ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

DB Mobility Networks Logistics

openETCS

openETCS: An Idea becomes Reality

First "Open Proofs" Implementation for the European Train Control System

supported by:

Federal Ministry of Education and Research

Région de Bruxelles-Capitale

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

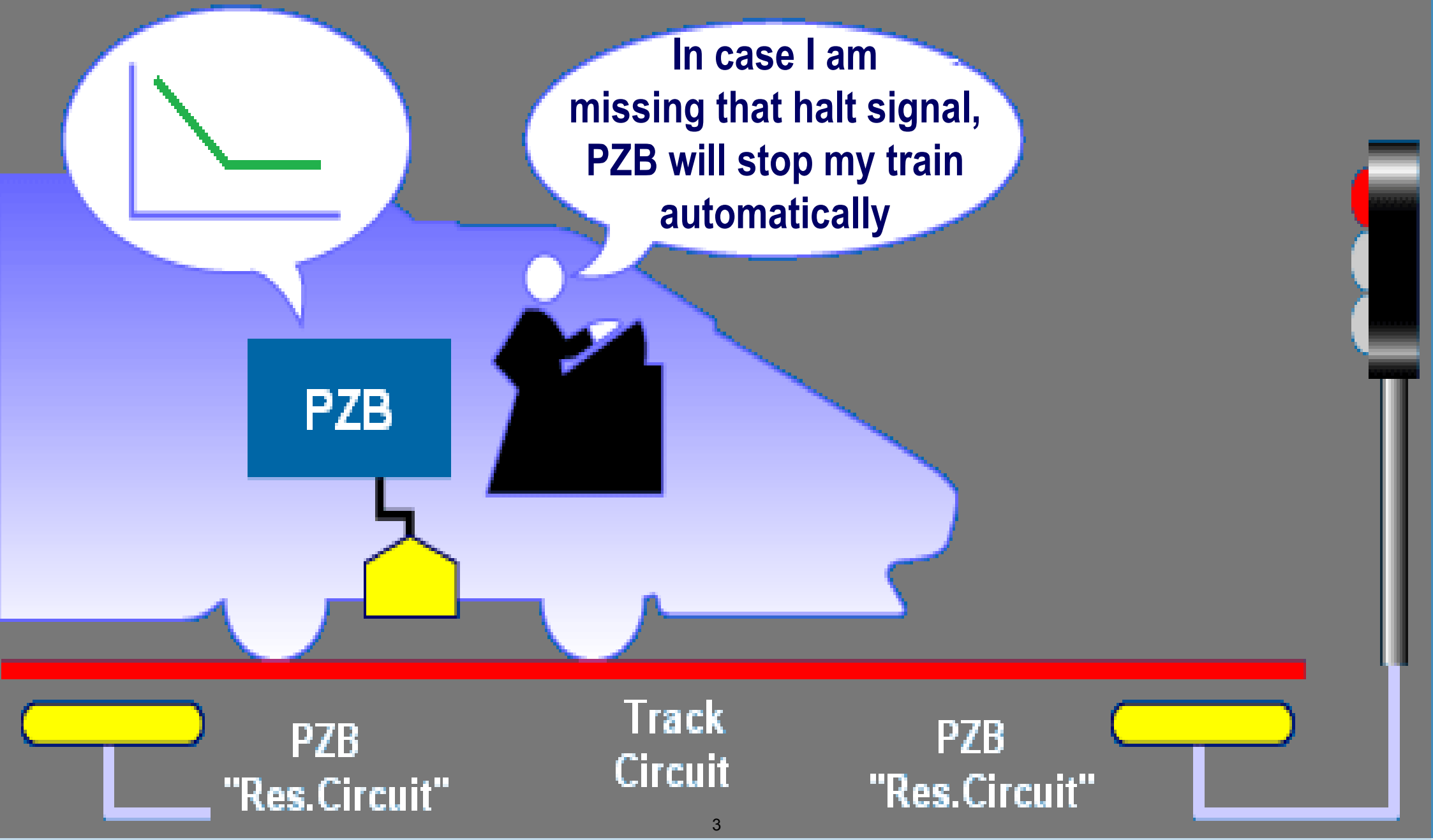
openETCS@ITEA2 Project

Klaus-Rüdiger Hase, DB Netz AG

INNOTRANS 2014, Berlin 24.09.2014

Signals need ATP: Drivers can make mistakes

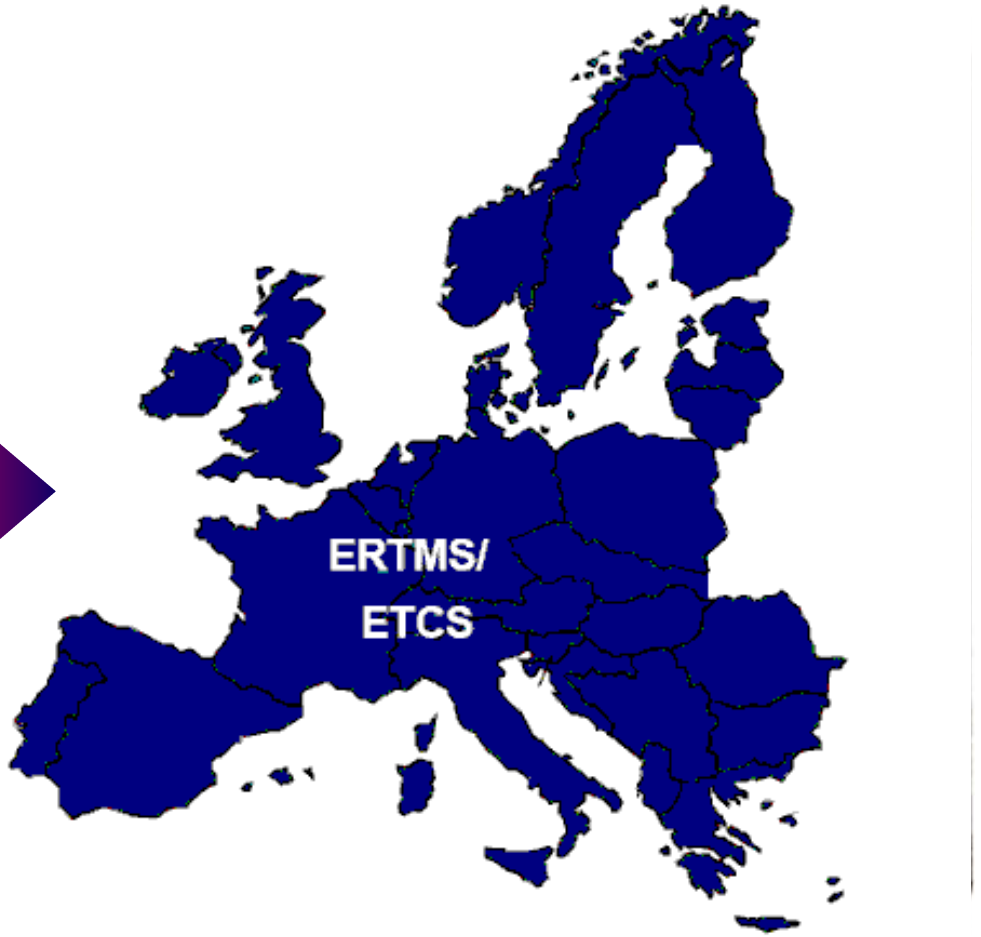
Automatic Train Protection (e.g. PZB since 1934)

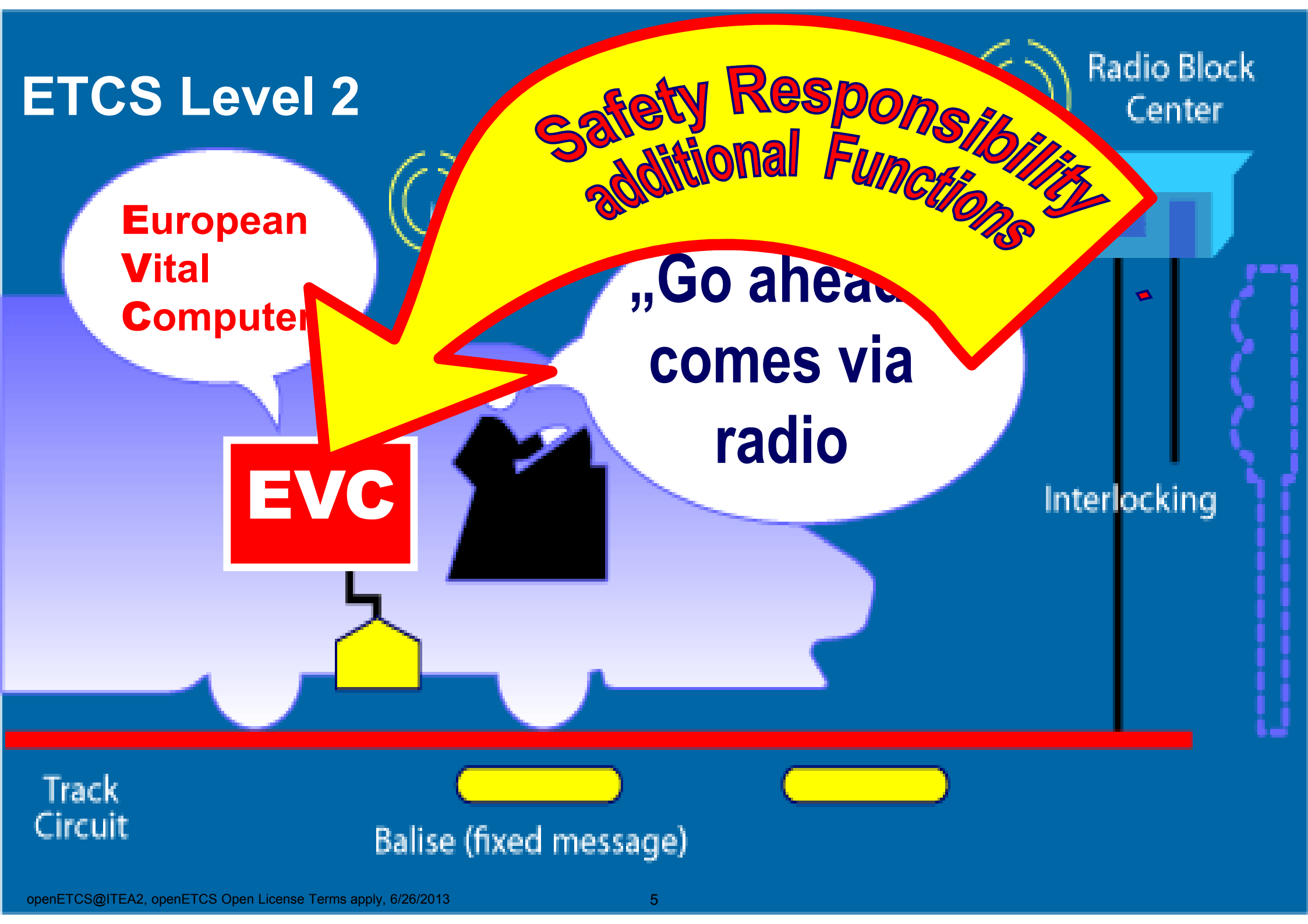


European Signaling Diversity due to History

Today: Diversity

Future: Unity




ETCS Level 2
Safety Responsibility
additional Functions
Radio Block
Center
European
Vital
Computer
„Go ahead
comes via
radio
EVC
Interlocking
Track
Circuit
Balise (fixed message)

BUT … Mission NOT Completed Yet

Until today:

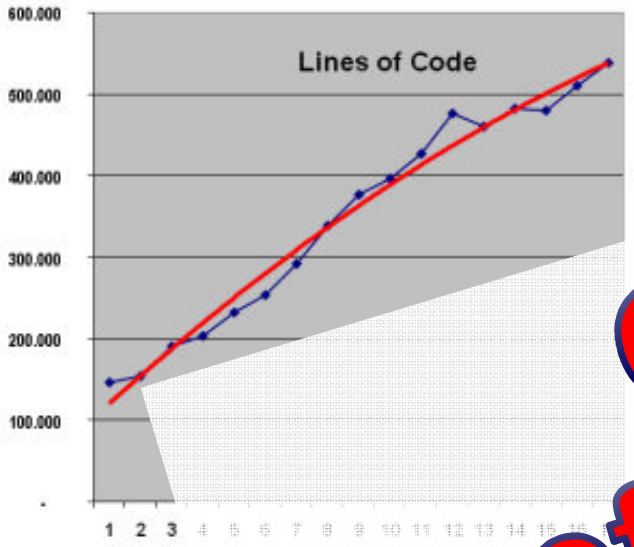
Not a single ETCS train set has been approved to operate on all ETCS lines !

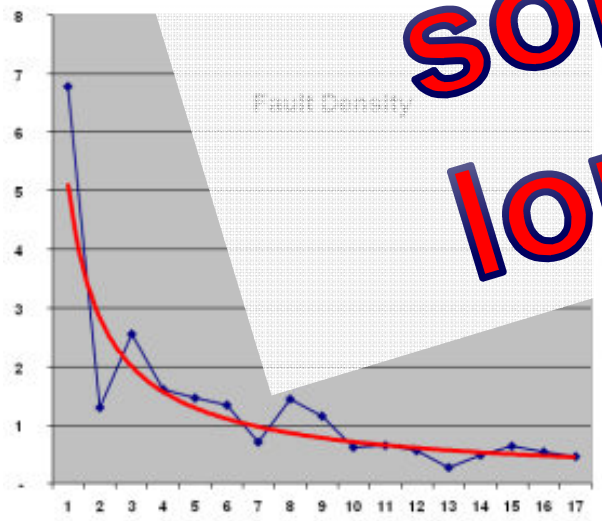
ETCS: A pure SOFTWARE project

- All hardware components, well known since the 1980th

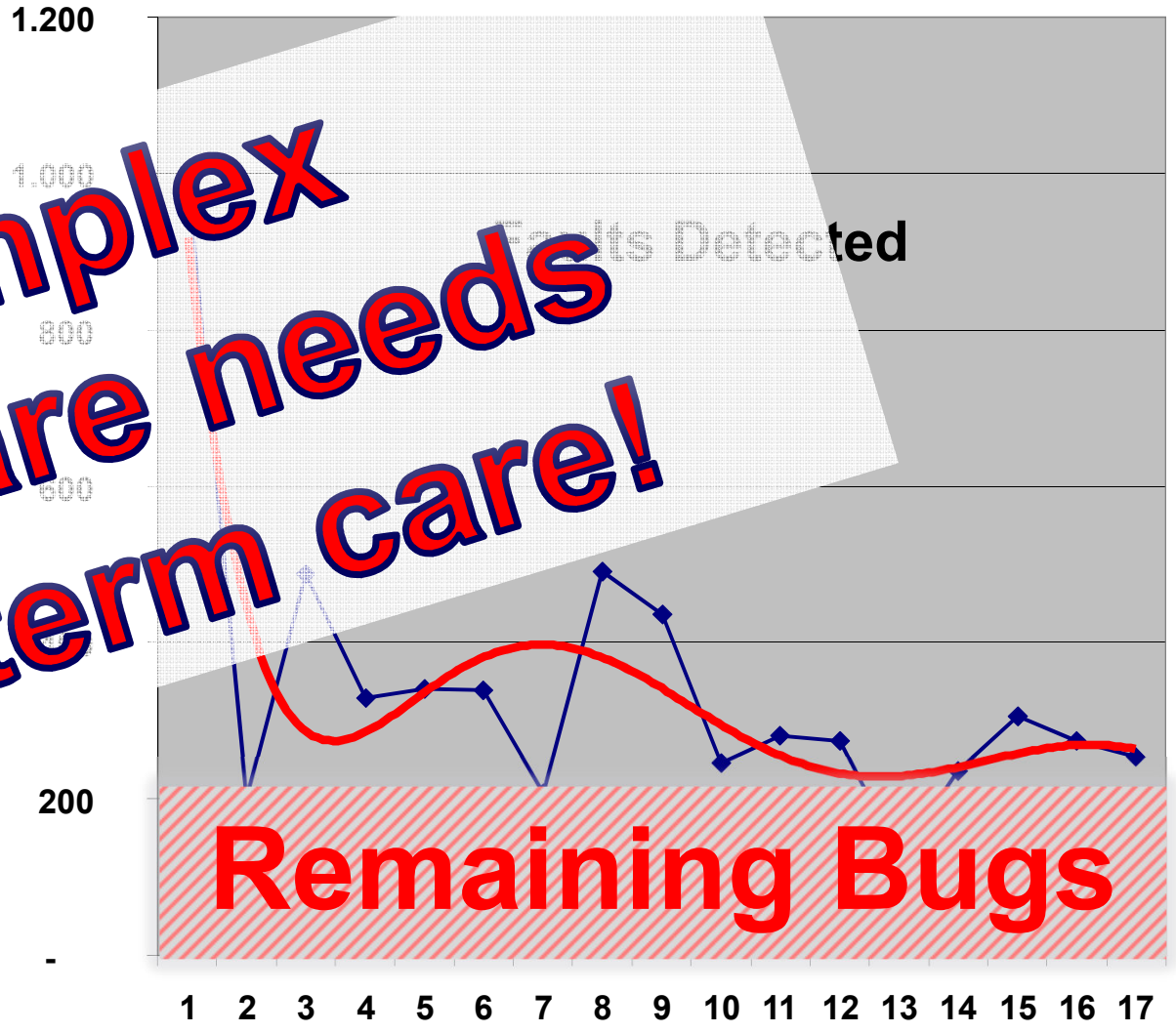
- SOFTWARE is not just bits & bytes, it is the immaterial part of a system

Characteristics of Complex Software





Complex software needs long-term care!



Computer worm triggers worldwide alarm

STUXNET was attacking safety critical systems.

What about ETCS?

Systems assault

Computers infected by Stuxnet virus worldwide
By country (%)

Q&A
Wriggling its way

Why is Stuxnet different?
It is the first time a worm has attacked the software that runs industrial operating systems.
Analysis by Siemens and security experts indicated the hackers were working as a team, and had a lot of IT knowhow – and money. The hackers also had an in-depth knowledge of their intended targets.

What has happened so far?
Siemens said 15 of its customers worldwide had reported finding the virus in their systems and had removed it. Siemens said no virus attacks had been reported since Microsoft patched the vulnerabilities.
Symantec, one of the companies tracking the virus, said it was unclear what the purpose of the attacks was, but said most of them appeared to have occurred in Iran, and a significant number in India and Indonesia.

Why are experts worried?
Once the worm enters the industrial controls systems it hides itself from most forms of monitoring.
It can be used for sabotage. The worm reverses the normal commands issued to facilities, which could include directives on pressure valves and a range of other functions.

Mary Watkins and

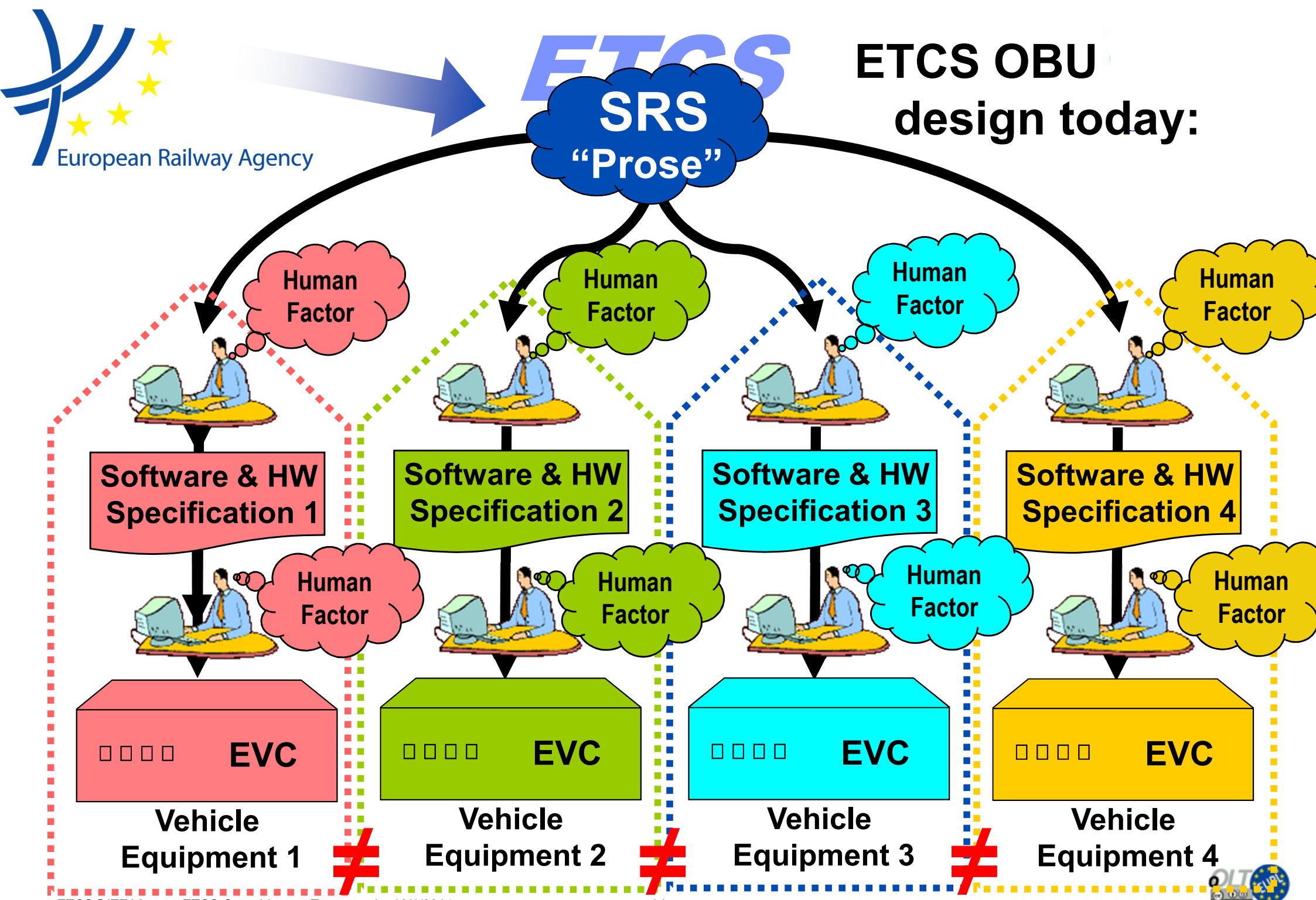
Polish teen derails tram after hacking train network

A 14-year-old Polish boy turned the *tram system* in the city of Lodz into his “train set”. He used a modified *TV remote control* to *change track points*, and *derailed four vehicles. Twelve people were injured.*

The Telegraph

European Railway Agency

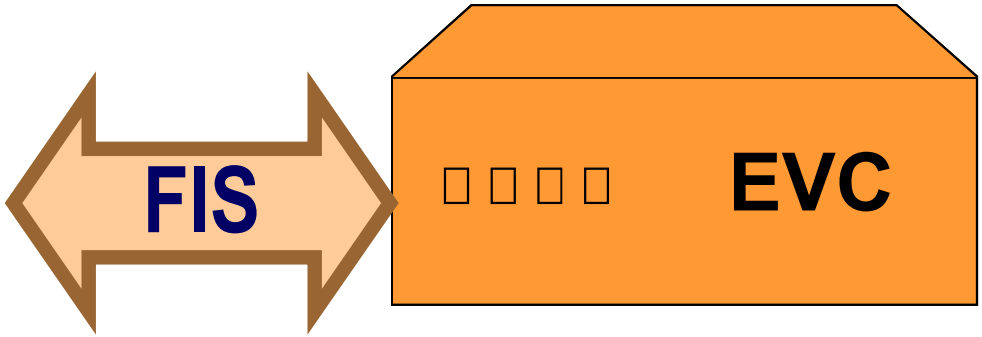
ETCS OBU design today:



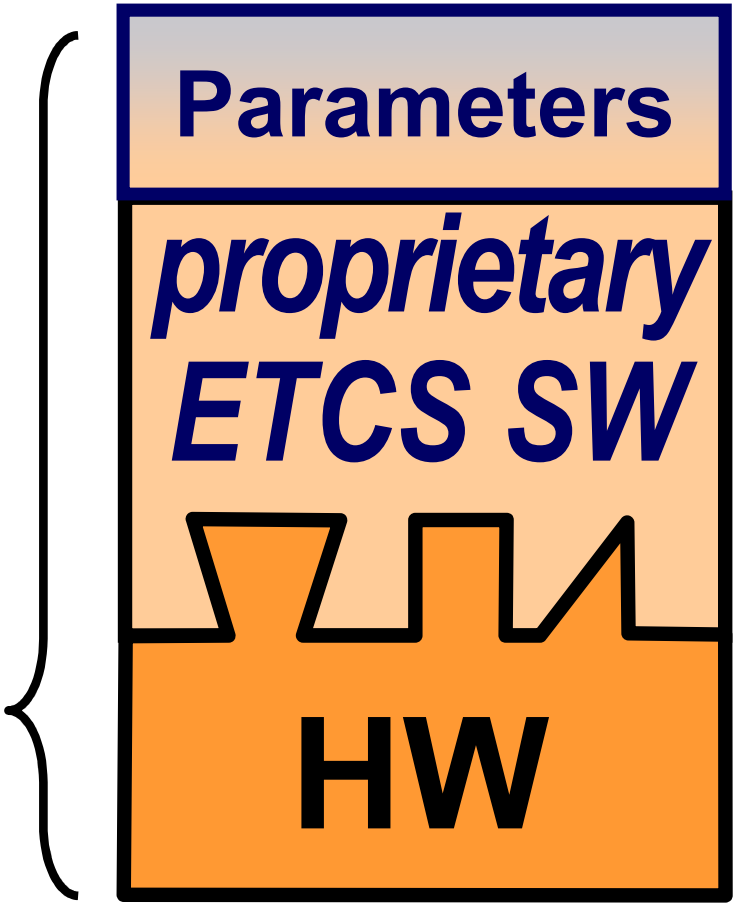
Low Level of Standardization Today

Most hardware, software and interfaces are proprietary design

➔ Vendor Lock-in



Vehicle Equipment



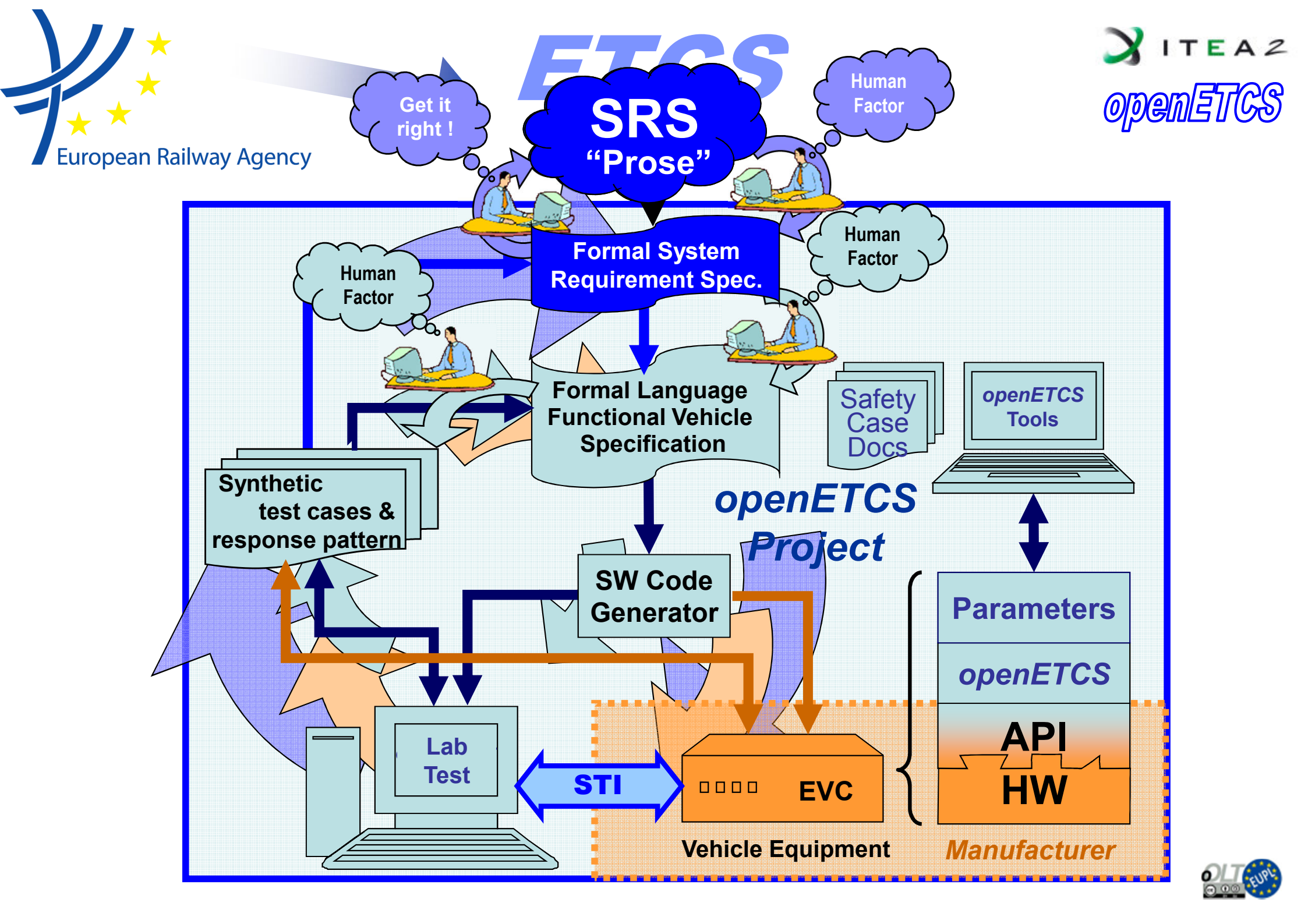
How to improve?

Lower Complexity	➔	1. Standardization
Reduce Ambiguities	➔	2. Make it “Formal” ➔ “Reference OBU”
Master “Bug” Surprises	➔	3. Life-time Service
No Vendor Lock-in	➔	4. “Open Proofs”

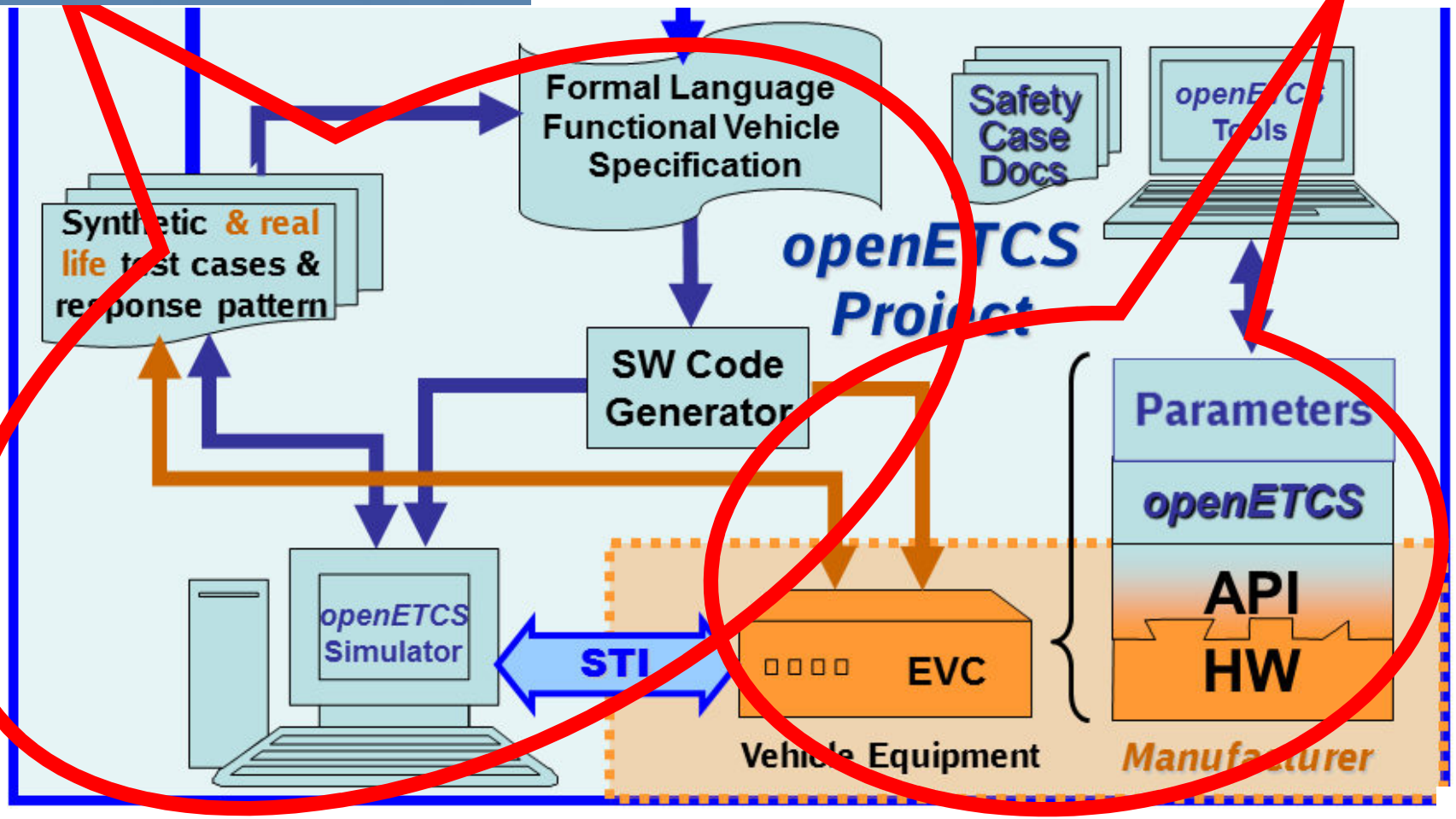
Institute for Defense Analyses, a US military think tank

- "Open proof" (new term):
  - Source code, proofs, and requi
- Anyone can examine/critique collaborate with others for im
  - Not just software, but what's pr
  - Example for training, or as usef
- Extends OSS idea for high assu
  - Enables legal collaboration
  - Similar to mathematics field
  - Method for speeding up tech transition
- Goal: Make supplier identity irrelevant
- Don't need *everything* to be an open proof
  - Examples & building blocks (inc. standards' API)

Mathematicians publish a new lemma and its proof including used tools or methods for centuries.

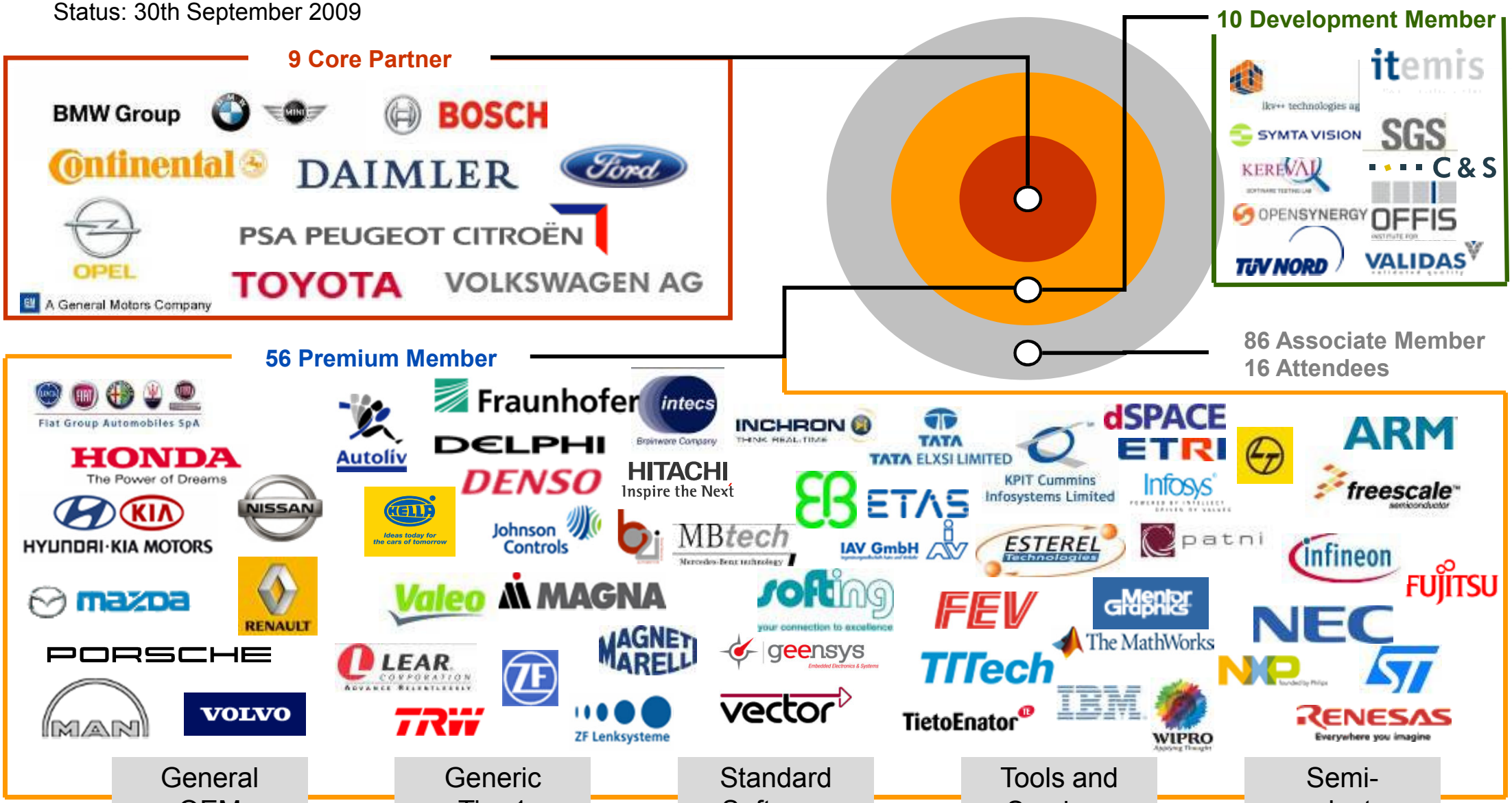

European Railway Agency
ETCS
Get it right !
SRS "Prose"
Human Factor
Human Factor
Human Factor
Formal System Requirement Spec.
Formal Language Functional Vehicle Specification
Safety Case Docs
openETCS Tools
Synthetic test cases & response pattern
openETCS Project
SW Code Generator
Parameters
openETCS
API
HW
Lab Test
STI
EVC
Vehicle Equipment
Manufacturer
ITEA 2
openETCS

Scope of openETCS



AUTOSAR – Core Partners and Members

Status: 30th September 2009

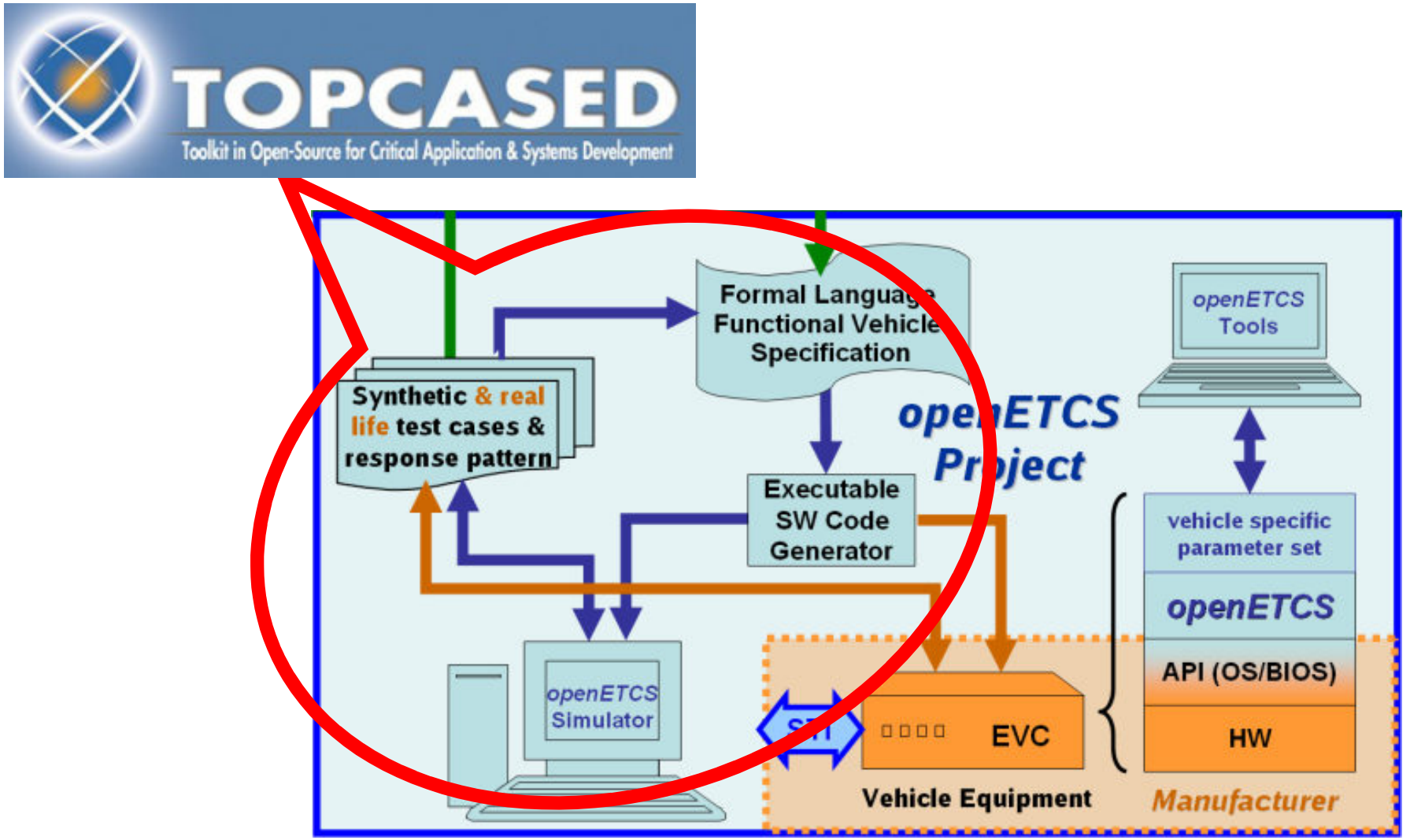


Up-to-date status see: http://www.autosar.org

Courtesy of

Overview on AUTOSAR Members

Scope of openETCS



TOPCASED project – initial members

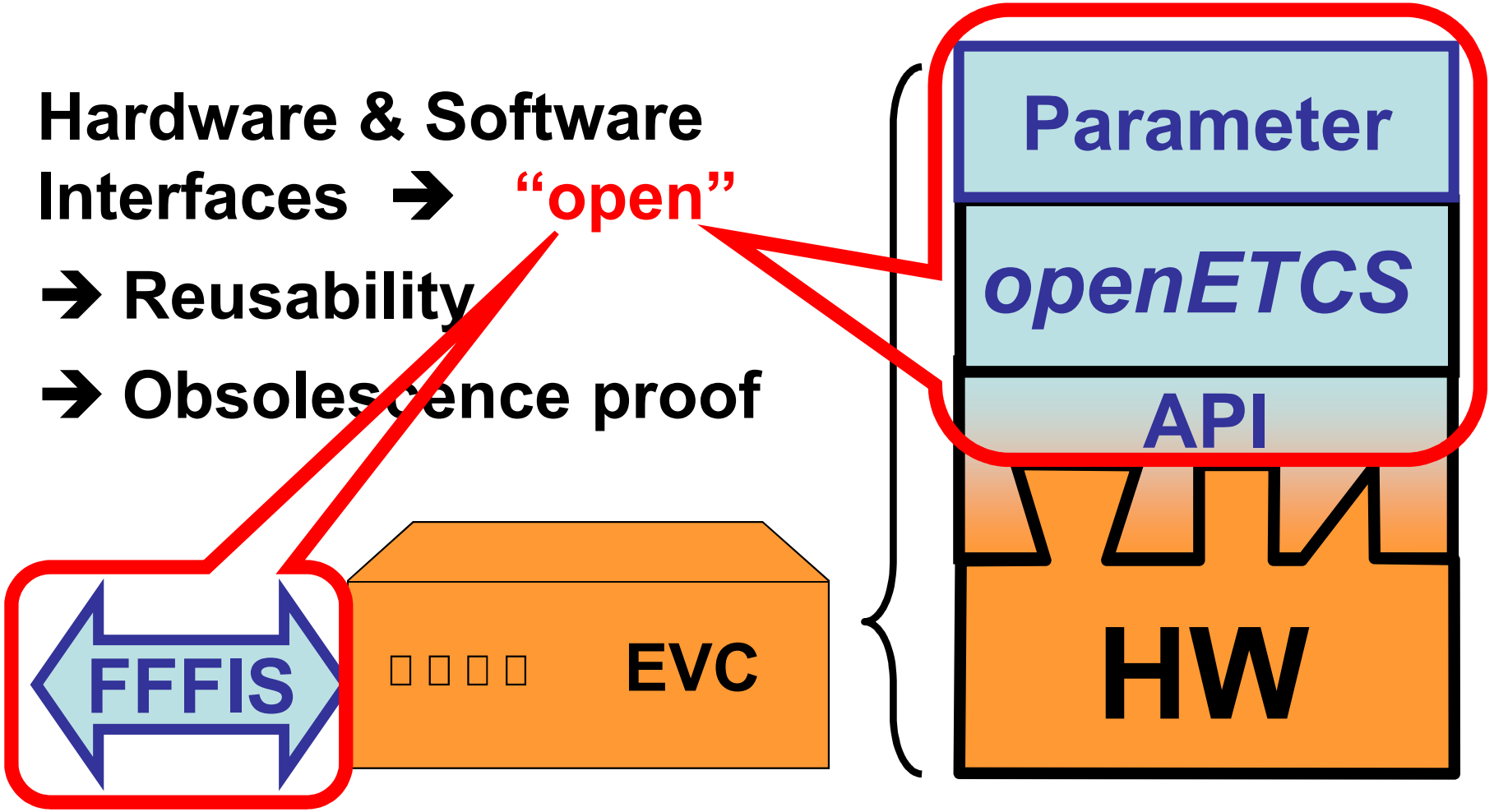
Reference: www.topcased.org

openETCS - Architecture

Hardware & Software Interfaces ➔ “open”

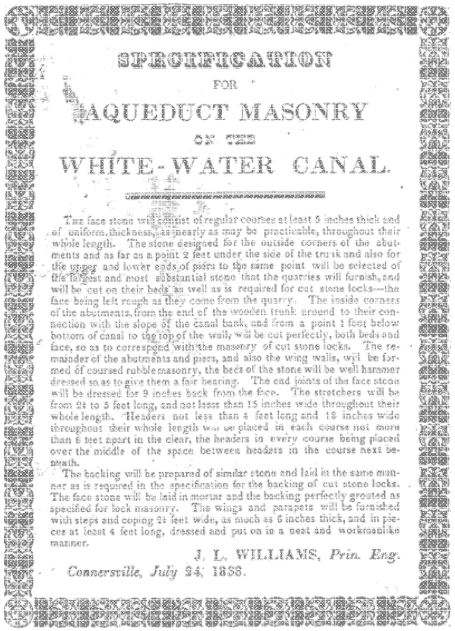
➔ Reusability

➔ Obsolescence proof



ETCS On-Board Unit

Objectives and major expected Outcomes



SPECIFICATION

FOR

AQUEDUCT MASONRY

ON THE

WHITE-WATER CANAL.

The face stone will consist of regular courses at least 5 inches thick and of uniform thickness, as nearly as may be practicable, throughout their whole length. The stone designed for the outside corners of the abutments and as far as a point 2 feet under the side of the trunk and also for the upper and lower ends of piers to the same point will be selected of the largest and most substantial stone that the quarries will furnish, and will be cut on their beds as well as is required for cut stone locks—the face being left rough as they come from the quarry. The inside corners of the abutments, from the end of the wooden trunk around to their connection with the slope of the canal bank, and from a point 1 foot below bottom of canal to the top of the wall, will be cut perfectly, both beds and face, so as to correspond with the masonry of cut stone locks. The remainder of the abutments and piers, and also the wing walls, will be formed of coursed rubble masonry, the beds of the stone will be well hammer dressed so as to give them a fair bearing. The end joints of the face stone will be dressed for 9 inches back from the face. The stretchers will be from 2½ to 3 feet long, and not less than 15 inches wide throughout their whole length. Headers not less than 4 feet long and 18 inches wide throughout their whole length will be placed in each course not more than 6 feet apart in the clear, the headers in every course being placed over the middle of the space between headers in the course next beneath.

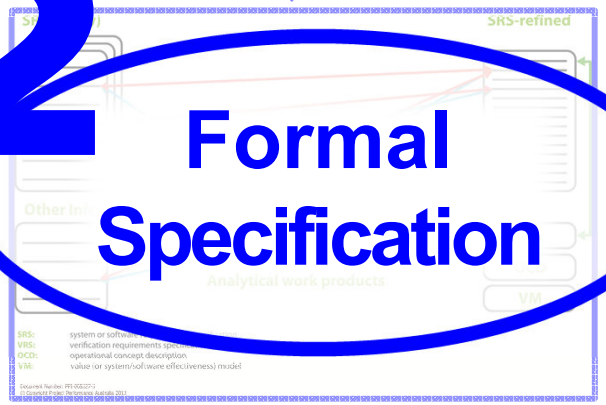
The backing will be prepared of similar stone and laid in the same manner as is required in the specification for the backing of cut stone locks. The face stone will be laid in mortar and the backing perfectly grouted as specified for lock masonry. The wings and parapets will be furnished with steps and coping 2½ feet wide, as much as 6 inches thick, and in pieces at least 4 feet long, dressed and put on in a neat and workmanlike manner.

J. L. WILLIAMS, *Prin. Eng.*

Connersville, July 24, 1838.

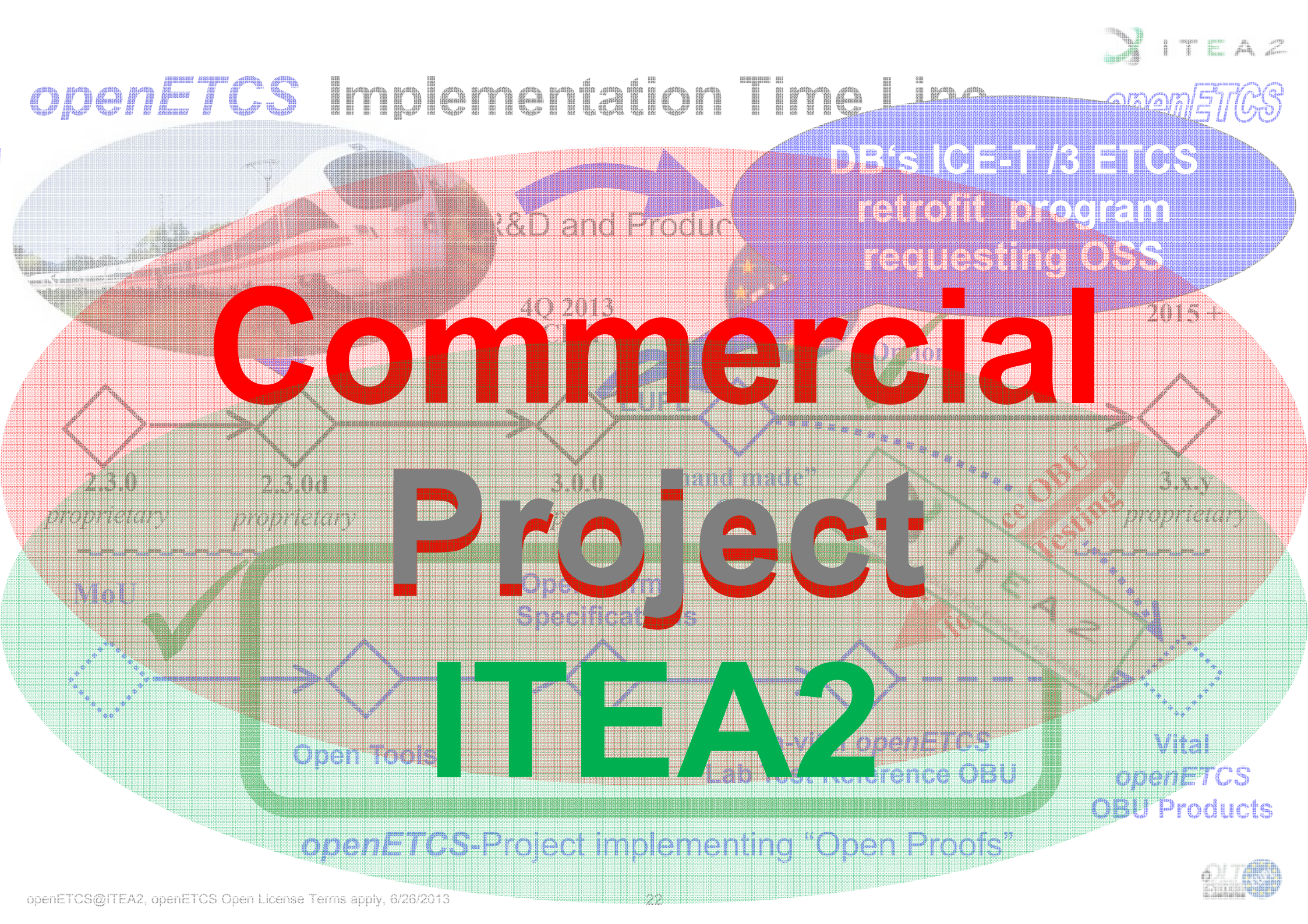
1 **Model based Development Framework Set of Software Tools**

2 **Formal Specification**



3 **Reference Unit**

openETCS Implementation Time Line



European Railway Agency

ETCS

SRS
"Prosa"

ITEA 2

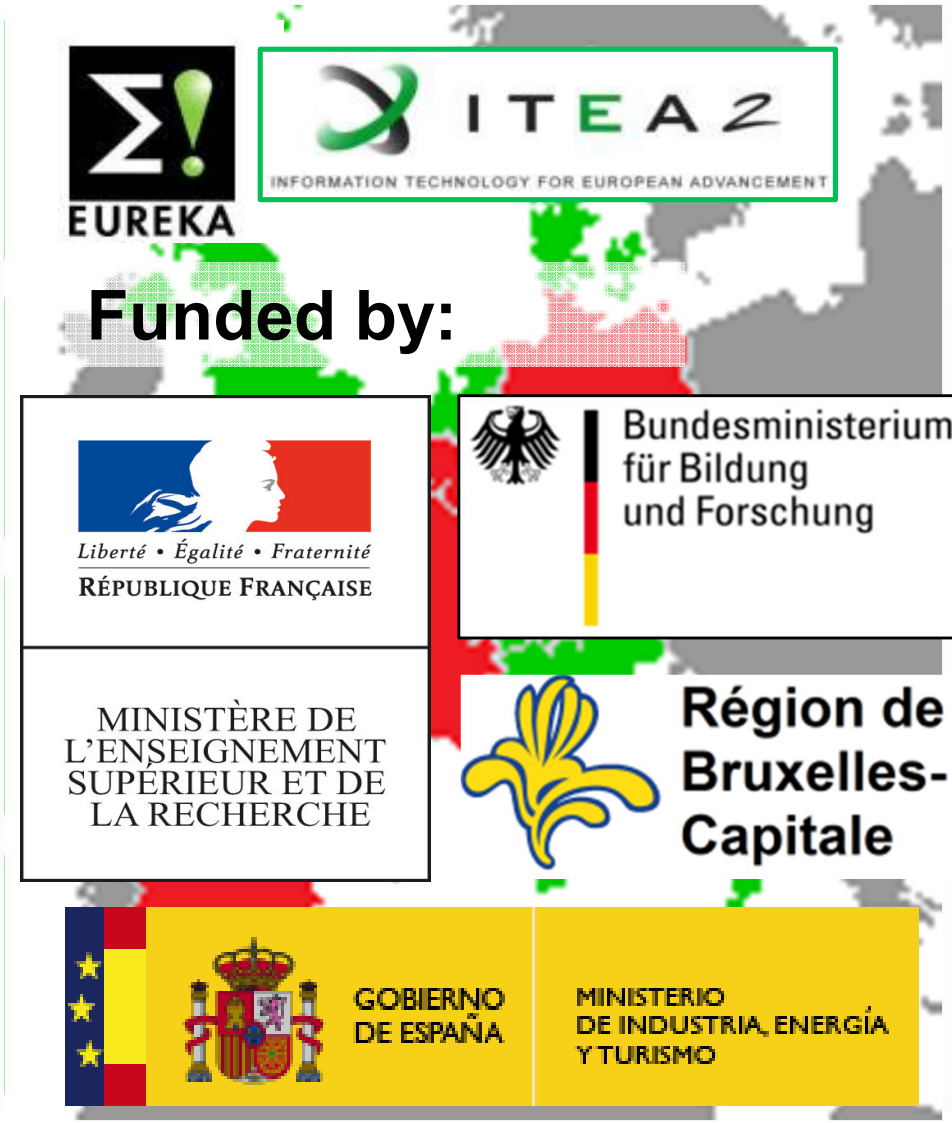
openETCS

openETCS

Linus' Law: "Many eyes make all bugs shallow"

Equipment 1 | Equipment 2 | Equipment 3 | Equipment 4

openETCS @ ITEA2 Project



openETCS

Programcall	ITEA 2 Call 6 11025
Title	Open Proofs Methodology for the European Train Control Onboard System
Period	Jul 2012 - Jun 2015
Status	Labelled
Domain	Services, Systems & Software Creation
Technology	Engineering and development
Effort	**156** man-year
Costs	**18,959,000** EURO

http://www.openETCS.org

openETCS

openETCS

projects principles members about

European Train Control System (ETCS)

Open Proof. Open Source.

The purpose of the openETCS project is to develop an integrated modeling, development, validation and testing framework for leveraging the cost-efficient and reliable implementation of ETCS. The framework will provide a holistic tool chain across the whole development process of ETCS software. The tool chain will support the formal specification and verification of the ETCS system requirements, the automatic and ETCS compliant code generation and validation, and the model-based test case generation and execution.

Upcoming Events

ERTMS Workshop
Date: December 17th and 18th
Location: Brussels
ERTMSFormalSpecs presentation + installation + tutorial
ERTMSFormalSpecs ...

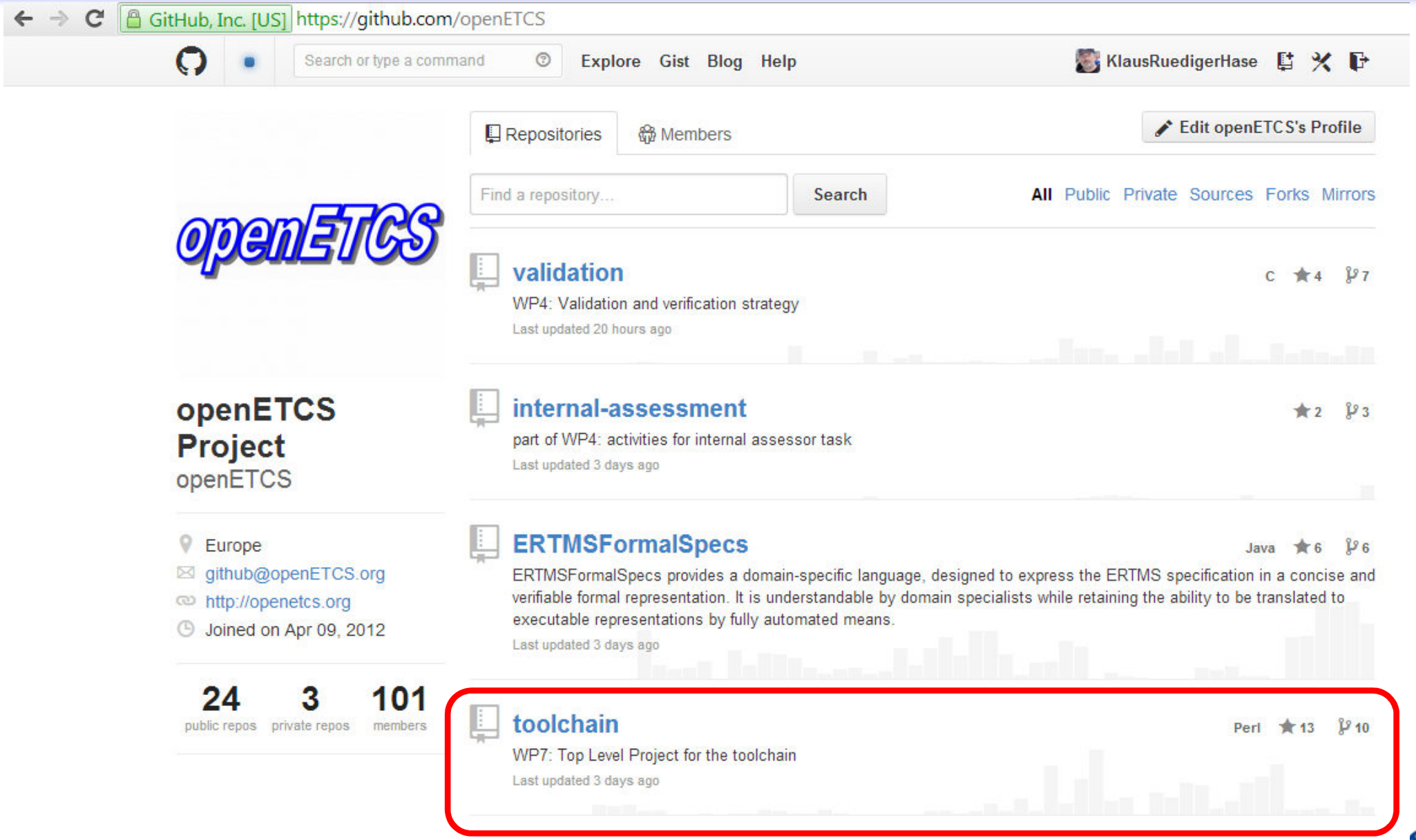
PMB Team Konferenz

Germany Cluster Meeting

FormalMethod Conference
Date: April 15th and 16th

FormalMethod Training
Date: April 17th, 22nd-23rd
Location: Munich
DB Freimann

https://github.com/openETCS



D7.1 Results

OETCS/WP7/D7.1 – 01/04

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

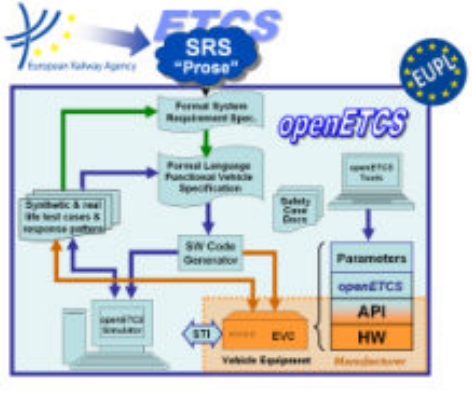
Work Package 7, Task 1: "Primary Toolchain"

Report on the Final Choice of the Primary Toolchain

Decision on the final choice for the means of description (O7.1.4), tools (O7.1.8) and tool platform (O7.1.11)

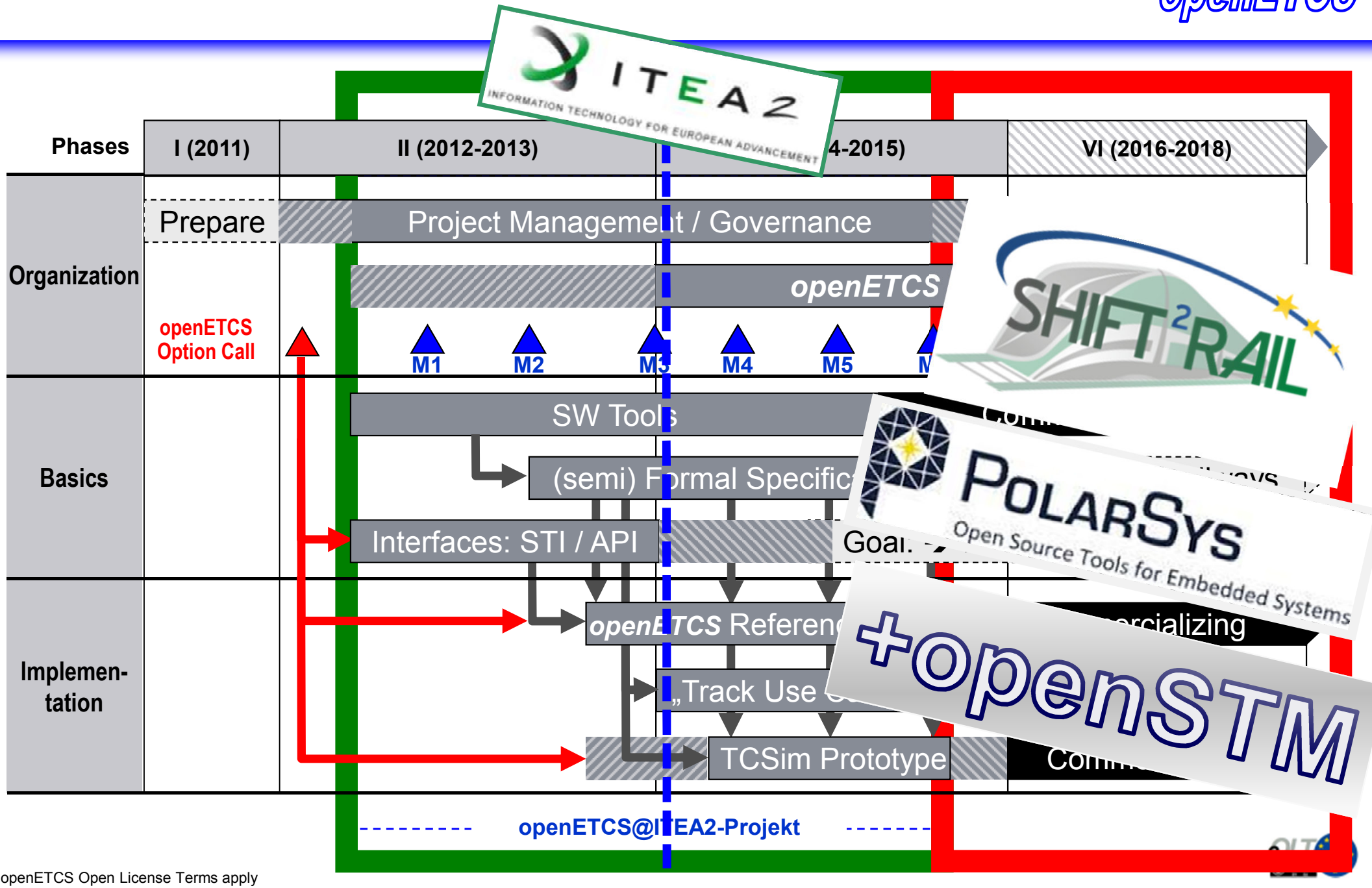
Michael Jastram, Mariello Petit-Doche and all participants of the decision process

September 2013



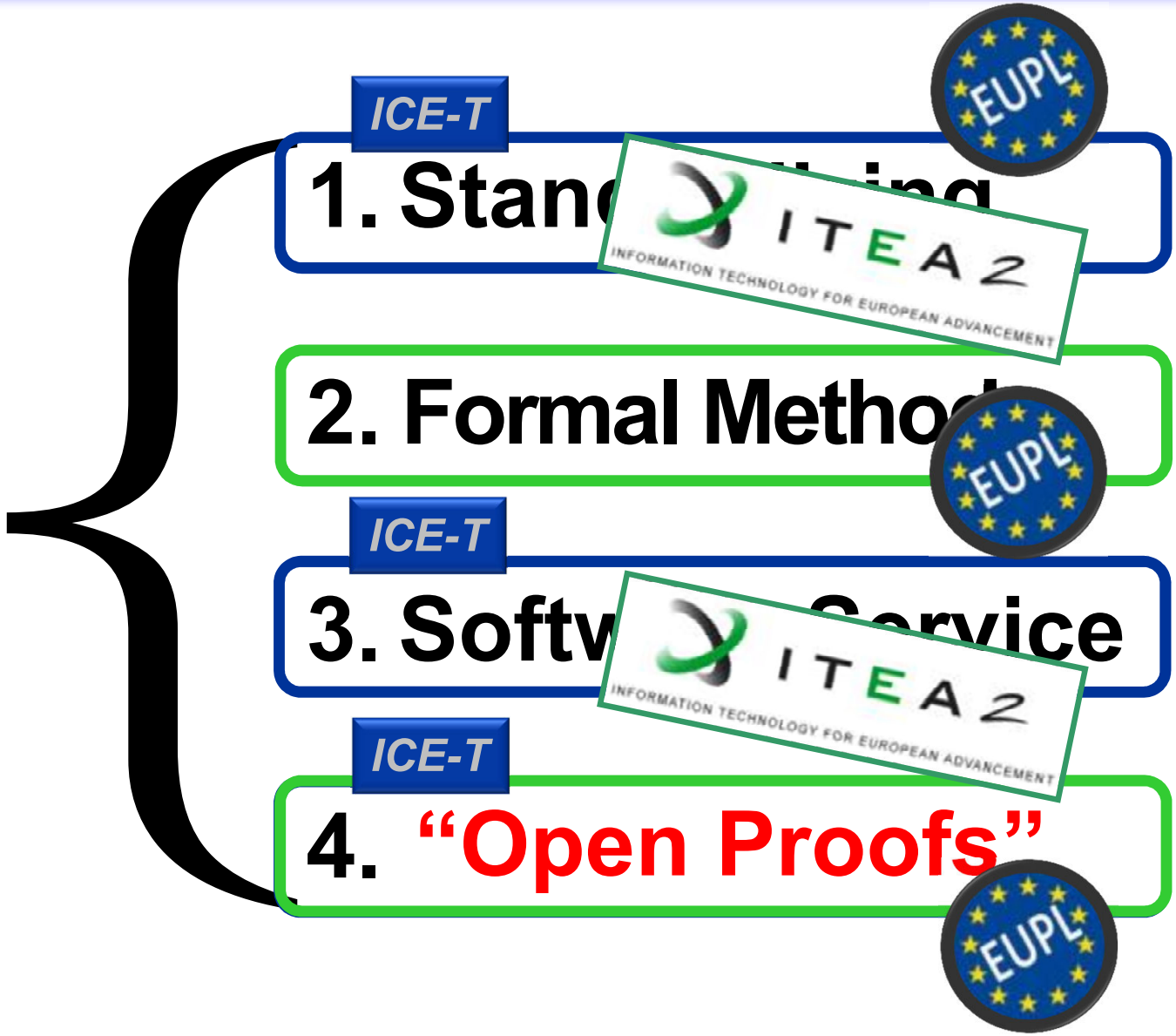
Funded by:

openETCS Project Schedule Overview



What is the status so far?

openETCS



One last word …

Arthur Schopenhauer:
[German Philosopher, 1788-1860]:

**“New ideas are first ridiculed,
then fought bitterly,
and when they got their way,
everyone was always for it.“**

That was it …

Thank you very much for your attention.

➔ www.openETCS.org