds has the smallest impact on latency overhead with 33% increase, whilst CCM had the biggest impact on latency with 48% increase.

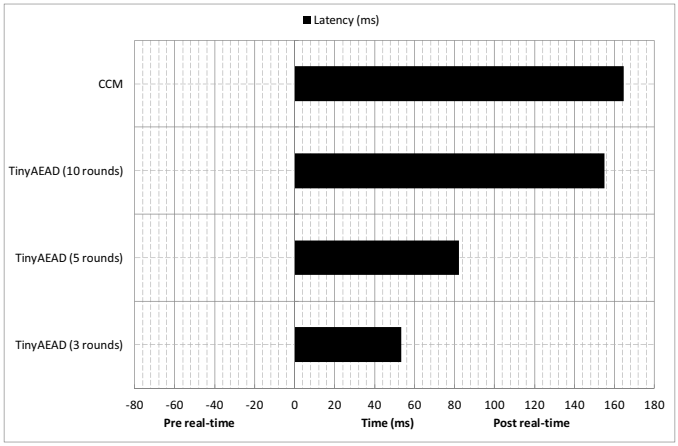

Figure 4. Simulated communication latency for a simulated single hop closed loop feedback link with security (84 byte packet length)

Analysing the results obtained from the experimentation adjustable cryptographic constructs are better suited to minimising communication latency in comparison to standardised constructs. Packet size also influences the latency generated with the smaller packet sizes processed faster than larger sized packet.

VII. Proposed Communication Latency Model

This section introduces the proposed mathematical model to calculate latency introduced by security constructs on communication link of closed loop control. The model is designed to take into consideration factors influencing the overall latency of the system whilst allowing for flexibility for the parameters used; making it advantageous as it can calculate latency for a closed loop control system.

$$\tau l = (\triangle\,(\eta + \delta + \psi)) + \frac{\nu}{\ell} + F \tag{1}$$

Formula 1: Calculating communication latency introduced by security constructs for a single hop closed loop control

The total latency is represented as (τl) with the instruction cycle time (at a specified clock frequency) is (δ). The transmission time of the data is represented as (η) and the time to process a byte of data though the security algorithm is (ψ). The size of the packet is $(\triangle)$ with the propagation delay (e.g. the speed of electrons through a copper cable or the vacuum of the speed of light) represented as (ν). The distance of the link in meters is (ℓ). The round trip time is (F).

VIII. Comparison between Proposed Model and Simulation Results

Utilising the proposed model presented in Formula 1; Table II compares the results obtained from the proposed model against the simulated results. The results take into consideration the latency incurred from the software security construct TinyAEAD at three rounds. A crystal frequency of 8 MHz was sampled. SPI divisors of 4 sampled with packet sizes of 36, 52 and 84 bytes examined.

Table II
Model versus Simulation results for varying packet sizes

Packet Size (bytes)	proposed model results (ms)	Simulated results (ms)	difference in results (%)
36	202.3	201.5	0.39
52	213.6	212.5	0.51
84	236	234.1	0.80

Data displayed in Table II compares the outcome achieved from the proposed mathematical model and the simulated tests. Results indicate calculated and recorded results correlate.

Comparison of the proposed mathematical model and the simulation results indicate that the results calculated from the model is within an average percentage of 0.56%. This infers that the model is a good predictor for calculating the communication latency for closed loop control with the inclusion of AEAD security constructs.

Summary of the experimentation conducted indicates that a range of factors influence the communication latency generated. Packet size contributes the total latency with results

indicating the larger sized packets have the biggest increase in latency in comparison to smaller packets. This indicates that protocols with larger payloads may not be best suited to meeting the real-time requirements of closed loop control systems.

IX. Predictive Modelling

This section uses the proposed model as a predictive tool against the results obtained from the simulation. The PIC18F45K22 microcontroller can use a maximum crystal frequency of 64 MHz [12] and the communication latency can be calculated by using the proposed model. The crystal frequency and packet size sampled has strong correlation with the latency output. To validate this hypothesis a contrived scenario has been derived with a PIC18F45K22 microcontroller operating at a crystal frequency of 32 MHz. TinyAEAD at three rounds has been selected as the security construct of choice as it better suited to meeting real-time constraints. Three packet sizes are selected for this test, being 36, 52 and 84 bytes in length. The SPI divisor has been set to 4. σ represents standard deviation in Table III.

Table III
Comparative results of model versus simulation for software implementation of TinyAEAD (3 rounds)

Packet Size (bytes)	Proposed Model Results (ms)	Simulated Results (ms)	Difference in Results (%)	Mean (ms)	σ
36	49.9	50.4	0.97	50.1	0.35
52	51.5	53.1	1.13	52.3	1.13
84	53.4	58.5	5.11	57.1	1.90

From the data obtained in Table III, the model is better suited for predicting the latency for small packet sizes, whilst larger packet sizes show an increased percentage difference between the proposed result and the simulated result. Utilising the specified crystal frequency for this scenario suggests that the real-time constraints in Table I would be meet. It is also inferred that the model is suited to predicting the latency incurred utilising different crystal frequencies.

X. Discussion

Section X examines the potential impact of applying security constructs to the system case scenario presented in Section III. The real-time requirement for this scenario is 25 milliseconds [13] before the pressure begins to incline, therefore this value is used to mimic a real world scenario. The results obtained in Section IX suggest that a 32 MHz crystal frequency was not suitable for meeting the real-time requirements for this context; however, for this case scenario the maximum crystal frequency of 64 MHz has been selected for the PIC18F45K22. A direct comparison between AEAD constructs CCM at ten rounds and TinyAEAD at three rounds were selected with packet sizes samples of 36, 52 and 84 bytes in size selected measure the effect of changing the crystal frequency.

Figure 5 results indicates that the selection of the most suitable security construct is required to meet the real-time requirements of a system with TinyAEAD impacting less on the latency in comparison to CCM.

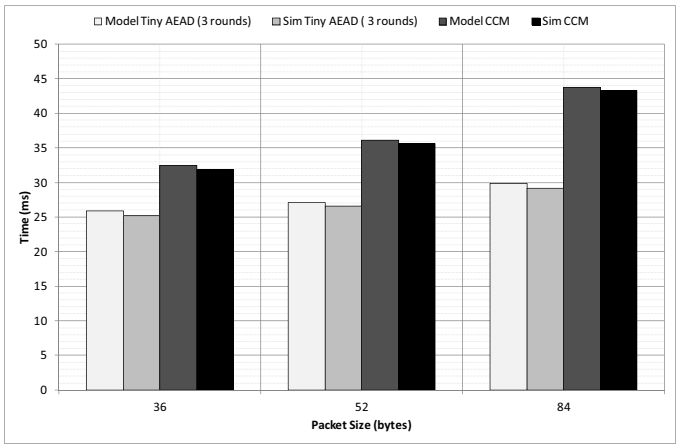

Figure 5. Model versus simulation of security construct impact for case scenario

Data illustrated in Figure 5 suggests that TinyAEAD would meet the real-time constraints using a packet size of 36 byte length only. The results obtained from the mathematical model correlate with the simulation, inferring that this model is applicable for predictive impacts.

As discussed throughout this paper the addition of security constructs on closed loop control increases the latency incurred. A result of missing the real-time constraints could impact on safety and operation of the staff and the plant. Figure 6 shows a consequence of compromising plant safety as shown in the DeBruce Grain Co incident in Haysville, Kansas.

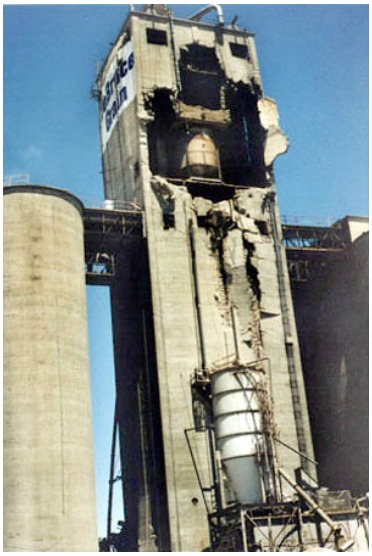

Figure 6. DeBruce Grain Co dust explosion incident [14]

XI. Conclusion

The proposed mathematical model presented in this paper is suitable for calculating the impact of security constructs for varying packet lengths and security constructs. Due to the flexibility of the model users can predict the impact of communication latency with the addition of security constructs applied without having to invest in a simulator or real world closed loop control system.

Concluding from the data obtained the impact of security constructs on closed loop control systems is significant with the overall communication latency increasing. The consequence of inducing delay on a real-time closed loop control system can be catastrophic as presented in the case scenario and therefore raises further questions regarding systems safety.

Consideration of the security construct is crucial towards the latency generated as the incorrect selection can cause a bigger impact on latency, causing disruption to the operation of the system and potential safety implications.

References

[1] A Cardenas, S Amin, and S Sastry. Research challenges for the security of control systems. In *Proceedings of the 3rd conference on Hot topics in security*, 2008.

[2] T Morris and W Gao. Industrial control system cyber attacks. In *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, 2013.

[3] M Luallen and D Harp. Breaches on the rise in control systems: A sans survey. Technical report, System Administration, Networking, and Security Institute, 2014.

[4] M. Franekova. Safety and security profiles of industry networks used in safety critical-applications. *Transport Problems*, 4:25–32, 2008.

[5] The Wolfson Centre for Bulk Solids Handling. Pneumatic conveying short course.

[6] Y Ma, W Jiang, N Sang, and X Zhang. Arcsm: A distributed feedback control mechanism for security critical real-time system. In *10th IEEE International Symposium on Parallel and Distributed Processing with Applications*, 2012.

[7] Z Pang and G Lui. Design and implimentation of secure network predictive control systems under deception attacks. *IEEE Transactions on Control Systems Technology*, 20:1334–1342, 2012.

[8] R.A Gupta, AK. Agarwal, Mo-Yuen Chow, and Wenye Wang. Performance assessment of data and time-sensitive wireless distributed networked-control-systems in presence of information security. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7, 2007.

[9] R. Dhand, G. Lee, and G. Cole. Communication delay modelling and its impact on real-time distributed control systems. In *ADVCOMP 2010 : The Fourth International Conference on Advanced Engineering Computing and Applications in Sciences*, 2010.

[10] Recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality.

[11] A. Adekunle and S. Woodhead. An aead cryptographic framework and tinyaead construct for secure wsn communication. In *Wireless Advanced (WiAd)*, 2012.

[12] Microchip. Pic18(l)f2x/4xk22 data sheet. Technical report, Microchip Technology Inc, 2012.

[13] H.J Hienrich. Ablauf von gas- und staubexplosionen gemeinsamkeiten und unterschiede. In *Sichere Handhabung brennbare Stäube, Band I, VDI Verlag, W. Germany.*, 1988.

[14] B Sturner, December 1998.