SYSTEMS & COMPONENTS

AGRI TECHNICA
The World's No.1

Forum Systems & Components
Hall 16, Stand C43

‘Is ISOBUS safe? Regulatory and Technical aspects for the use of ISOBUS in the context of ISO25119’

AGRITECHNICA - HANNOVER 11 NOVEMBER 2015

Michela AUDONE – Reggio Emilia Innovazione
Massimiliano RUGGERI- National Research Council

WHO?

REGGIO EMILIA INNOVAZIONE

WHY?

National Research Council of Italy

REGGIO EMILIA INNOVAZIONE

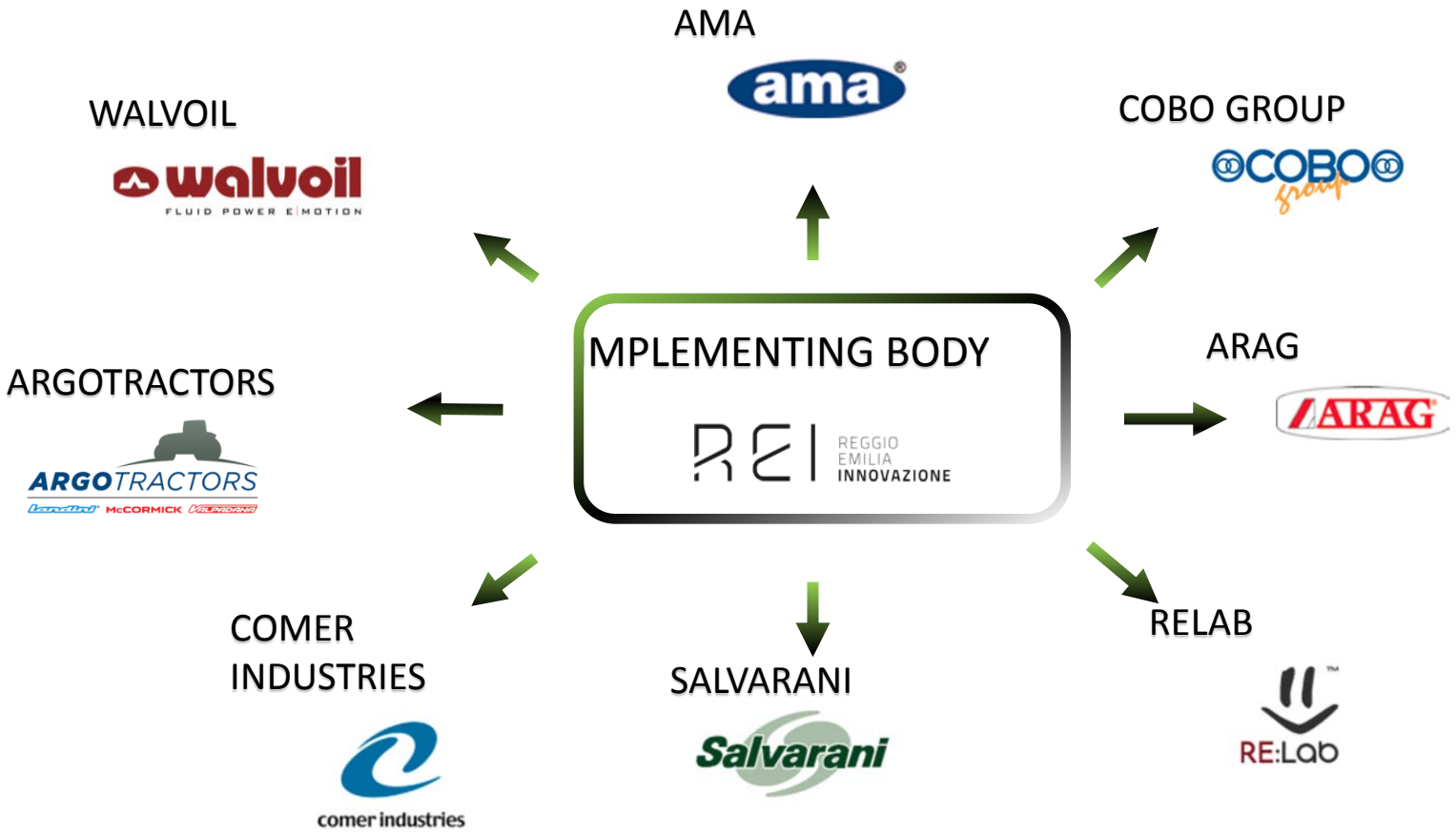
CONNECTION

IDE_AGRI NETWORK

IDEAgri
GROWING THE FUTURE

IDE_AGRI NETWORK

YEAR OF CONSTITUTION: JULY 2013
8 ENTERPRISES IN AGRICULTURAL SECTOR



IDE_AGRI NETWORK

THE NETWORK SUPPORT AND IS SUPPORTED IN ITS ACTIVITY BY:

REGGIO EMILIA INNOVAZIONE

ITALIAN ISOBUS CERTIFICATION CENTER

PRE COMPLIANCE ➔ COMPLIANCE

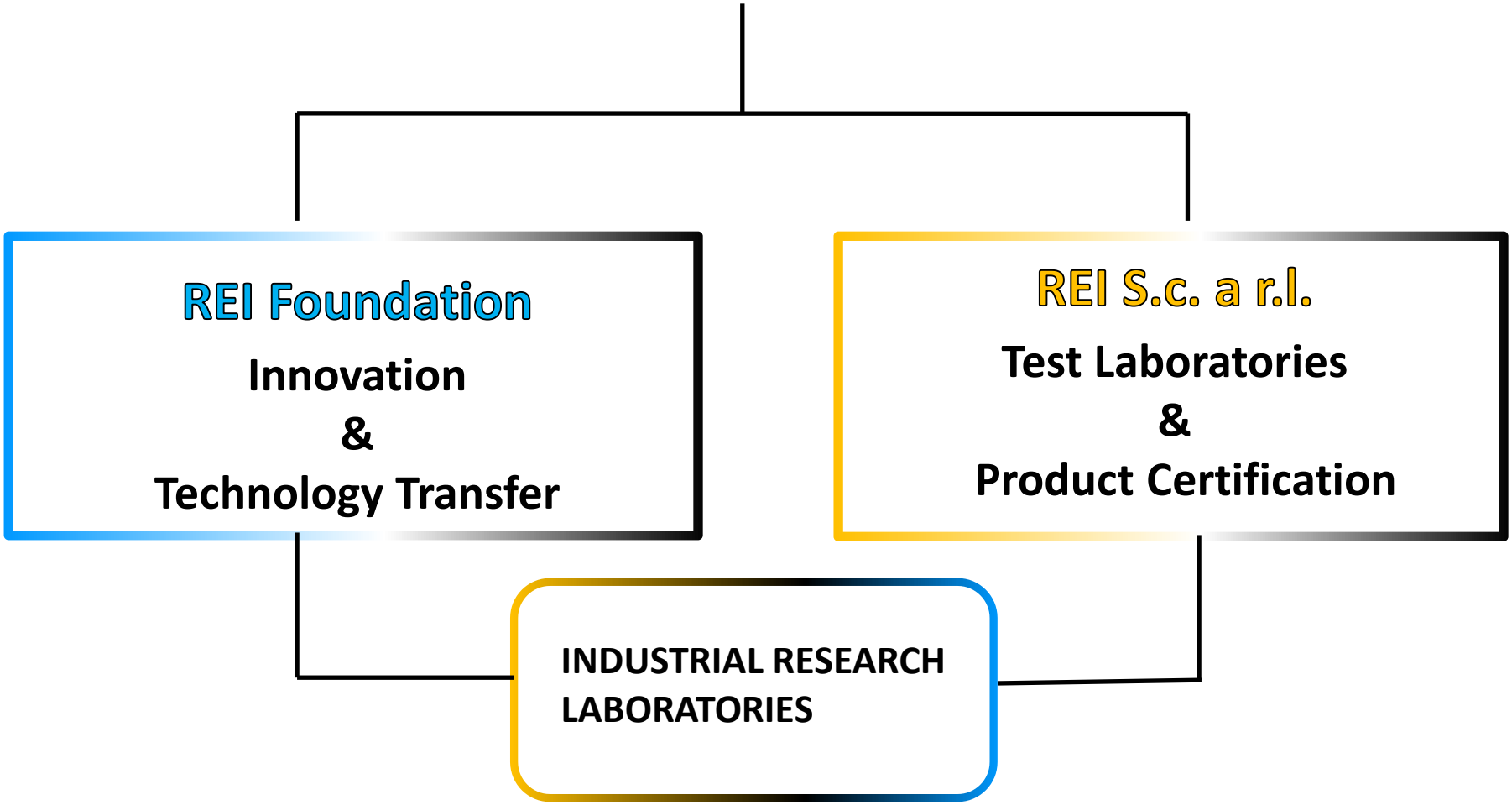
CERTIFICATION

REI is one of the five recognised Laboratory by AEF for Isobus Certification in the world and the only one in Italy.

Main instruments:

- AEF ISOBUS Conformance Test Tool (CT)
- AEF ISOBUS DataBase (DB)

REI- Reggio Emilia Innovazione



REI- Reggio Emilia Innovazione

TECHNOLOGY TRANSFER

INDUSTRIAL RESEARCH LABORATORIES

TEST LABORATORIES

- **EMC:** ELECTROMAGNETIC COMPATIBILITY
- **PFE:** ELECTRICAL & FUNCTIONAL TEST
- **MVR:** MACHINE VIBRATION & NOISE
- **ENDURANCE:** RELIABILITY & DURATION
- **EML:** ELECTRICAL MOTORS
- **ISOBUS:** ISOBUS PROTOCOL CERTIFICATION

IDE_AGRI – Objectives

- Create an electronic italian district in agricultural sector
- Collaborate and share each experiences in order to adopt and disseminate ISOBUS technology and digital electronics
- Work together in ambitious project (es: MIX@Tractor)

THANK YOU !!!

Ing. MICHELA AUDONE
TTO - Technology Transfer Office
email: audone@reinnova.it

Via Sicilia 31, 42122 - Reggio Emilia
Tel. +39 0522 922238
Cell. +39 3387373805
www.reinnova.it

IS ISOBUS SAFE? REGULATORY AND TECHNICAL ASPECTS FOR THE USE OF ISOBUS IN THE CONTEXT OF ISO 25119

Massimiliano Ruggeri

CNR-IMAMOTER National research Council of Italy

Safety Definition

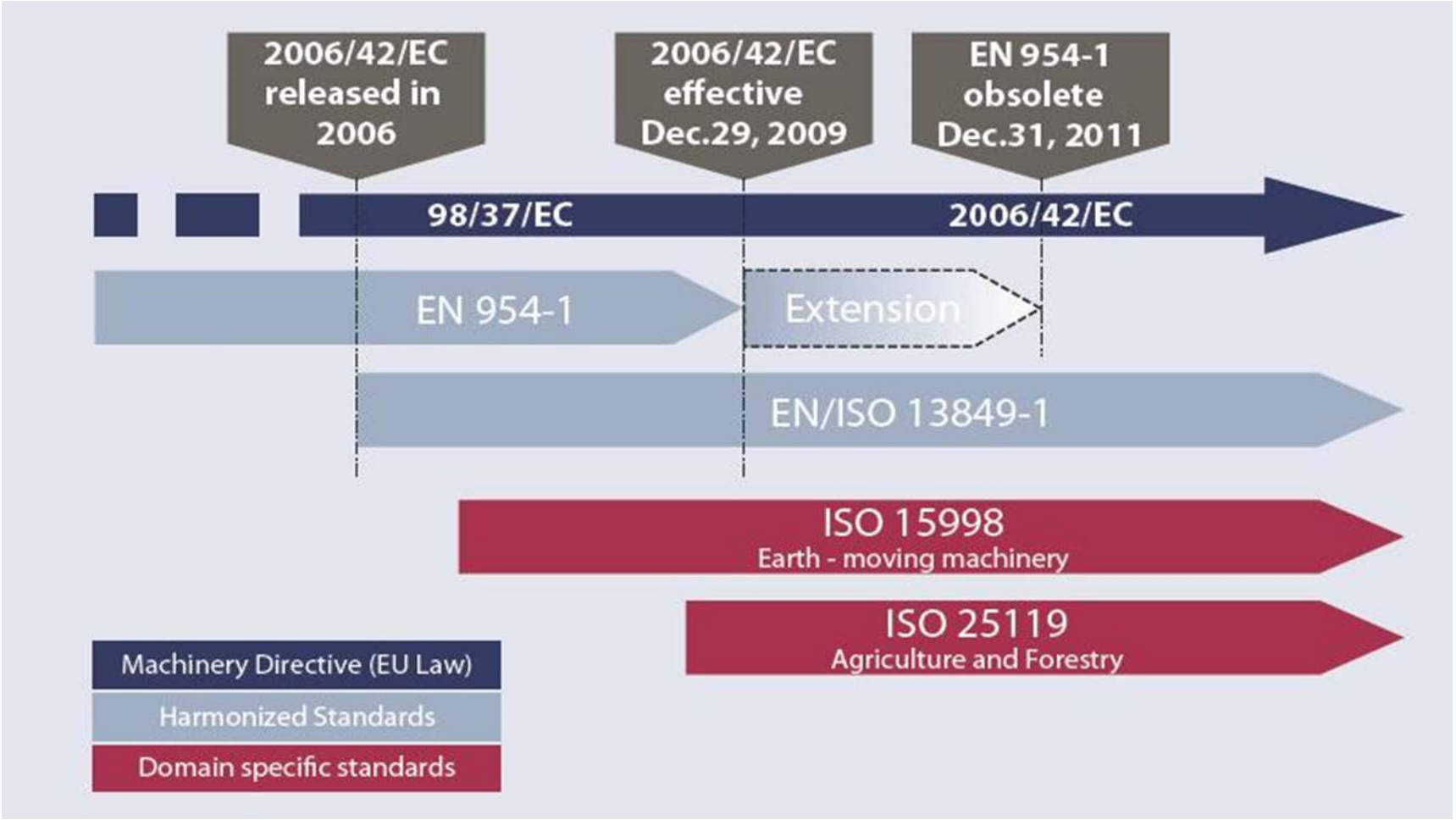
Functional Safety is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly (through damage to property or to the environment).

Focus of Functional Safety

Functional Safety is a series of rules and techniques mainly (but not only) focused on Electrical, Electronic and Programmable Electronic Systems (E/E/PES), designed and standardized to reduce the risk of injury or damage under an acceptable threshold, as a function of system, system mission and environment.

Functional safety is *end to end in scope* and, in practice, Functional Safety methods have to extend to the non-E/E/PES parts of the system that the E/E/PES actuates, controls or monitors.

Safety Standards Roadmap Story in EU Community



Safety Standards Roadmap for Agricultural and Construction Machines in EU

2012

2014

2016

TRACTORS ONLY

For best practice reason ISO 25119 is strongly recommended for any AG machinery.

Voluntary path. No Safety norms required

TRACTORS ONLY DO HAVE HOMOLOGATION 2003/37, No link with functional safety norms Homologation is a subset of MD.

Homologation path. No Safety norms required

2003/37 revision will ask compliancy with ISO 25119 harmonized as part of homologation of new products

OTHER AGRICULTURAL MACHINES

For best practice reason ISO 25119 is strongly recommended for any AG machinery.

Referred by MD, new EN ISO 4254 is released requesting ISO 25119 to be applied.

CE ONLY

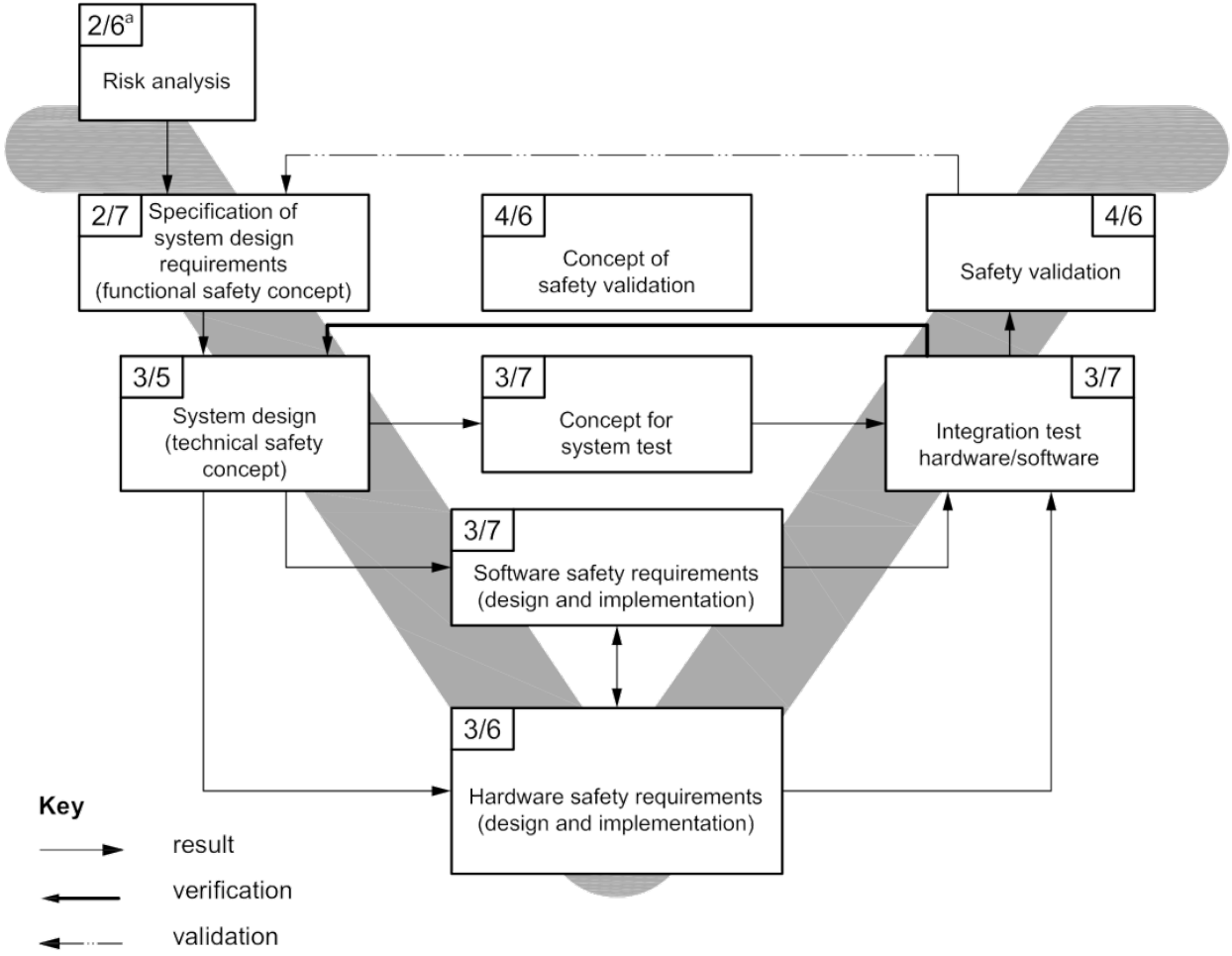
MD : Harmonized norm ISO 13849 mandatory on **new machines**

ISO 13849 mandatory path

ISO 15998 is the harmonized norm for risk calculation on CE

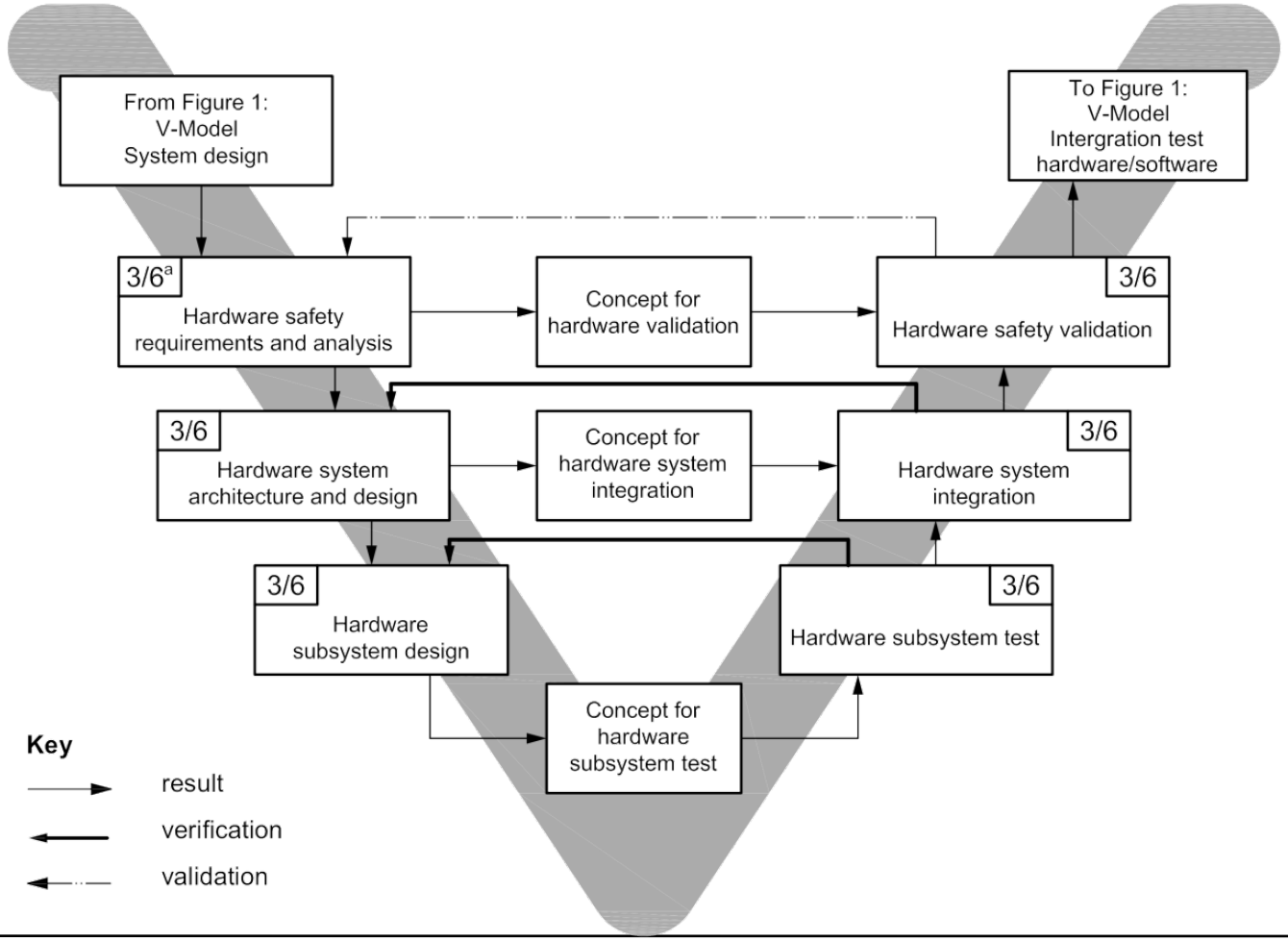
System Design

The objective is to define a development process for producing a design that fulfils the safety requirements for the entire safety-related system.



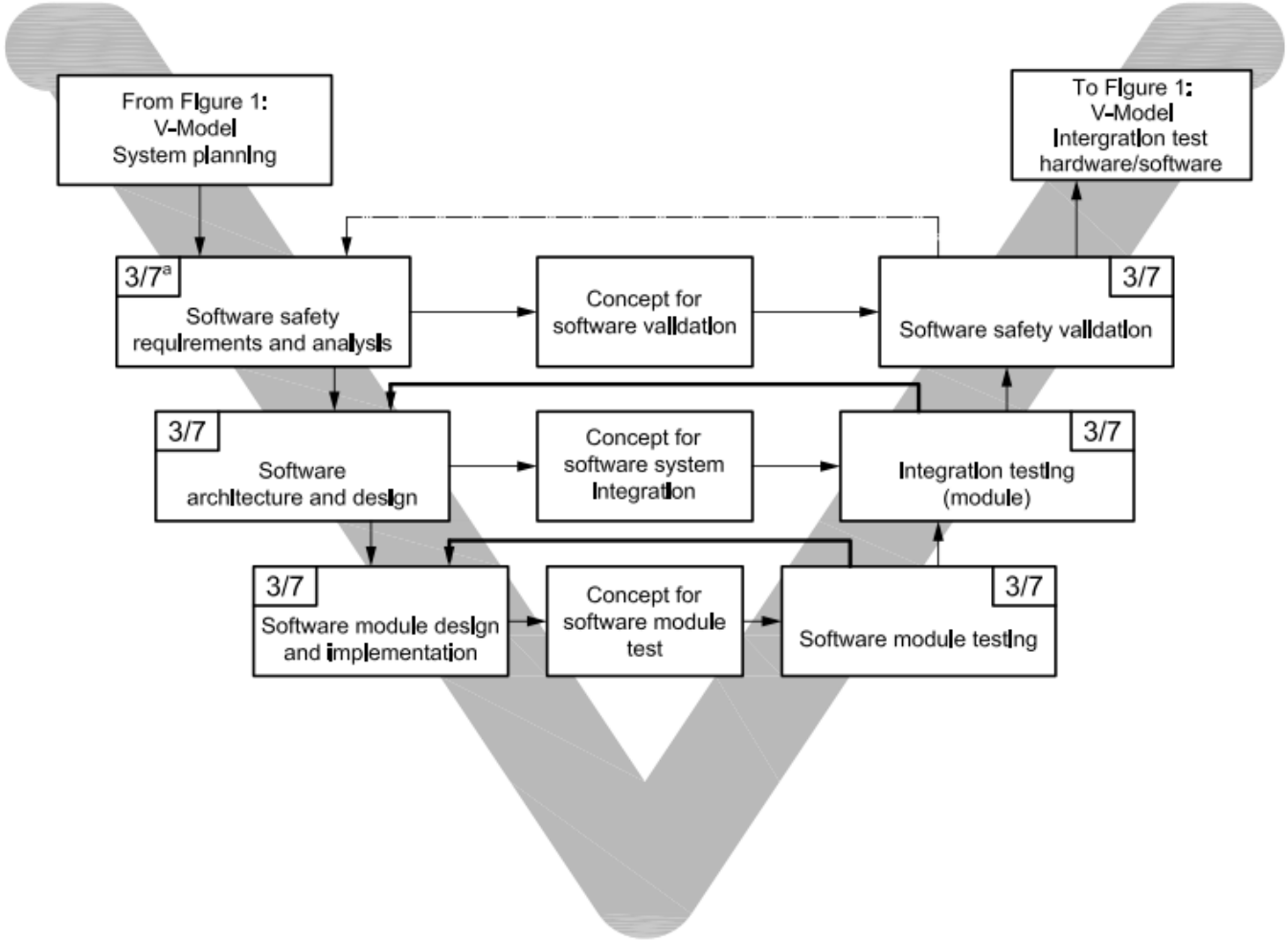
Hardware Design

The hardware development process shall begin at the system level where safety functions and associated requirements are identified

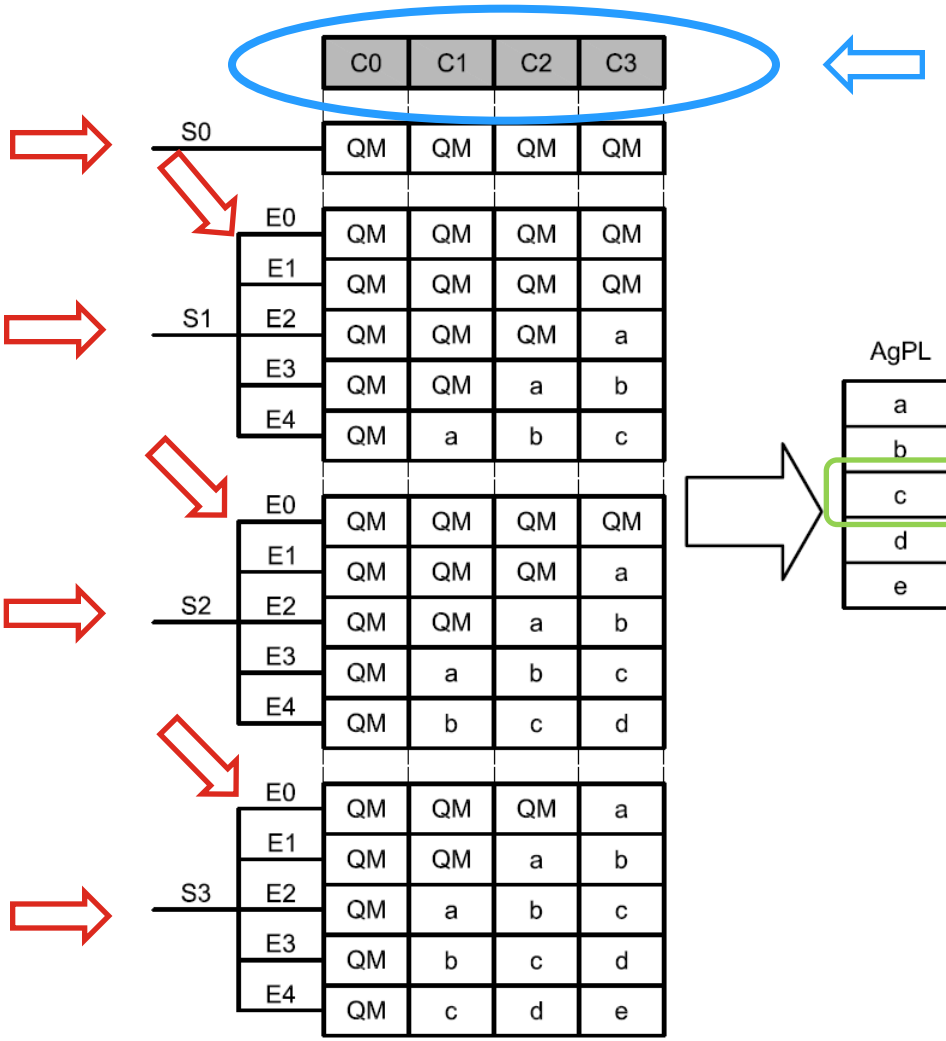


Software Design

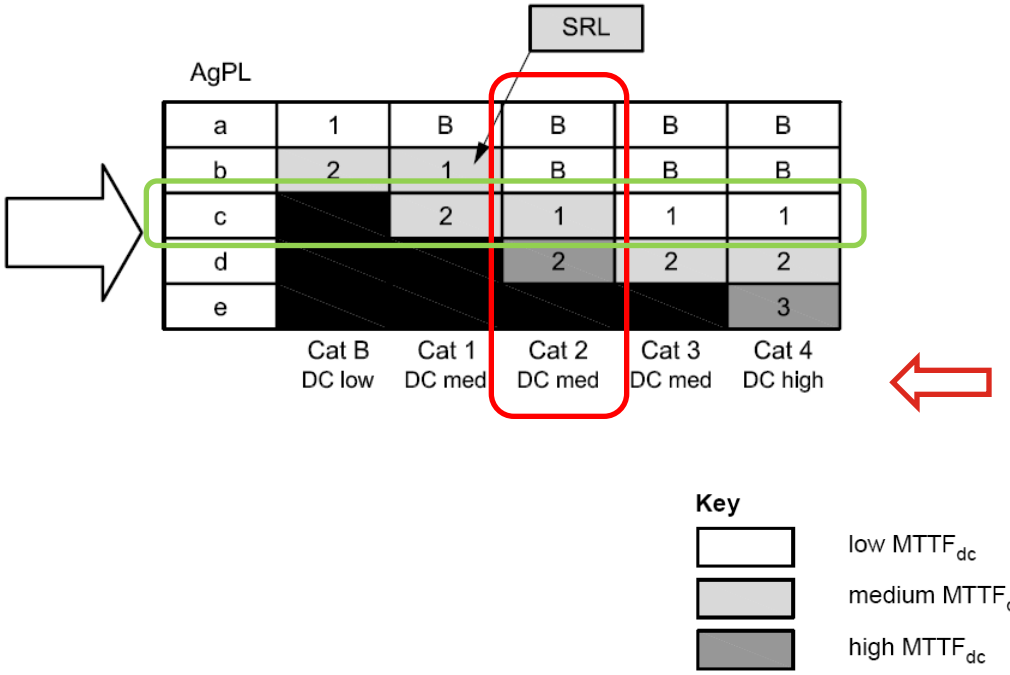
"Software Development planning" includes, tools, languages, methods, traceability.



The System Safety Performance (AgPL) and System Design

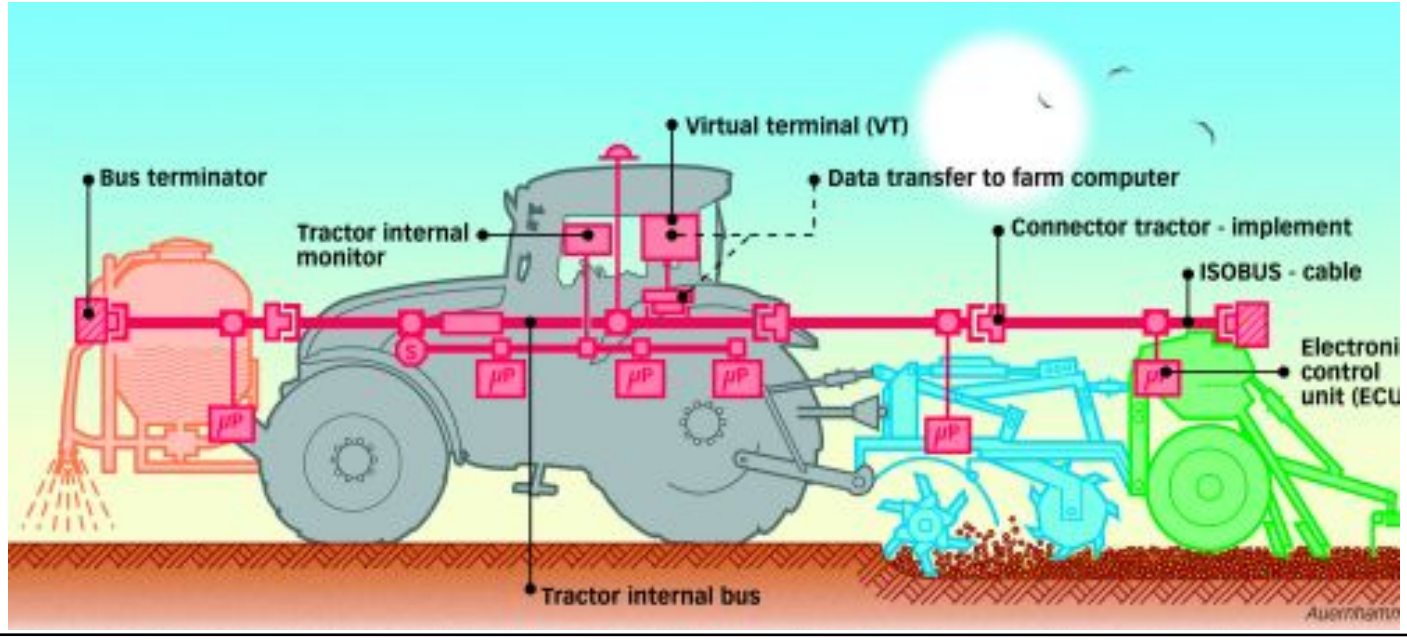


The Process starts with an Hazard Analysis where risk is related to severity of fault consequences, esposure to the safety related function and to the controllability of it.

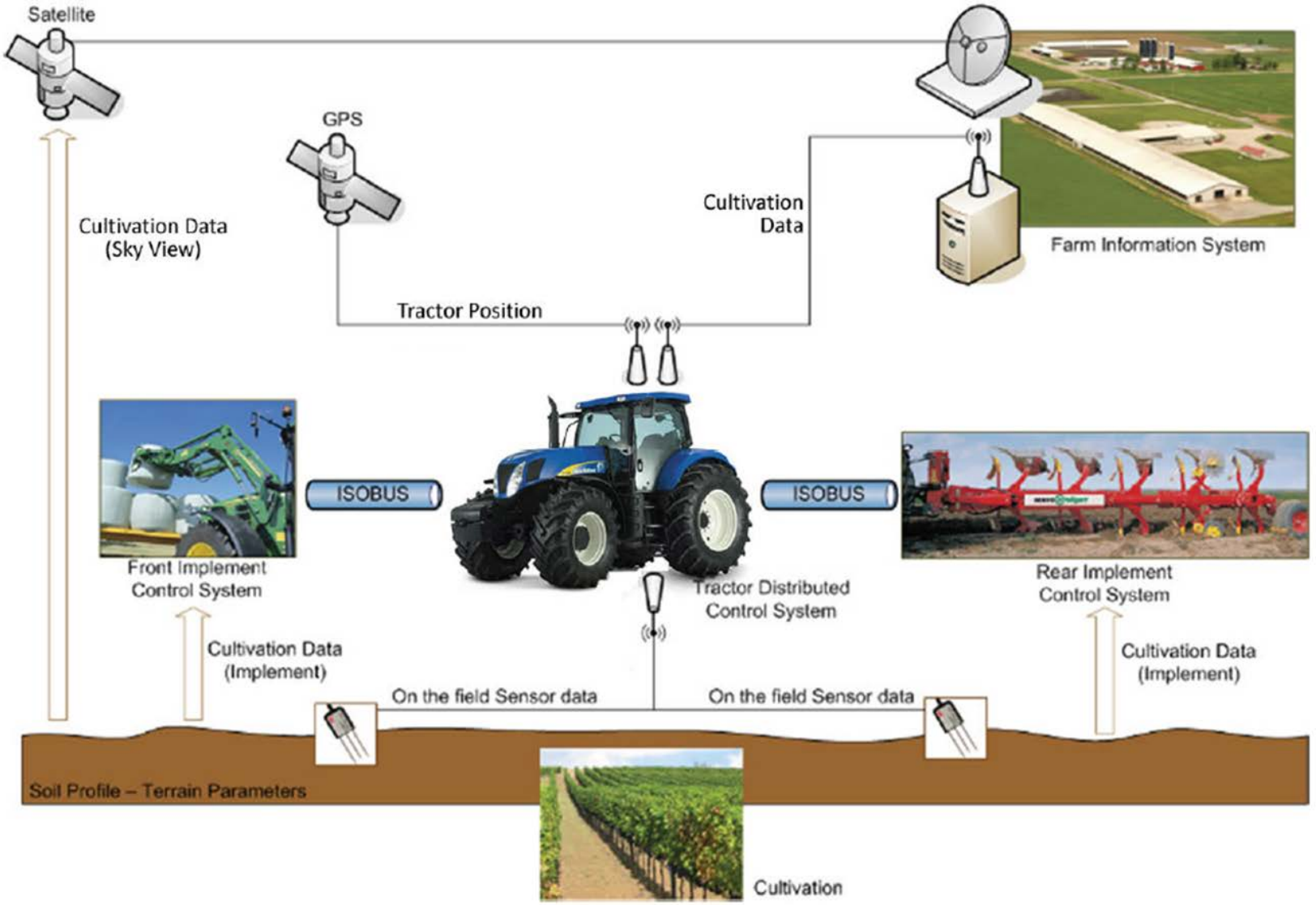


ISOBUS: Briefly the complexity explained

- **ISOBUS is a complex Plug & Play protocol that allows Agricultural Tractors and Implements working together, regardless of Brand;**
- **ISOBUS includes distributed control principles and structures for real DSC and Sequenced or automated operations;**
- **ISOBUS includes a complex process control that allows both programming of working sessions, collecting data, automating machine work and apply concepts of precision farming;**
- **Finally ISOBUS allows the connection with Farm IT Infrastructure in order to allow the Farm management control;**
- **ISOBUS is based on a single CAN network @ 250 kbit/s.**



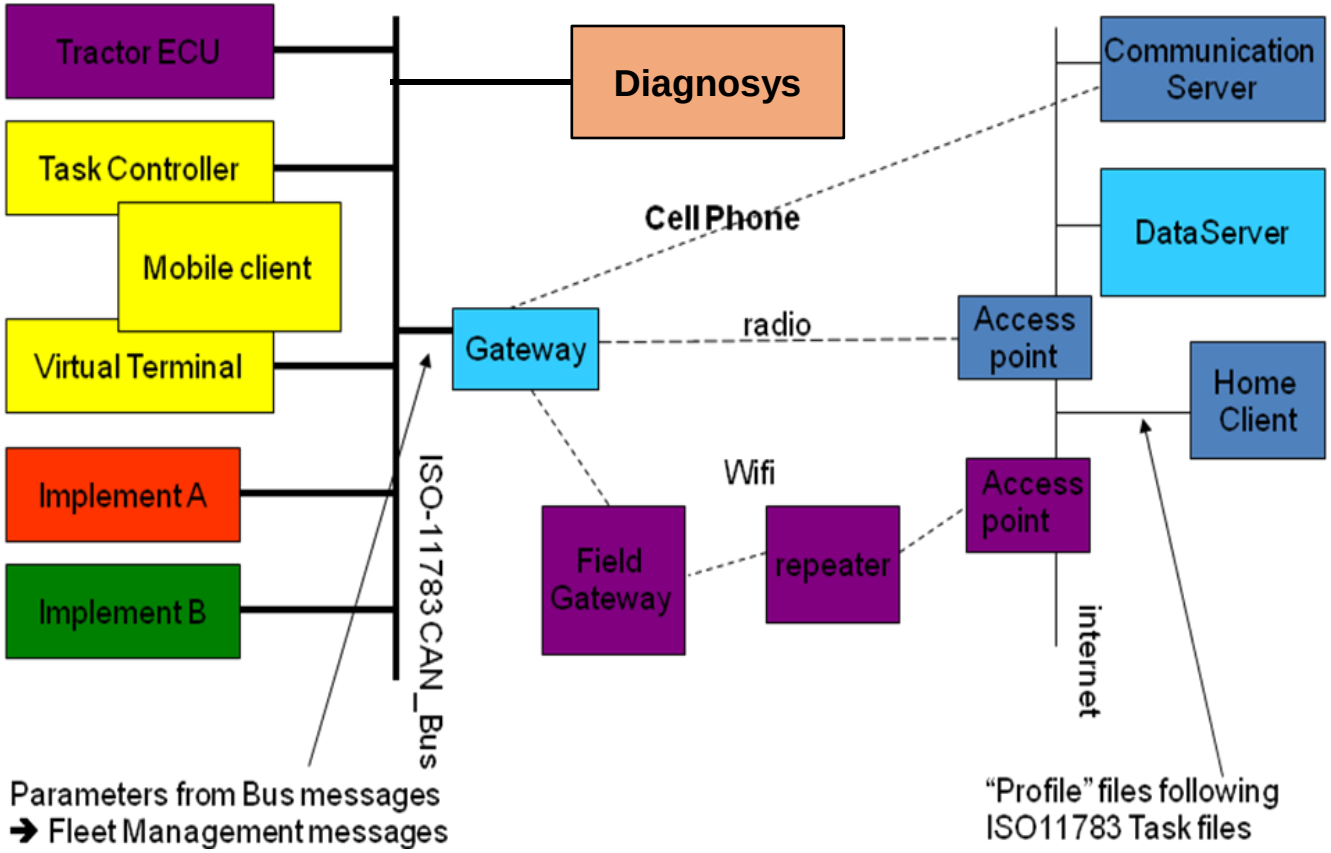
Is a Tractor with ISOBUS a «Closed System» in respect to Internet?



Is a Tractor with ISOBUS a «Closed System» in respect to local or remote heterogeneous connectivity?

No it isn't!

Both Fleet Management and Precision Farming ask for a openness for the access through Internet, diagnostics ask for a door available both on machine and through remote connection.



Is a Tractor with ISOBUS a «Closed System» in respect to CAN Network? (1)

No it isn't!

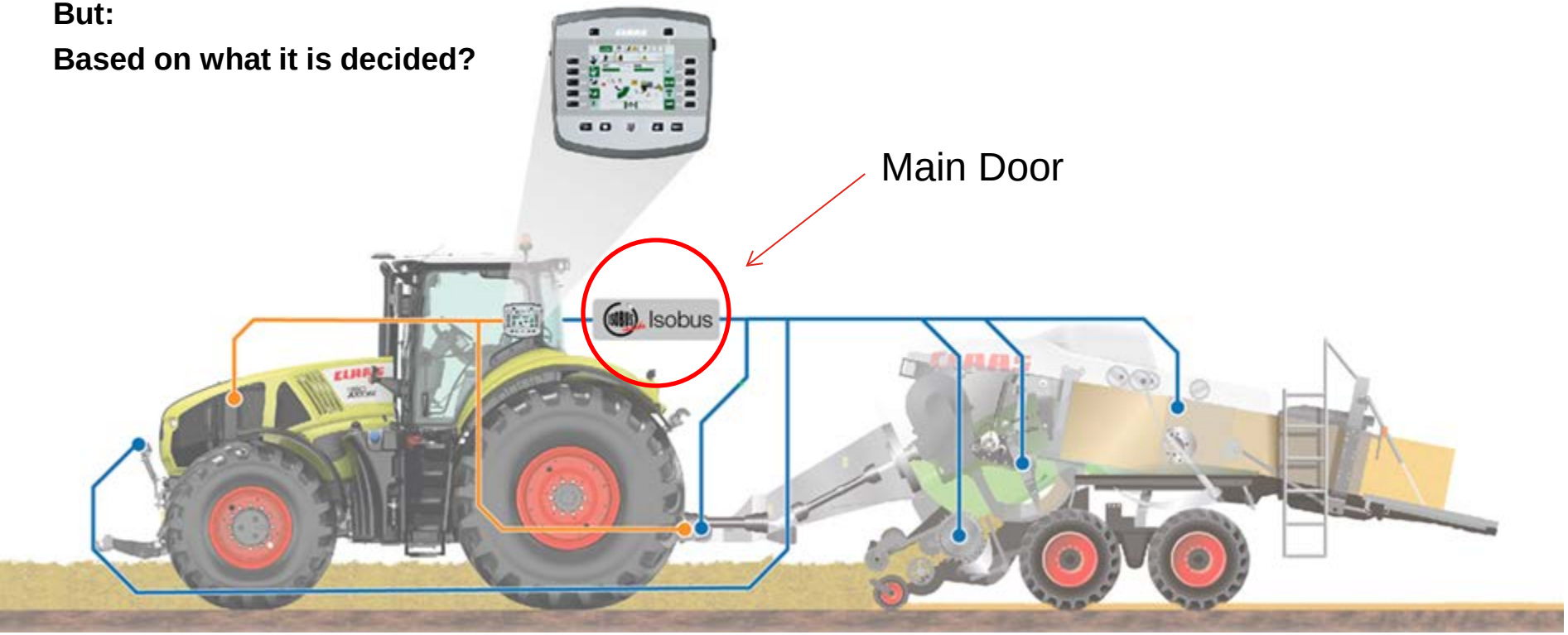
The ISOBUS Plug-ability and the ISOBUS itself make the network an open and hot-pluggable system, where more units can be connected and authenticated.

The Breakaway Connector is the perfect open connection to allow all kinds of attacks.

The Virtual terminal has the main function of allowing the usage of Functions to all implements that respect the ISOBUS standard.

But:

Based on what it is decided?

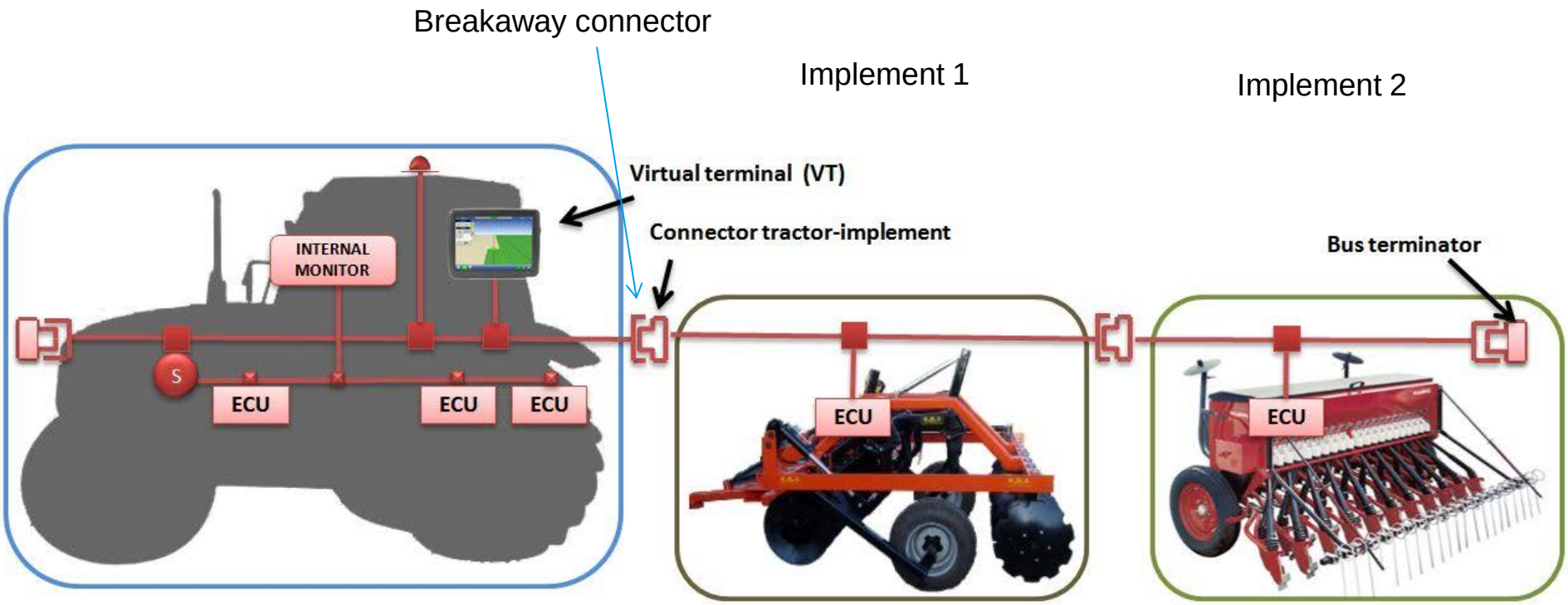


Is a Tractor with ISOBUS a «Closed System» in respect to CAN Network? (2)

In case of more implements, due to the CAN Network characteristics, one of them can affect the other ones' functionality.

The ISOBUS backbone is a real open system where implements are hot-plugged.

Both Implements are able to sniff messages of other one. A malfunction of one of these implement can affect the other one.



Does ISOBUS Offer Safety Critical Functions as defined in ISO 25119? YES

1. **VT;**
2. **Auxiliary Functions;**
3. **Critical Functions;**
4. **Class 3 functions:**
    1. PTO
    2. REAR HITCH
    3. FRONT HITCH
    4. SPEED/TORQUE
    5. REMOTE VALVES
    6. STEERING ANGLE
    7. CRUISE CONTROL
    8. SLIP CONTROL
    9. MAXIMUM DRAFT;
5. **Sequence Controller (Automated Functions);**
6. **Task Controller Features;**
7. **Tractor remote Control;**
8. **Class 3 TECU Related Controls (like point 4);**
9. **Navigation (GPS based);**
10. **Steering;**

Class 3 Functionalities allow real Process Control and real Remote Control, where the distributed control system manages the Tractor Power and direction with remote commands. The TECU has the responsibility to supervise the process based on the Tractor status and information available.

There are Possible Faults and Possible Attacks.

Possible (and most common) Communication Errors (Faults) on CAN

- **Loss of peer to peer communication;**
- **Unintended message repetition due to the same message being unintentionally sent again;**
- **Message loss during transmission;**
- **Insertion of messages due to receiver unintentionally receiving an additional message, which is interpreted to have correct source and destination addresses;**
- **Re-sequencing due to the order of the data being changed during transmission, i.e. the data is not received in the same order in which it has been sent;**
- **Message corruption due to one or more data bits in the message being changed during transmission;**
- **Message delay due to the message being received correctly, but not in time;**
- **Blocking access to data bus due to a faulty node not adhering to the expected patterns of use and making excessive demands for service, thereby reducing its availability to other nodes, e.g. while wrongly waiting for non existing data;**
- **Constant transmission of messages by a faulty node, thereby compromising the operation of the entire bus.**

BUT ISOBUS is SINGLE Channel = NO RECOVERY POSSIBLE in case of fault

Are attacks possible?

Yes, as long as there can be a local or remote connection to the network and the network is not adequately protected.

Some Automotive cracking cases, despite CAN network in passenger cars should be "closed systems":

1. Jeep remote control (1)
2. Cracking via aftermarket product (2) e.g. "for insurance" products or "ISO-Port connected" products (diagnostics, tuning etc…)

(1) Charlie Miller, Chris Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle", 23th DEFCON, 6-9 August 2015, Las Vegas, http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

(2) Ian Foster, Andrew Prudhomme, Karl Koscher, and Stefan Savage, «Fast and Vulnerable: A Story of Telematic Failures», 9th USENIX Workshop on Offensive Technology, 10-11 August 2015, Washington D.C. https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf

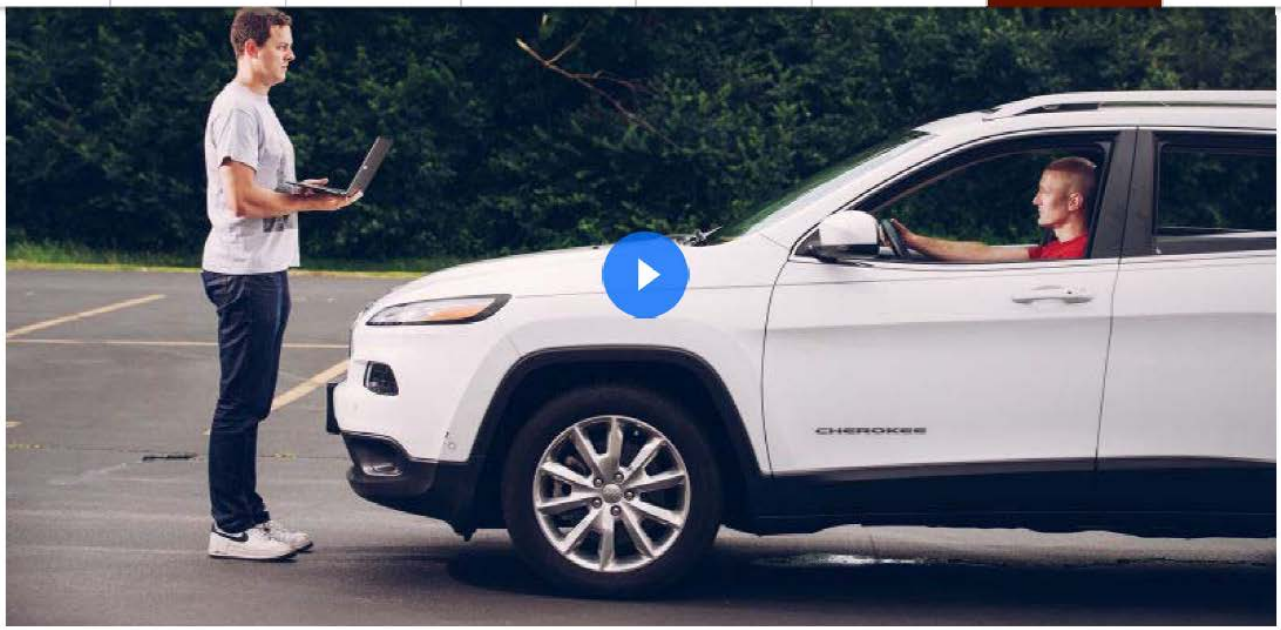
A very special History

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It SUBSCRIBE

BUSINESS DESIGN ENTERTAINMENT GEAR SCIENCE SECURITY



SHARE

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

And, after the scandal, …..

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Do We need a similar Experience?
I think we can work to prevent it!

Attacks on CAN networks

Are they interesting?

1. Unauthorized access to navigation data, statistics, task plan …
2. Use of cloned ECUs (Task Controller, Navigation, Automated Steering System, GPS, Implement ECUs with Class 3 features…..) for example to cheat the TECU,

…

The main topics to evaluate possible attacks are:

1. **A vulnerability on a part of the network (FMIS, 3G access, WI-FI, etc.) can provide access to other parts of the network (ISOBUS network, SAE J 1939, Diagnostics etc.);**
2. **The plug-ability of ISOBUS represents itself a vulnerability point to access to the whole ISOBUS network and the connected network;**
3. **Connectivity -> bigger attack surface (internet).**

Basic Attacks on CAN networks

CAN is normally considered a trusted network.

What if a malicious agent is able to connect to this network?

Sniffing:

I can listen on the bus and capture all messages, including sensitive information

Spoofing:

I can use other ECU's id, Name and Certificate to communicate on the bus, just sending messages with the right CAN id

Replay:

I can capture messages and then reply them on the bus

D.o.S., Denial of Service

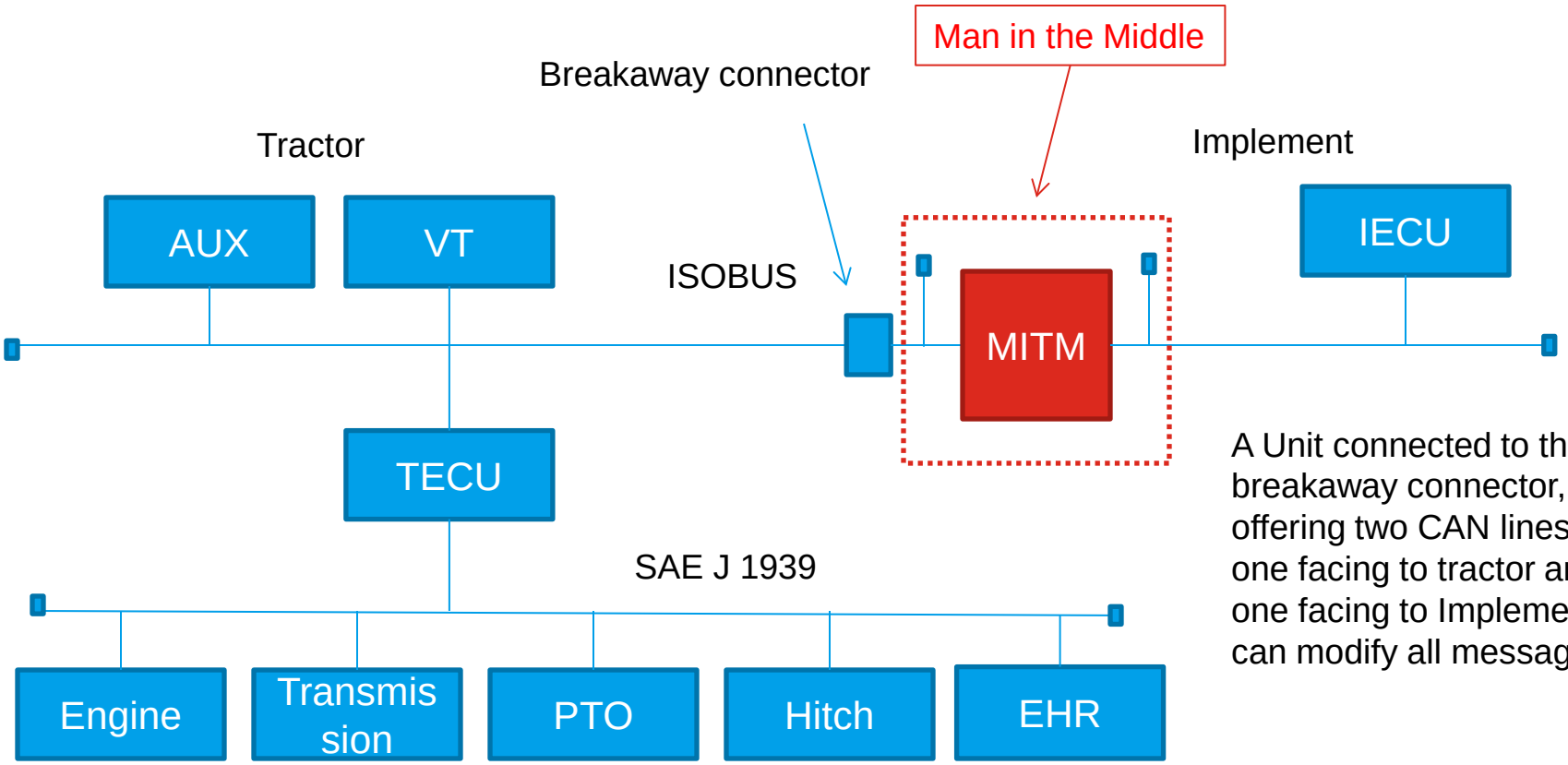
I can connect to a bus and with the right hardware I can disturb or block any communication (it is sufficient a connected HW with a wrong CAN speed).

Message forging

I can connect to a bus and, with the right hardware, I can modify a message on-the-fly (Man in the middle in two versions possible)

Man In The Middle (1)

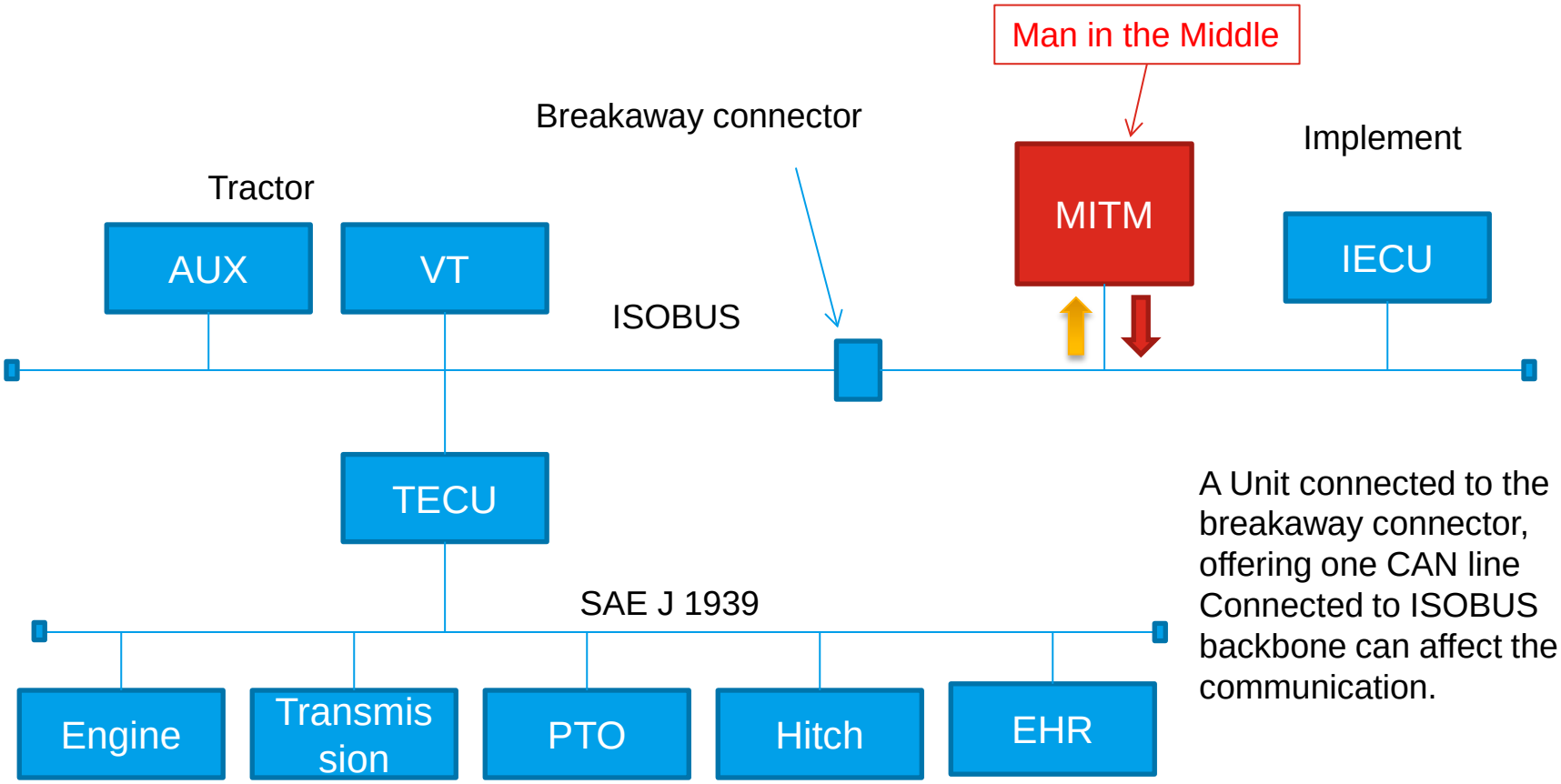
A simple unit with two can ports can “forge” messages. Messages can be received and modified on the fly before forwarding on the other sub-network .
Or the unit can simply sniff messages and collect critical information to be used with an Implement that is not in the AEF List of certified applications (name, certificates etc…).



A Unit connected to the breakaway connector, offering two CAN lines one facing to tractor and one facing to Implement can modify all messages.

Man In The Middle (2)

A simple unit with one can ports can capture and use information. Messages can be sniffed. Communication can be altered or blocked by a non-certified or malfunctioning electronic control unit. Wrong ECU Ids, wrong acknowledges, unauthorized activations of Class 3 functionalities….



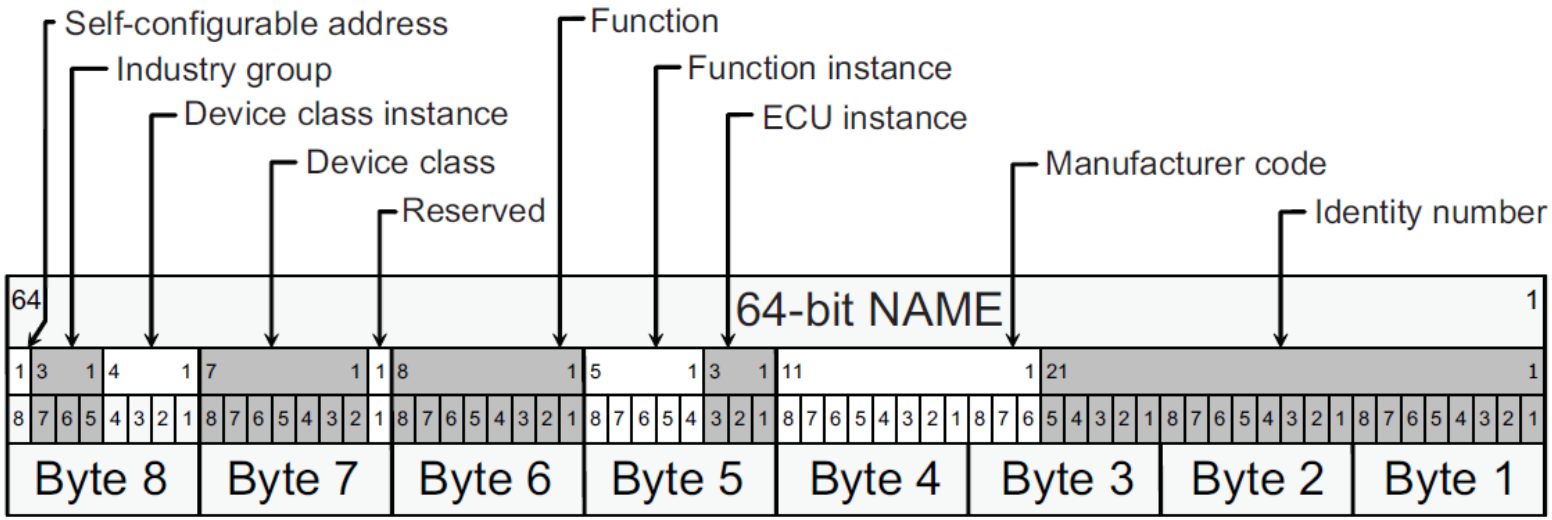
A Unit connected to the breakaway connector, offering one CAN line Connected to ISOBUS backbone can affect the communication.

The «Name» field, a Key to Open the Doors (1)

Some ISOBUS features are today based on the «Name» filed, the one used by the Control Function to connect to a network.

The Name field can be related to a Trusted Names or Trusted Sources Data Base in order to have a list of Names that are enabled to access ISOBUS functions and to ISOBUS Class 3 Functions.

But the NAME Field is transmitted unencrypted on the CAN network and it can be Sniffed.



The «Name» field, a Key to Open the Doors (2)

In order to make the authentication process more robust a «Compliance Certification Message» was added (ISO 11783-7 Appendix B.27, PGN = 0xFD42), where the «Compliance Certification Reference Number» field in byte 7 and 8 can be found.

But it can be copied or altered.

The only security measure is the possibility to query the AEF database in order to validate data (database only for members? For all? For registered users?).

Once the data are validated, the ISOBUS functions are available for the connected system.

And based on the TECU policy also class 3 functions can be activated.

No serial number is available in the database, only names and certificates.

Some constructors use Proprietary B messages to exchange authentication messages, but if these messages are not time variant and are clear in the network, they can be sniffed.

Good and Bad Habits: Auxiliary Inputs & Functions

Some good work was performed on Auxiliary Inputs. In fact with the **Auxiliary Type 2** definition it is possible to define a **«Critical Control»**.

A **«Critical Function»** can only be assigned to a **«Critical Input»**.

But some critical points are available on Auxiliary management:

1. The responsibility for function classification is up to the implement manufacturer;
2. The Maintenance Message Management;
3. The Status Message Management;
4. The Single Assignment Management vs. the Critical Definition.

Auxiliary Inputs: maintenance message Annex J.7.10

A maintenance message for all type 2 auxiliary was defined received by all ECUs, but with no safety measures (no running number),

But bytes 5 to 8 seems to be free……

Transmission repetition rate:			100 ms
Data length:			8 bytes
Parameter group number:			ECU to VT, sent to global address
Priority:			3
Byte	1	VT function = 35_{10}	
	Bits	7 - 4 0010	Command: Auxiliary Control
	Bits	3 - 0 0011	Parameter: Auxiliary Input Maintenance
Byte	2, 3		Model Identification Code of the Auxiliary Input Unit (Manufacturer defined) in the range of 0 – $FFFE_{16}$.
Byte	4		Status 0 = Initializing, pool is not currently available for assignment. 1 = Ready, pool as been loaded into the VT and is available for assignments.
Bytes	5 - 8		Reserved, Set to FF_{16}

Auxiliary Inputs: Status message Annex J.7.9

A status message for all type 2 auxiliary was defined received by all ECUs, but with no safety measures (no running number) so it's not possible to understand if the input has no changes or the Auxiliary is in a "babbling Idiot" condition (byte 8 bits 2 to 7 are free…….)

Transmission repetition rate:	Once per second and on change to a maximum of twenty messages per second. At least 50 ms shall pass between status messages for a particular input. Every 200 ms, when a non-latched Boolean input is held.
Data length:	8 bytes
Parameter group number:	When not in learn mode: VT to ECU, sent to global address by the Auxiliary Input unit when enabled. When in learn mode: ECU to VT, sent to the VT where the NAME indicates Function Instance zero.
Priority:	3

Byte	1	VT function = 38_{10}	
	Bits	7 - 4 0010	Command — Auxiliary Control
	Bits	3 - 0 0110	Parameter — Auxiliary Input Type 2 Status
Bytes	2, 3		Auxiliary Input Object ID (0-65534)
Bytes	4, 5		Value 1 (See Table J.5 — Auxiliary Function Type 2 types)
Bytes	6, 7		Value 2 (refer to Table J.5 — Auxiliary Function Type 2 types)
Byte	8		Operating State Bit 0 = 1 = Learn mode active Bit 1 = 1 = Input activated in learn mode, bit 0 must be 1 Bits 2-7 = Reserved, set to 0

For All the Auxiliary Functions (Critical and not Critical): Single Assignment

Auxiliary Functions can be defined “Single Assignment”, and then associated to a dedicated Auxiliary Input

This can increase the consistency of critical functions and safety functions management.

In fact in case of Single Assignment defined Function, the dedicated Auxiliary Input can’t be associated to a group function but only to the Single Assignment Function.

BUT

Due to the independent bits used to define a function critical and single assignment, in the ISOBUS standard it is possible to combine more critical functions to a single critical input.

See Table J.2 — Auxiliary Function Type 2 attributes and record format in ISO 11783 part 6 annex J

Bit 5 Critical Control 0 = this function may be controlled by any compatible Auxiliary Input. 1 = This function can only be controlled by a critical Auxiliary Input (see ISO 15077)	Bit 7 Single-assignment 0 = Function can be assigned with other Auxiliary Functions to same input 1 = Function shall not be assigned with other Auxiliary Functions to same input

Auxiliary Function in General

An Auxiliary Function can be associated only to Auxiliary Inputs

But a Implement Function can be associated both to a VT SoftKey and to an Auxiliary Function,

then the Auxiliary Function can be associated to an Auxiliary Input.

So the Implement Function is then associated both to a SoftKey and to an Auxiliary Input.

The choice is in the program of the Implement (it is responsibility of the Implement Manufacturer).

The Sequence Control

Sequence Controller is a real Automation System that allows sequenced operations.

Sequenced operations can be performed in open loop based on:

1. **Time**
2. **Distance**
3. **Georeferenced**

The protocol safety is ensured by the TAN (Transaction Number) numbers that are a good method to verify the status of the Sequence.

Then Sequence Control can only be affected by attacks but it seems enough protected from CAN errors or faulty participant ECUs

Attacks can change distance or GPS information affecting the right execution of the Sequence (but it's just an example and this kind of attack is a remote hypotesis, but not an error on calculating GPS based position!).

Virtual Terminal, Commands, Hazard Analysis and ISOBUS Certification

ISOBUS Certification does not require a Hazard/Risk Analysis for each application to be certified.

Then a function that should be logically defined as «critical» can be easily defined not critical and can be associated to a Soft-Key or to a button on the Virtual terminal, despite its criticality.

All the *command -> function* associations are certified without a risk analysis of the function safety Performance Level Required.

In this case the ISO 11783 certification and Safety Certification ISO 25119 compliant are not harmonized!

Not Only Problems!

Here some suggestions for increase ISOBUS Safety

- **Solutions for CAN Network Faults**
- **Solutions for protecting the access to functions only to real trusted systems.**

Other standards Suggestions: ISO15998 describes the Network Safety giving a summary of problems/countermeasures

Transmission error	Measures per message							
	Running number	Time stamp	Time expiration	Reception Acknowledgement	Identification for sender and re-ceiver	Data integrity assurance	Redundancy with cross check	Different data integrity assurance systems of SR and non-SR messages
Repetition	**x**	**x**					x	
Loss	**x**			**x**			x	
Insertion	**x**			**x**[a]	x[b]		x	
Incorrect sequence	**x**	**x**					x	
Message falsification				**x**		x	x[d]	
Retardation		**x**	x[c]					
Coupling of SR and non-SR information				**x**[a]	x			x

a depends on application

b only for sender identification. Detects only insertion of an invalid source

c Required in all cases and can implemented in the sink of messages in case of a static map of messages to be received

d This measure is only comparable with a high quality data assurance mechanism if by calculation it can be proved that the residual error rate Λ reaches the values according to in Paragraph “Data Integrity Assurance” if two messages are sent through independent networks or network addresses and hardware.

But practically Speaking?

SAE J1939 is moving toward safety aspects with some small steps:

TSC1 message structure is now:

	bit1	bit2	bit3	bit4	bit5	bit6	bit7	bit8
Byte1	Eng.Ov.Cntrl.Mode		Eng.Req.Sp.Cntrl.Con.		Overr.C.ModePrio.		EngineReqS./S.lim	
Byte 2	Engine Requested Speed/Speed Limit (0,125 rpm/bit) (2 byte)							
Byte3								
Byte 4	Engine requested Torque/Torque Limit (%) (1byte)							
Byte5	**TSC1 Transm. rate**			TSC1 Control Purpose				
Byte6	Eng. Req. Torq. Fractional							
Byte 7								
Byte 8	**Message Counter**				**Message Checksum**			

Allows setup of Timeout And time expectation in the receiver

Protect from lot of faults Loss, sequence, repetition…

Reduces Failure per Hour is the Safety code lenght

Security over ISOBUS some Proprietary Solution

Some Companies applied a proprietary solution. The presence of a Tractor and a Implement of the same brand allows some functionalities that are not available in the standard ISOBUS offered by the Tractor.

How is it possible?

In that case security is made using the Proprietary Messages feature: once the Implement is recognized in the network, the VT, the Auxiliary and the TECU can send proprietary messages and arrange for the usage of some special feature and/or automation not available for implements of different constructors.

This is normally called: Security through Obscurity. And it is based on the secrecy of the protocol.

But it can be sniffed.

The security of this solution is a weak solution and it is strongly discouraged by standardization bodies.

https://en.wikipedia.org/wiki/Security_through_obscurity

”Security through obscurity is discouraged and not recommended by standards bodies. The National Institute of Standards and Technology (NIST) in the United States specifically recommends against this practice: "System security should not depend on the secrecy of the implementation or its components.”

Authentication in other available protocols

ISOBUS doesn't offer authentication procedures.

While in SAE J 1939 and in KWP 2000 some mechanism where introduced in order to perform secure upgrade of ECUs firmware.

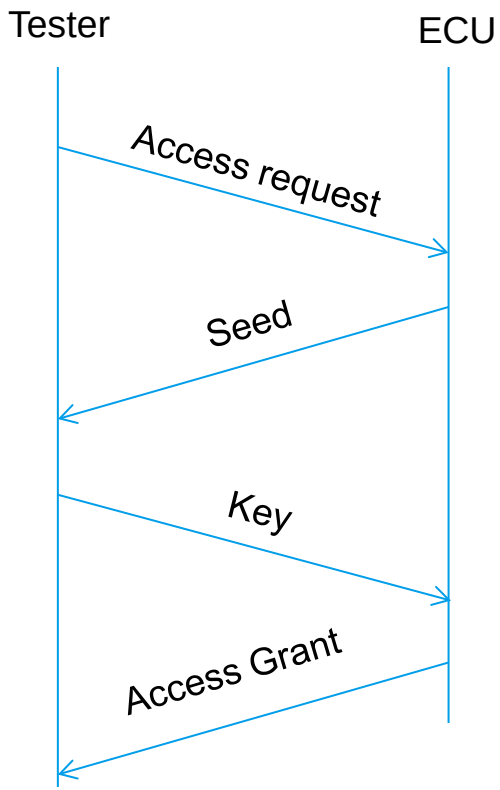
It is called Seed & Key protocol and it is used to access special ECUs functionalities, like:

- **Firmware upgrade,**
- **Safety disable (for test)**
- **Active diagnosis**
- **Calibration…**

It is a simple XOR, where normally the Key is equal to a Fixed Number XOR the Seed

The Seed & Key protocol should be more secure

As an example an Asymmetric Key should be available, in order to be used to create a symmetric key as a function of public and private keys and to be used for real time communication



How to protect the CAN bus

1. **Add encryption (for sniffing)**
2. **Add authentication (for spoofing, forging)**
3. **Add time-dependent protection (for replay, spoofing, forging)**

Limits of CAN:

- Short messages (8 bytes), real-time messages can not be split (standard database and real time data consistency);
- Full payloads! No free space available in the ISOBUS messages;
- Shared bus, every ECU sees all the traffic (easy D.o.S.);
- Public SAE J1939 database and public ISO11783 database and communication/authentication methods;
- Messages in clear;
- Public authorized Names (in the future).

Encryption over CAN

Direct plaintext encryption with symmetric block cipher:

max 64 bit key, needs proper key management and refresh. 56-bit keys could be cracked in a few days back in 1998(1), in a few hours in 2009, now probably in a few minutes (with the right hardware);

Symmetric block cipher in counter mode -> operates as stream cipher:

128 bit key and 64 bit ciphertext -> strong security, but needs distributed information (counter, timestamp, …), not available in current networks

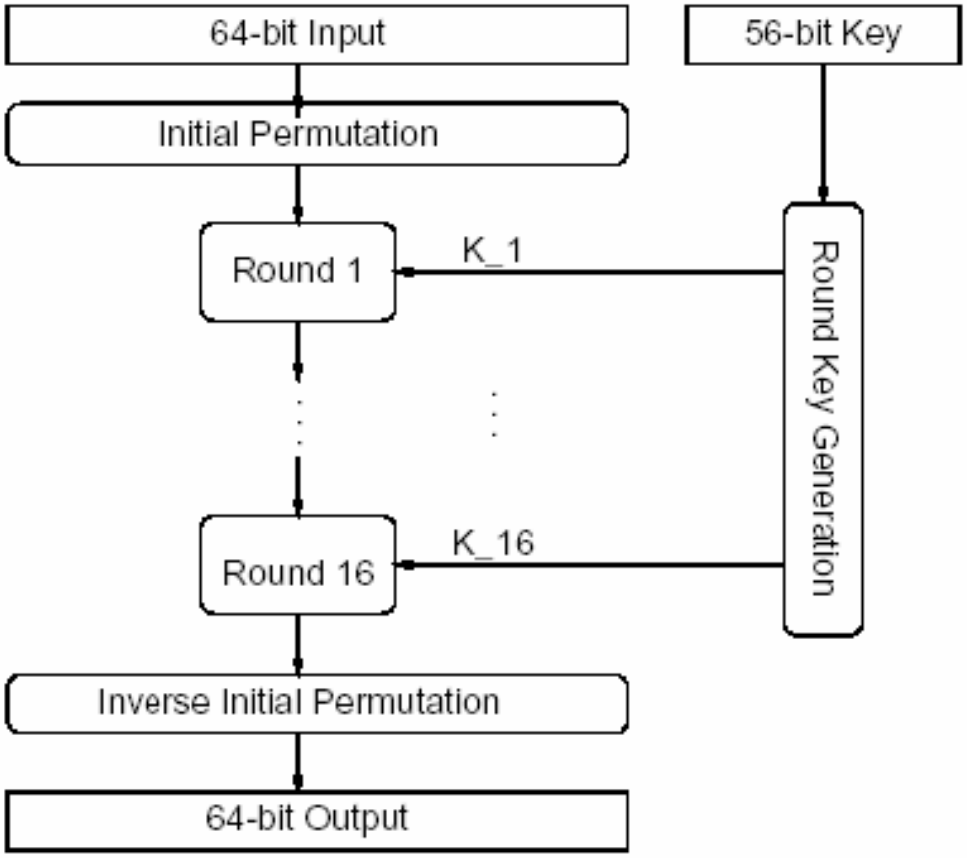
(1) “Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design” Electronic Frontier Foundation, O’Reilly Media, 1st Edition July 1998 (US) 272 pages, Print ISBN: 978-1-56592-520-5 ISBN 10: 1-56592-520-3

Encryption over CAN: symmetric Key encription

An example of the Feistel Scheme for a symmetric based data encription is shown.

Using a 56 bit key, a 64 bit payload can be crypted, based on a shared symmetric key (and shared Initial permutation).

The famous DES algorithm is based on it.



Authentication over CAN

Add authentication tag to messages

- Needs spare bits on a message, many CAN messages have none
- Limited tag length, weak protection

Use encryption + integrity check

- Integrity tag must be added on 64-bit message
- What is the probability of random guessing a correct message? (open point)
- With good encryption algorithms: Probably same problem as above

Real time CAN

Good encryption possible with pre-shared, time-variant information -> need to develop new protocols, some partial work exist in literature (1)

Good authentication difficult or impossible, can not send a message with data and another with the authentication tag, would introduce too much delay (and what if either one of the messages is lost?)

(1) C.-W. Lin and A. Sangiovanni-Vincentelli, “Cyber-security for the Controller Area Network (CAN) communication protocol,” ASE International Conference on Cyber Security, pp. 344–350, 2012.

Non real-time CAN

Can split data in 64-bit chunks and use a Transport Protocol, allows to use strong encryption without additional information.

Can use longer authentication tags, allows to use asymmetric crypto (ECC) and certificates to identify ECUs.

ECC = elliptic curve Criptoraphy

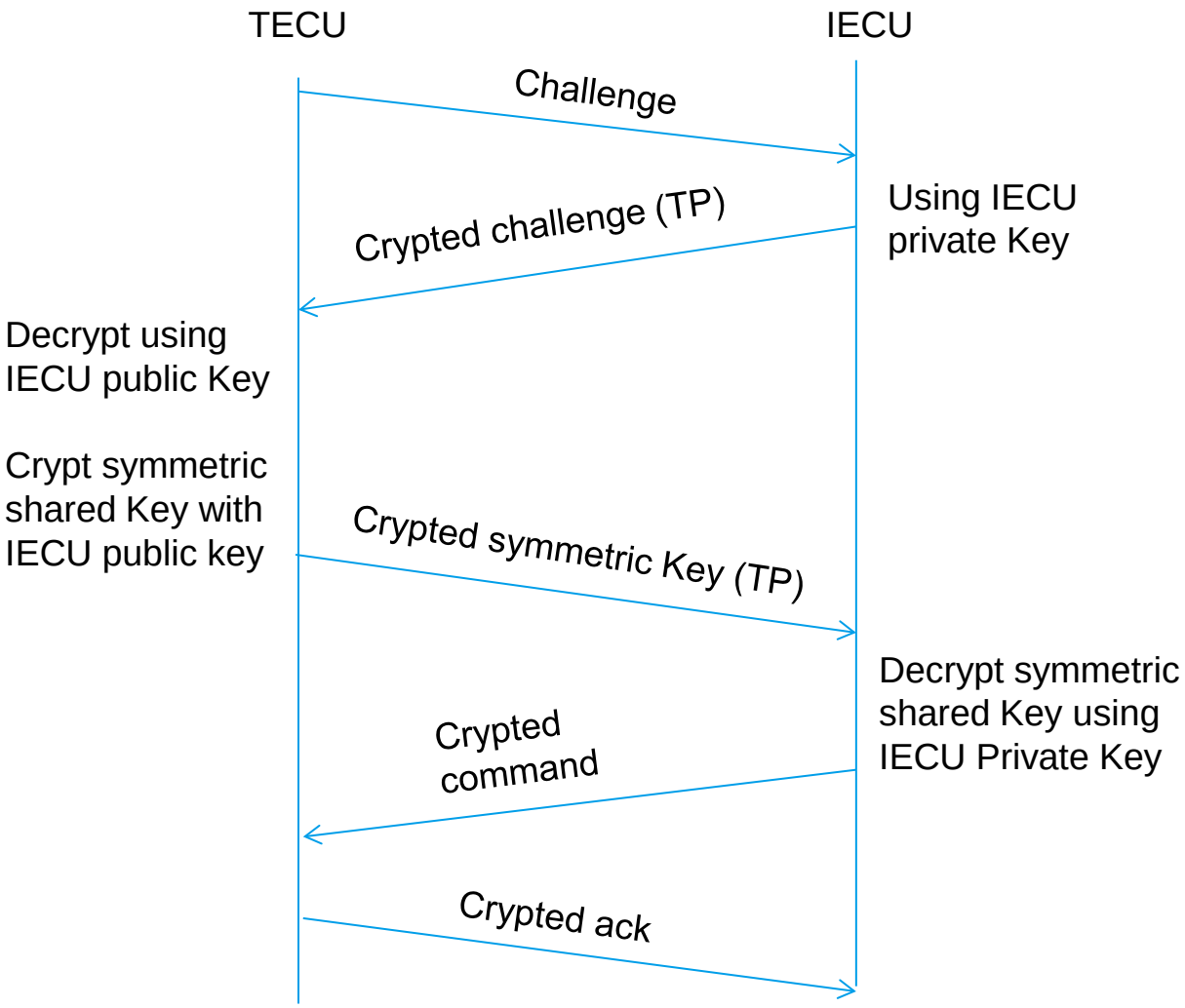
It’s an Asymmetric Algorithm, like the famous RSA but with shorter keys

Cetificate = public key with a signature of a different subject.

A possible solution for Encryption over CAN

Using Asymmetric keys in authentication phase (non real time CAN)

And using symmetric keys (fast) during working sessions (real time CAN).



Conclusion

Safety is not the best quality of ISOBUS protocol.

Practically speaking the main problems are related to a high freedom in design of Control Functions, that can lead to a hazard as a consequence of a malfunction.

Then faults on CAN network and on components (Inputs) can lead to a Hazard.

Attacks on CAN are possible but are strongly dependent from the market and from untrusted competitors that are now unlikely.

Some solutions here shown could be used to try to arrange a better ISOBUS from the Functional Safety point of view.

Q & A

Thank You for Your Kind Attention

Questions?

Ing. Ruggeri Massimiliano
CNR – Ferrara
email: m.ruggeri@imamoter.cnr.it