Fitness for use of ISOBUS network in safety-critical functions

Ari Ronkainen
MTT AgriFood Research Finland
COISTA 2011
30.6.2011 Vienna

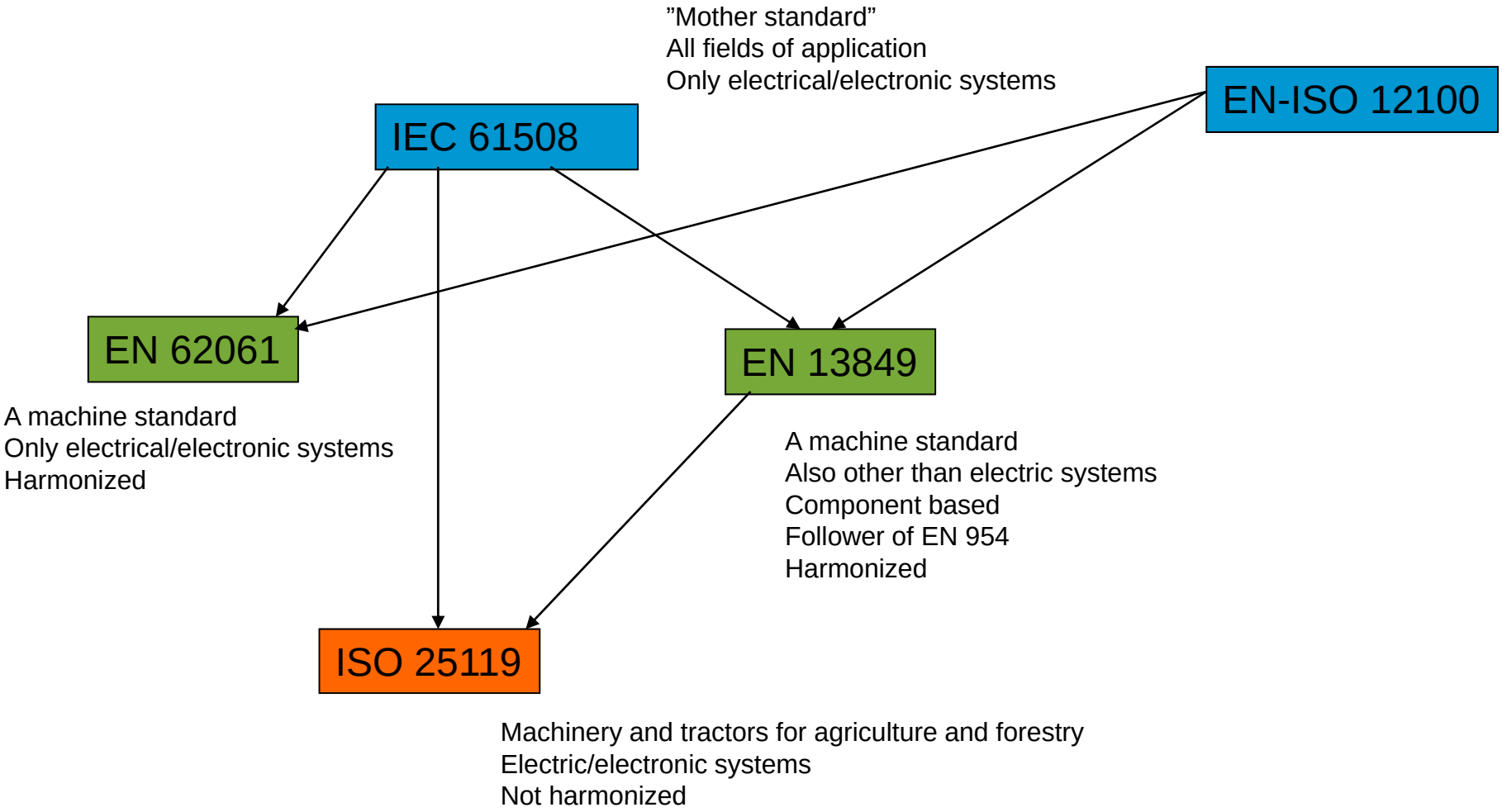
Introduction

- A research prototype of ISOBUS class 3 machine combination
- Advanced automated functions
- Few hazardous functions
  - What is required for this to enter markets?
  - What is required from safety?
    - “Machine directive”
    - ISO 12100
  - Can ISOBUS network be used in safety-related functions?

Legal framework

- 2003/37/EC Tractor directive
  - Applies to tractors and towable interchangeable machinery
  - Sets requirements for type approval
    - For example: registration plates, headlights, safety cabin, access ways…
- 2006/42/EC Machine directive
  - All machinery sold in EU must comply with this directive
  - Manufacturer must ensure that products comply with this directive
  - Relevant to all machinery
    - Tractors and towable interchangeable machinery are excluded for risks that are covered in 2003/37/EC directive
  - If manufacturer follows a harmonized standard, the manufacturer can assume to fulfill requirements in the field of the standard
  - Requires risk analysis and reduction of risks to a tolerable (minimal) level

Standards for safety-related parts of control systems



Requirements for data communications from standards

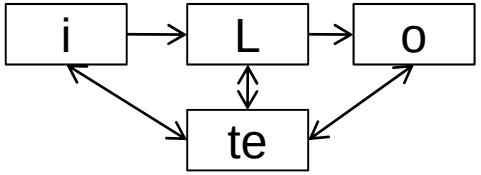
- No explicit requirements for use of data communications
- Data communications must be inspected as a part of safety-related system
- Also data communications that may have an effect on performance of safety-related system need to be evaluated as a part of safety-related system
- Performance and integrity requirements as well as architectural constraints apply

- IEC 61508-2
  - The probability of undetected failure of data communications is to be taken into account when evaluating integrity of safety-related system
  - Repetition, deletion, insertion, re-sequencing, corruption delay and masquerade errors are to be taken into account
  - Refers to EN 50159-2

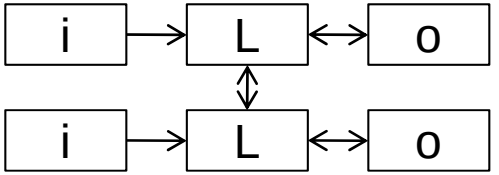
Architectural constraints or System category

- Imposed by all four standards (IEC 61805, EN 62061 EN13849 & ISO 25119)
- Force designers to use redundancy and diagnostics
- 5 named structures
- Category B & 1
  - Single channel system

- Category 2
  - Singe channel system, with external test equipment



- Category 3 & 4
  - Dual channel system, with cross monitoring

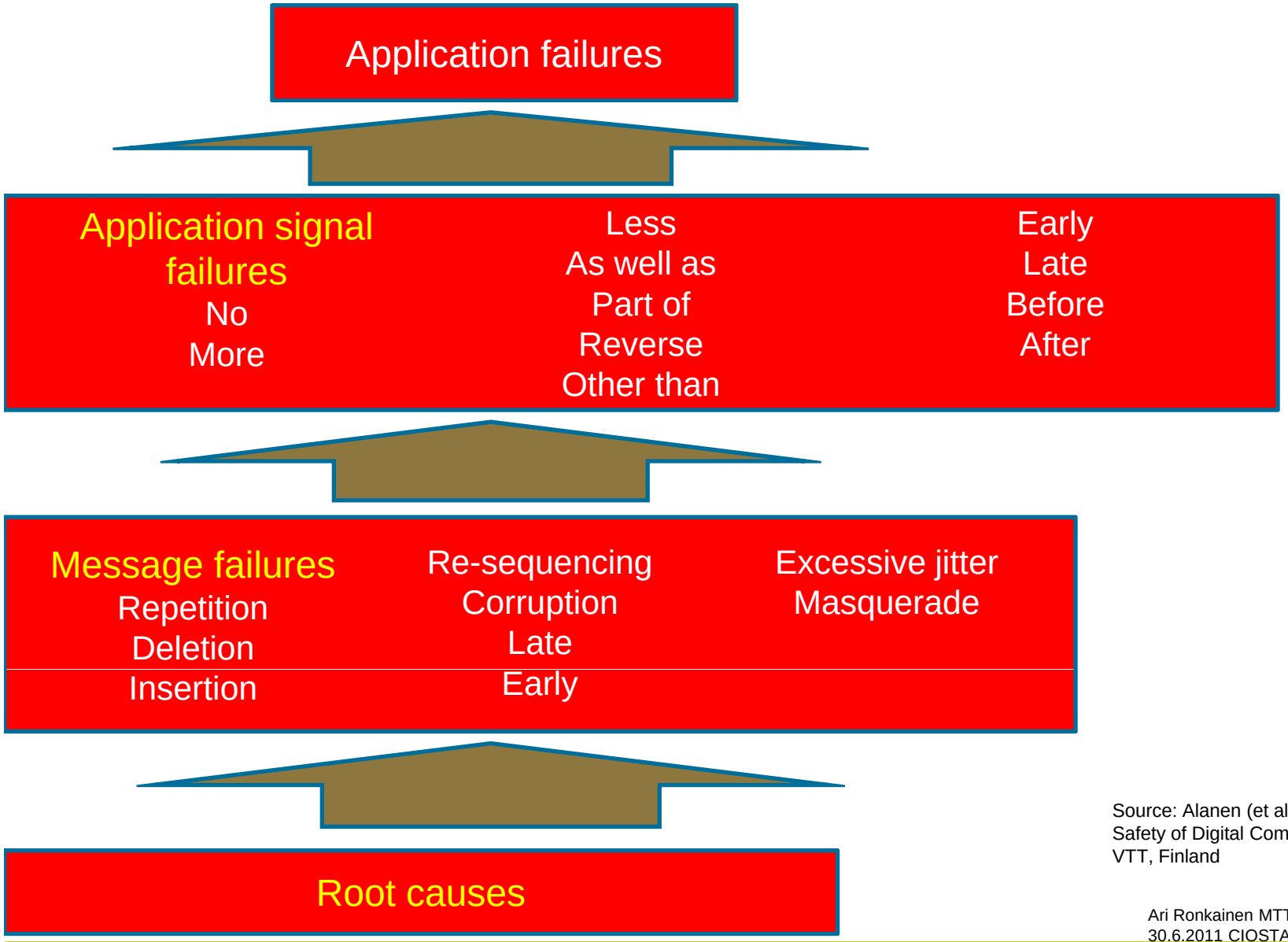


Determining performance level in ISO 25119

- AgPL Agricultural performance level
  - How big risk can be related to failure of safety-related system
- MTTF Meantime to failure
- DC Diagnostic coverage

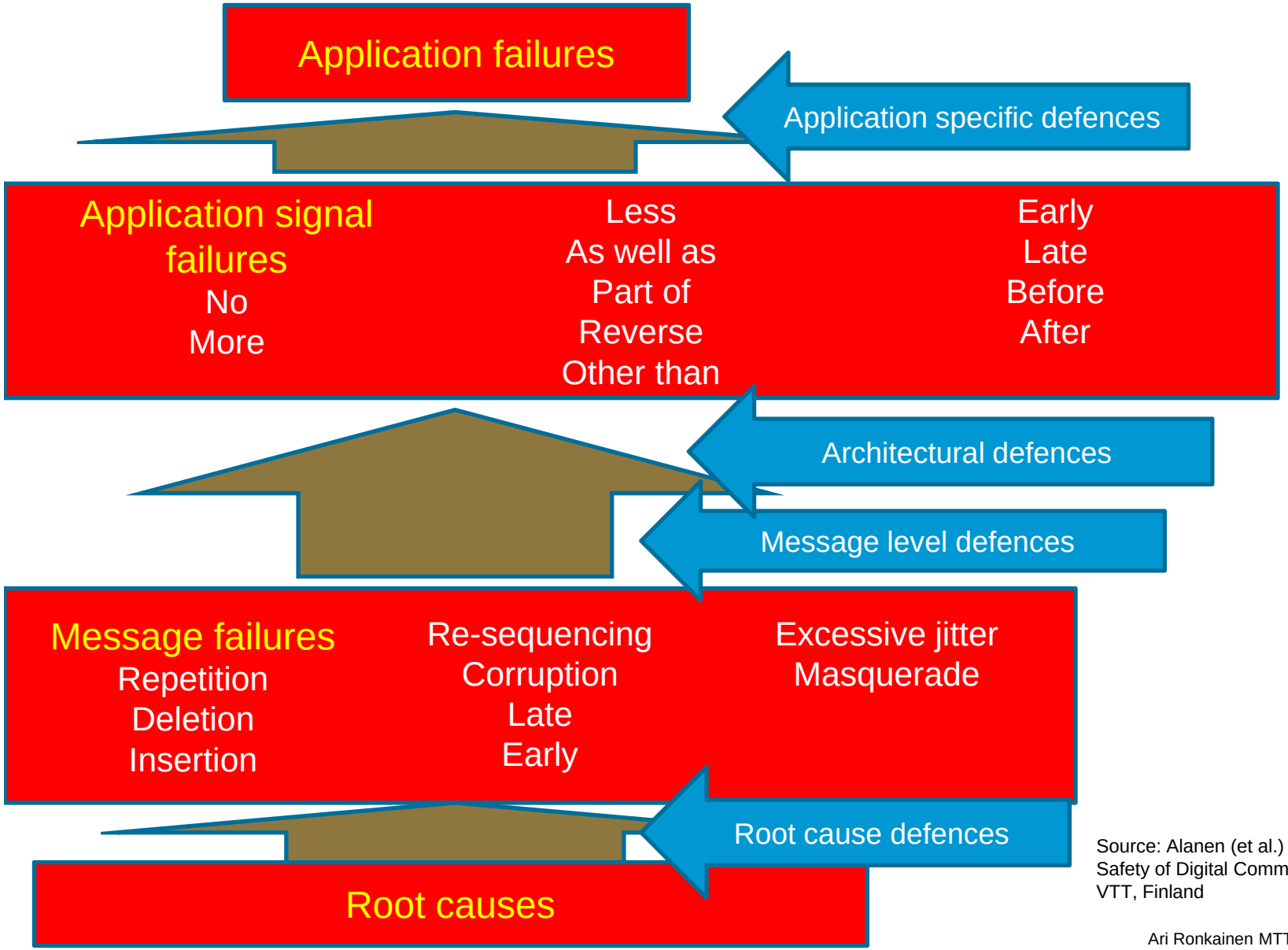
AgPl	Software Requirement Level MTTF					
a	1 Low	B Low	B Low	B Low	B Low	
b	2 Med	1 Med	B Low	B Low	B Low	
c		2 Med	1 Med	1 Low	1 Low	
d				2 Med	2 Med	
e					3 Hi	
	B DC low	1 DC med	2 DC med	3 DC med	4 DC hi	system category (class in EN 13849)

Failure model



Source: Alanen (et al.) 2004
Safety of Digital Communications in Machines
VTT, Finland

Failure model



Source: Alanen (et al.) 2004
Safety of Digital Communications in Machines
VTT, Finland

Defences against message failures

Threat	Possible defences	
Repetition	Sequence number Redundancy/Replication Bus guardian	Timestamp Time triggered architecture Inhibit times
Deletion	Sequence number Feedback/acknowledgement Time triggered architecture	Time out Redundancy/Replication
Insertion	Sequence number Feedback/acknowledgement CRC Identifier's Hamming distance	Source and destination identifiers Identification procedure Redundancy/Replication
Incorrect sequence	Sequence number Redundancy/Replication	Timestamp Time triggered architecture
Corruption	Feedback/acknowledgement Cryptographic techniques	CRC Redundancy/Replication
Late	Timestamp Feedback/acknowledgement Message prioritisation	Time out Time triggered architecture Inhibit times
Early	Timestamp	Time triggered architecture
Excessive jitter	Timestamp Message prioritisation	Time triggered architecture Inhibit times
Masquerade	Feedback/acknowledgement CRC Identifier's Hamming distance	Identification procedure Cryptographic techniques
Inconsistency	Membership control	Atomic broadcast

Source: Alanen (et al.) 2004
Safety of Digital Communications in Machines
VTT, Finland

Communication defences available in ISOBUS

Defence	Availability in ISOBUS
Redundancy/Replication	In physical layer Two signal lines with inverted signals Provides defence against EMI and cable faults
Sequence number	No
Timestamp	No
Time out	for some messages
Source and destination identifiers	Yes
Feedback/acknowledgement	Yes Acknowledgement in data link layer Feedback in application layer for some messages
Identification procedure	Address claim when the bus is initialised and when a node first time connects to the bus
CRC	Yes 15 bit CRC in data link layer
Cryptographic techniques	No
Membership control	For some nodes
Atomic broadcast	Yes
Time triggered architecture	No
Bus guardian	No but error counters in transceivers
Message prioritisation	Yes Pre set priorities in standard
Inhibit times	Yes for some messages
Identifier's Hamming distance	No

Defences against communication failures in ISOBUS

Threat	Defence available in ISOBUS	
Repetition	No	
Deletion	Time out for some messages Acknowledgement	Feedback for some messages
Insertion	Source and destination identifiers CRC	Acknowledgement Feedback for some messages
Incorrect sequence	No	
Corruption	Feedback/acknowledgement Redundancy/Replication	CRC
Late	Time out for some messages Message prioritisation (fixed)	Feedback for some messages
Early	No	
Excessive jitter	Message prioritisation	
Masquerade	Feedback for some messages CRC	Identification procedure Membership control
Inconsistency	Membership control	Atomic broadcast

Other features of ISOBUS

- Single channel system
  - Architectural constraint
- Non deterministic & fail-silent
  - Low diagnostic capabilities
  - High availability
  - Additional diagnostic measures needed

Conclusion

- Use of ISOBUS network in safety-critical functions is problematic
- Fitness depends on application
  - Level of associated risk
  - Possibility to build additional safety measures
  - Possibility to build application specific defences
  - Can required integrity be achieved
    - Can execution of safety-function be guaranteed
- Usable as is for only low integrity requirement systems
  - For higher requirements additional safety measures are needed