Safety evaluation of digital post-release environment sensor data interface for distributed fuzing systems

57th Fuze Conference, Newark, NJ

Wednesday, July 30th, 2014

Open Session IIIA, 3:20 PM

S. Ebenhöch, C. Schoppe, Dr. I. Häring

Funded by Federal Office of Bundeswehr Equipment,

Information Technology and In-Service Support (BAAINBw K 1.3)

Contact:

Stefan.Ebenhoech@emi.fraunhofer.de

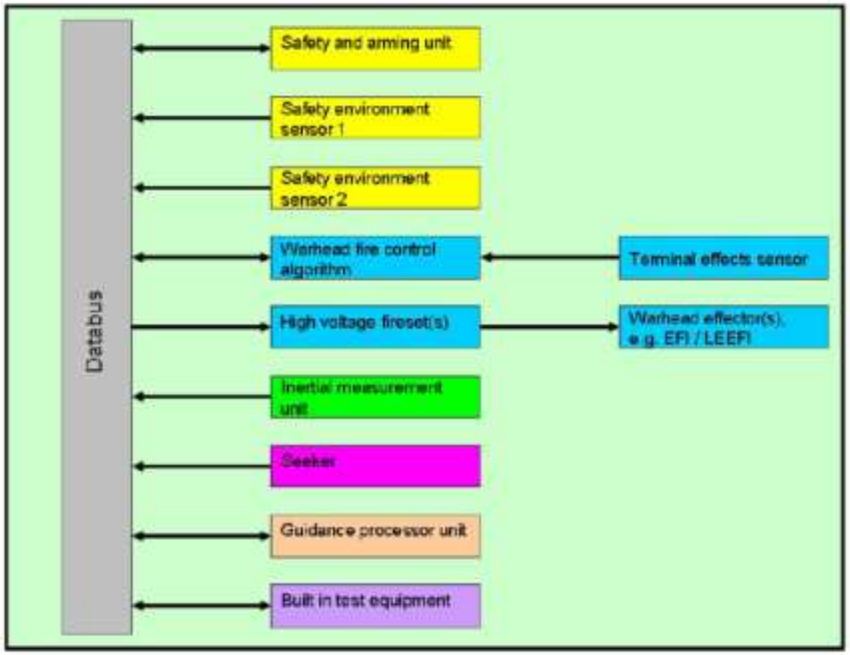
Safety evaluation of digital post-release environment sensor data interface for distributed fuzing systems: Content of presentation

- Motivation
- Post-release environment sensor (PRES) interface
- Simulation tool
- Safety evaluation results
- Conclusion

Motivation: Distributed fuzing systems

- Flexibility in geometry
- Compatibility of different fuzing, sensor weapon systems
- Improved replaceability of components
- Scalability of system performance
- Simpler realization of redundancy and separation of safety functions

Distributed modular fuzing system*

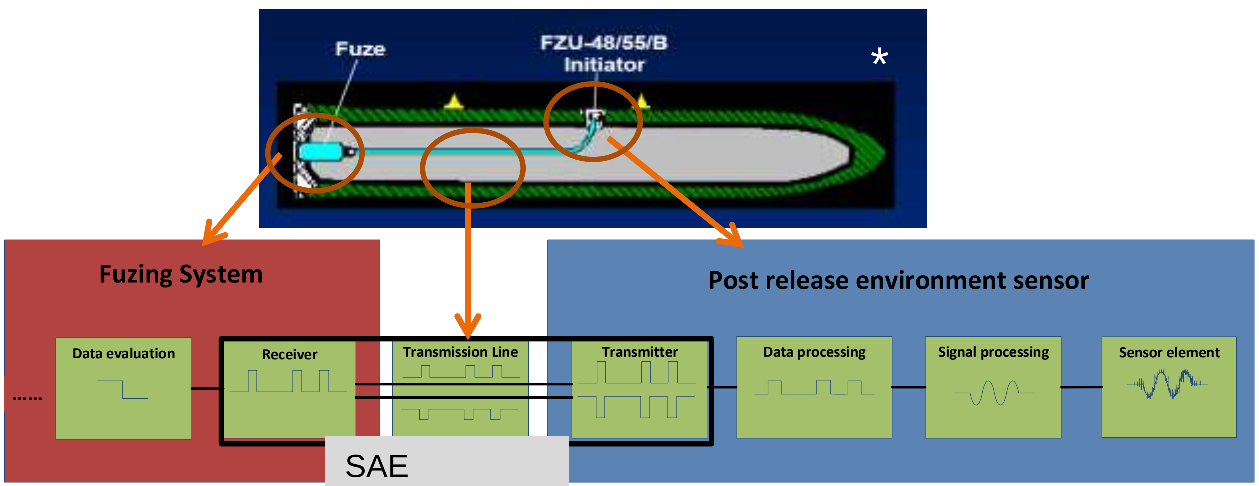


- **Application of digital non-proprietary standard interfaces**

*NATO Indusrial Advisory Group (NIAG): Study Group (SG) 117, *Future Fuzing Safety and Arming Technologies and Implications*, 2008.

Motivation: Standard SAE AS5716A

- Current situation: mainly analog interfaces in airborne fuzing systems
- SAE AS5716A: “Standard Electrical and Logical Interface for Airborne Fuzing Systems“
  - Addresses weapons using MIL-STD 1760
  - New revision: Pure digital data interface between sensor for detection of arming environment and fuzing system



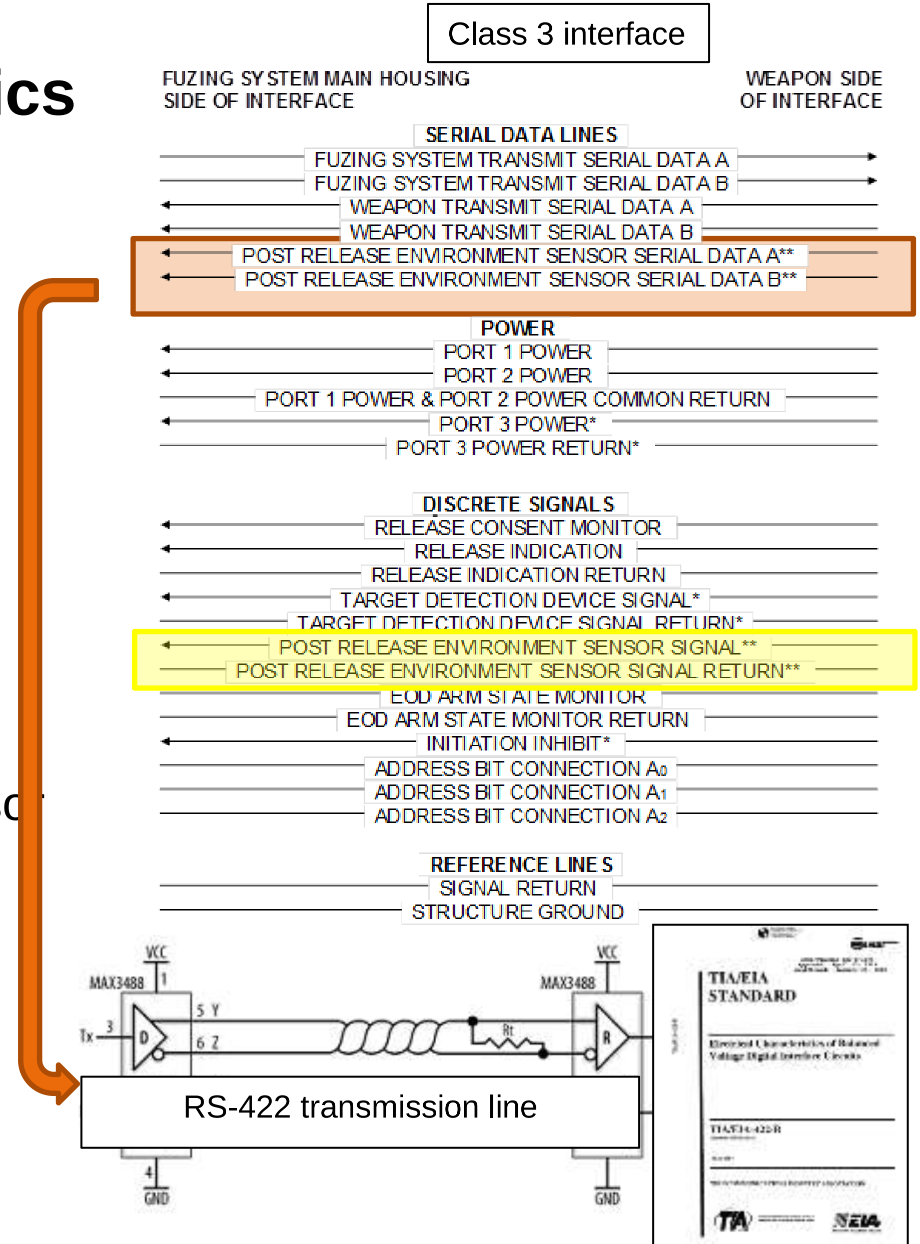
- **Goal: Evaluation of safety level** - Is the new digital data transmission at least as safe as the established analog transmission in airborne fuzing systems?

*Frank Robbins, Presentation: Fuzes for Air Force Unguided and Precision Guided Weapons, 2001: held at 45th NDIA Fuze Conference.

Fraunhofer EMI

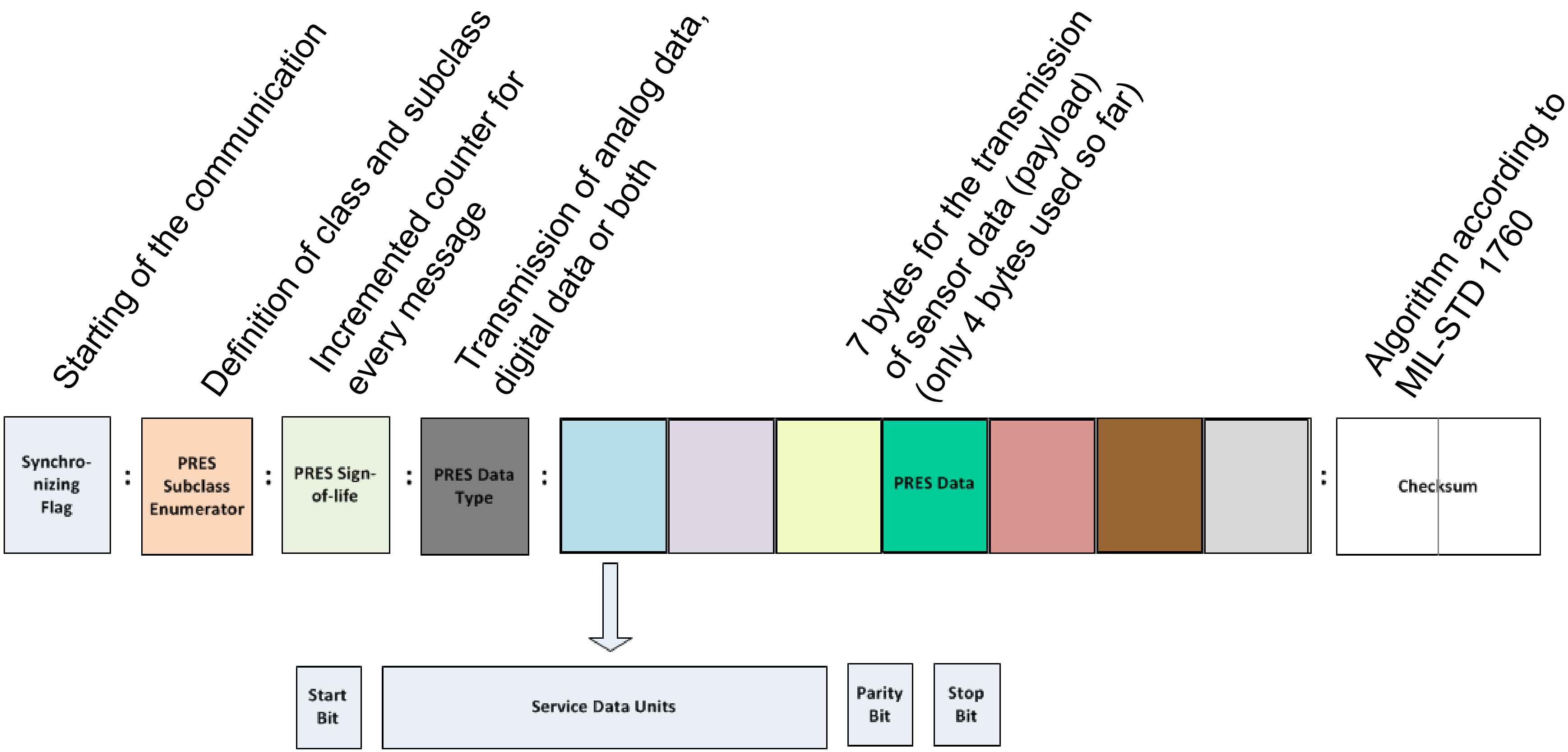
PRES-Interface: Characteristics

- Definition of electrical interface characteristics
  - RS-422 standard
  - Transmission rate: 38.4 kbps
  - Simplex mode
- Classification of interfaces
  - PRES-Interface only in class 3
  - Subclasses specify data type of sensor (analog, digital)
- Definition of protocol structure for serial data interface



Fraunhofer EMI

PRES-Interface: Protocol



- Every byte (service data unit, SDU) is added by start, stop and (even) parity bits

Fraunhofer EMI

PRES-Interface: Checksum

- Checksum algorithm: »When each data word (including the checksum word) of a message is rotated right cyclically by a number of bits equal to the number of preceding data words in the message, and all the resultant rotated data words are summed using modulo 2 arithmetic to each bit (no carries), the sum shall be zero.«

Word = 2 SDUs; Parity bits

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$	$b_{0,4}$	$b_{0,5}$	$b_{0,6}$	$b_{0,7}$	$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$	$b_{1,4}$	$b_{1,5}$	$b_{1,6}$	$b_{1,7}$	p_0	p_1
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$	$b_{2,4}$	$b_{2,5}$	$b_{2,6}$	$b_{2,7}$	$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$	$b_{3,4}$	$b_{3,5}$	$b_{3,6}$	$b_{3,7}$	p_2	p_3
$b_{4,0}$	$b_{4,1}$	$b_{4,2}$	$b_{4,3}$	$b_{4,4}$	$b_{4,5}$	$b_{4,6}$	$b_{4,7}$	$b_{5,0}$	$b_{5,1}$	$b_{5,2}$	$b_{5,3}$	$b_{5,4}$	$b_{5,5}$	$b_{5,6}$	$b_{5,7}$	p_4	p_5
$b_{6,0}$	$b_{6,1}$	$b_{6,2}$	$b_{6,3}$	$b_{6,4}$	$b_{6,5}$	$b_{6,6}$	$b_{6,7}$	$b_{7,0}$	$b_{7,1}$	$b_{7,2}$	$b_{7,3}$	$b_{7,4}$	$b_{7,5}$	$b_{7,6}$	$b_{7,7}$	p_6	p_7
$b_{8,0}$	$b_{8,1}$	$b_{8,2}$	$b_{8,3}$	$b_{8,4}$	$b_{8,5}$	$b_{8,6}$	$b_{8,7}$	$b_{9,0}$	$b_{9,1}$	$b_{9,2}$	$b_{9,3}$	$b_{9,4}$	$b_{9,5}$	$b_{9,6}$	$b_{9,7}$	p_8	p_9
$c_{0,0}$	$c_{0,1}$	$c_{0,2}$	$c_{0,3}$	$c_{0,4}$	$c_{0,5}$	$c_{0,6}$	$c_{0,7}$	$c_{1,0}$	$c_{1,1}$	$c_{1,2}$	$c_{1,3}$	$c_{1,4}$	$c_{1,5}$	$c_{1,6}$	$c_{1,7}$	p_{10}	p_{11}

Checksum

PRES Subclass Enumerator

PRES Sign-of-Life

PRES Data Type

PRES Data-1st byte

PRES Data-2nd byte

PRES Data-3rd byte

PRES Data -4th byte

PRES Data 5th byte

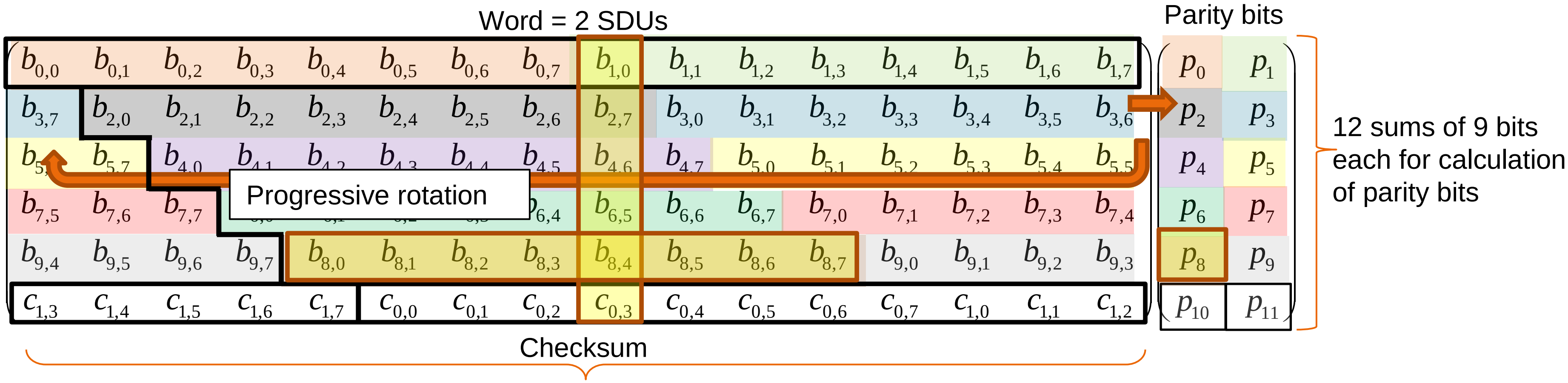
PRES Data -6th byte

PRES Data-7th byte

PRES-Interface: Checksum

- Checksum algorithm: »When each data word (including the checksum word) of a message is rotated right cyclically by a number of bits equal to the number of preceding data words in the message, and all the resultant rotated data words are summed using modulo 2 arithmetic to each bit (no carries), the sum shall be zero.«

$$(b_{i,0}+b_{i,1}+b_{i,2}+b_{i,3}+b_{i,4}+b_{i,5}+b_{i,6}+b_{i,7}+p_i) \mod 2 = 0$$



16 sums of 6 bits each for calculation of checksum bits

$$b_{1,0}+b_{2,7}+b_{4,6}+b_{6,5}+b_{8,4}+c_{0,3} \mod 2 = 0$$

PRES Subclass Enumerator | PRES Sign-of-Life | PRES Data Type

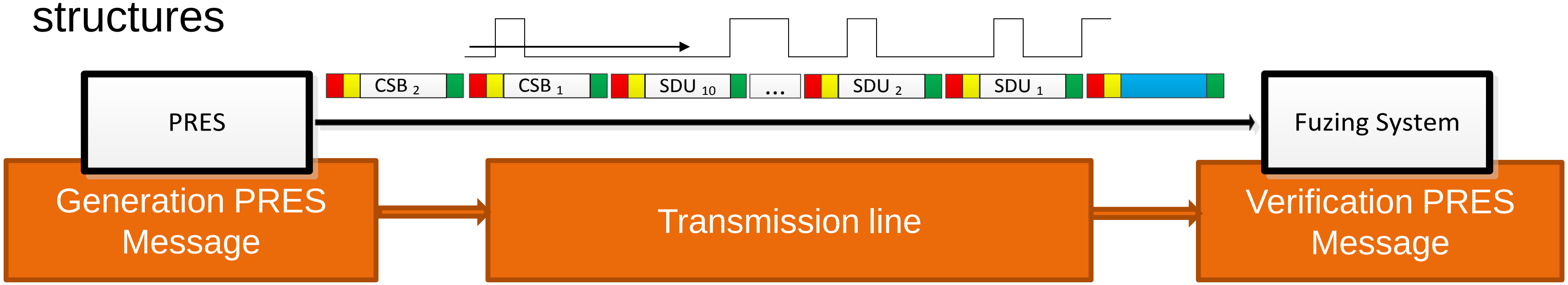
PRES Data-1st byte | PRES Data-2nd byte | PRES Data-3rd byte

PRES Data -4th byte | PRES Data 5th byte | PRES Data -6th byte

PRES Data-7th byte

Simulation tool: Architecture

- Development of flexible simulation platform for the analysis of various protocol structures



Calculation of checksum

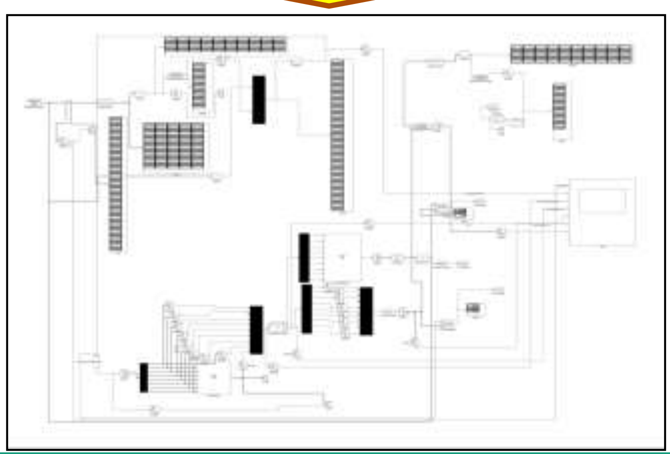
Calculation of parity bits

Injection of bit flips in message

Implementation of error models

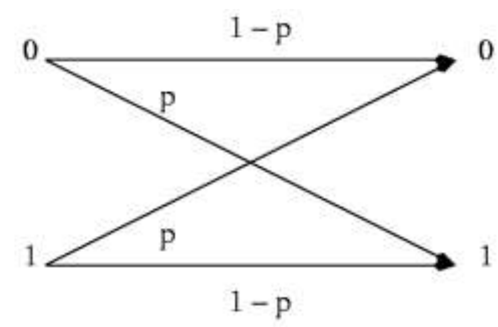
Verification checksum

Checking parity bits

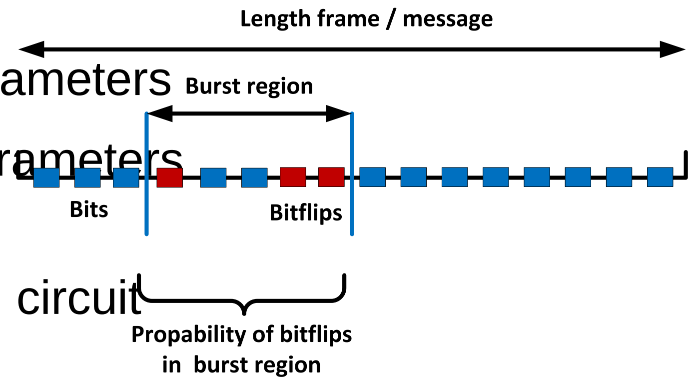


Fraunhofer EMI

Simulation tool: Error modeling



- Random errors
  - Model: Binary symmetric channel
  - Transmitted bit is flipped with the probability p
- Burst errors
  - Specific burst model with several parameters
  - Dynamic variation of model parameters in simulation



- Coupled simulation (combination of protocol and circuit level):
  - Circuit model of transmission line
  - Electrical modeling of interferences (e.g. lightning)

Generation PRES Message →

Schematic of transmission line

→ Verification PRES Message

Simulation tool: Mathematical validation

- Assuming that bit flips occur independently with probability p
- Using binomial distributions we find the following probabilities for n words
  - For not detecting bit flips using checksum only:

$$P^{CSA\ \text{unrecognised}}(p) = \left(\sum_{i=1}^{\lfloor n/2 \rfloor} \binom{n}{2i} p^{2i} (1-p)^{(n-2i)} + (1-p)^n \right)^{16} - (1-p)^{16n}$$

  - For not detecting (actual) bit flips using parity bits only:

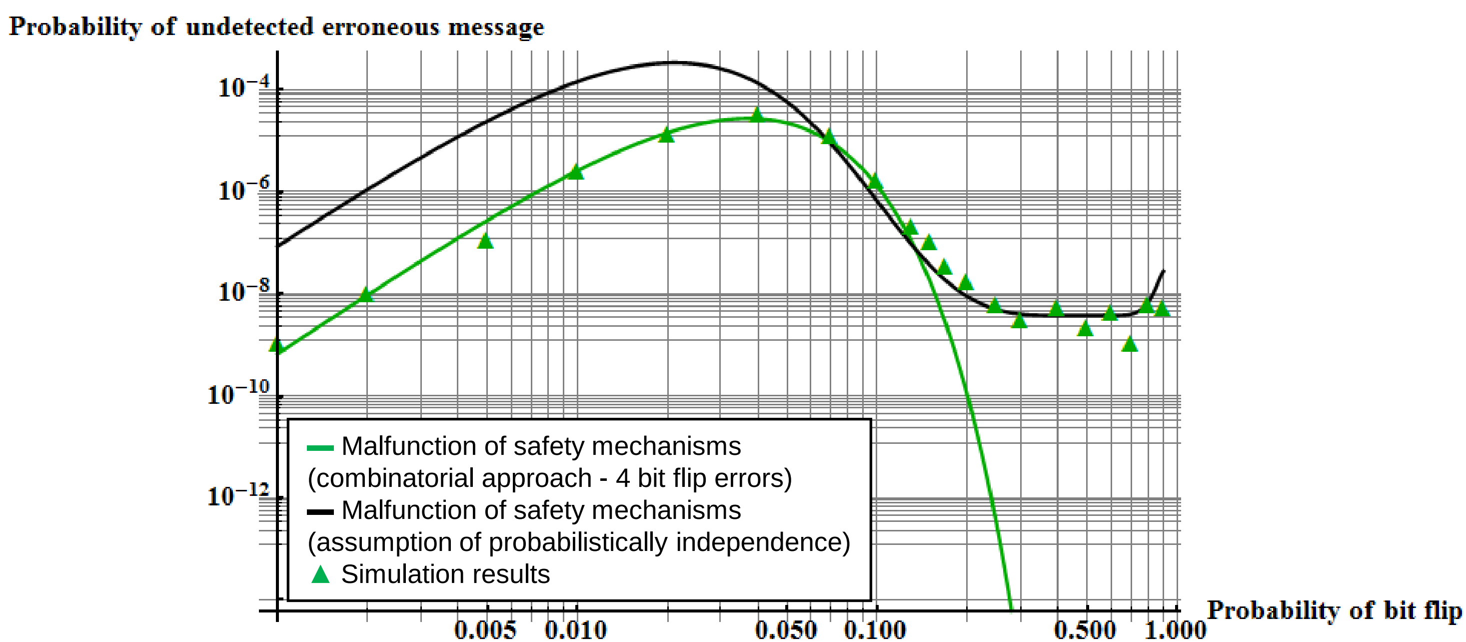
$$P^{PB\ \text{unrecognized}}(p) = \left(\sum_{i=0}^{4} \binom{9}{2i} p^{2i} (1-p)^{9-2i} + (1-p)^9 \right)^{12} - (1-p)^{12n}.$$

- Combinatorial considerations yield that there have to be at least four bit flips so that CSA as well as PB do not detect defectiveness of message
  - Mathematical transformation of presented progressive rotation

$$P^{\text{Four bitflips undetected}}(p) = 2\left(\sum_{i=0}^{8} \sum_{j=0}^{n-1} \min\{i, n-1-j\}(8-i) + \sum_{i=0}^{8} \sum_{j=0}^{n-1} \sum_{k=0}^{(n-1)-(i+j)} k \right) p^4 (1-p)^{18n-4}$$

Safety evaluation results: Random errors

- Simulation of 10^{10} messages for every bit flip probability
- Good match between simulation and combinatorial consideration (for small p)
- For high bit flip probabilities checksum and parity bits mechanisms are probabilistically independent ($P^{CSA\ unrecognized} * P^{PB\ unrecognized}$)



- Probability of bit flip 10^{-3} ➔ Probability of undetected erroneous message 10^{-9}

Fraunhofer EMI

Safety evaluation results: Burst errors

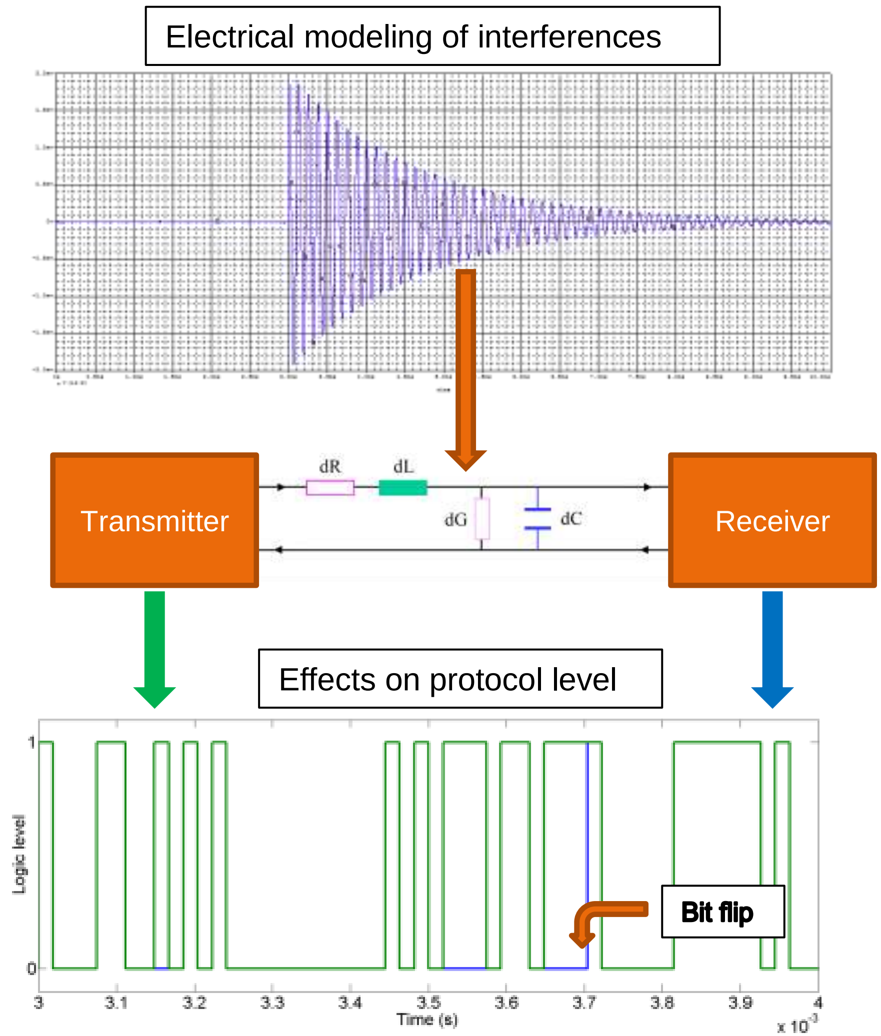
- Burst error model
  - Simulation of $3 \cdot 10^6$ messages
  - Variation of model parameters

➔ No undetected erroneous messages

- Electrical modeling of interferences
  - Performance of coupled simulation
  - Modeling interferences according to MIL-STD 464 (Electromagnetic environmental effects)

➔ No undetected erroneous messages

- Future work
  - Evaluation of data transmission reliability in laboratory experiments



Fraunhofer EMI

Conclusion

- Digital data transmission: Minor sensitivity to electrical interferences
- High efficiency of mechanisms for error detection (check sum and parity bits)
  - Random errors: For common bit flip rates, probability of undetected erroneous message less than 10^{-9}
  - Burst errors: Acceptable safety levels achieved by first analyses, no undetected erroneous messages

➔ Fraunhofer EMI has an efficient simulation platform for safety and reliability analysis of digital data transmission (analysis on circuit and protocol level)

Conclusion

- Further (possible) safety features of PRES-interface to prevent unintentional arming
  - For fuzing activities several messages in sequence have to represent the same value
  - Plausibility checks of fuzing system could identify erroneous sensor data (for some SDUs only a few valid states are possible)
  - Checking compatibility between sensor and fuzing system (correct class & subclass)
  - Detection of illegal transmission sequences (sign-of-life & start/stop bits)
  - New interface offers better set-up between PRES, fuzing system and weapon for specific safety criteria

➔Usage of digital PRES-Interface would provide a considerably improved transmission reliability and therefore safety in most of the standard relevant applications.

➔PRES-Interface could be an important element for future distributed systems

Thank you for attention! Questions…?

Stefan Ebenhöch
Group Leader System Reliability
Safety Technology and Protective Structures

Fraunhofer EMI
Am Klingelberg 1
79588 Efringen-Kirchen
Germany
Tel.: +49 7628 / 9050 - 738
Stefan.Ebenhoech@emi.fraunhofer.de