ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

openETCS@ITEA2
Project Overview

supported by:

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

INVESTISSEMENTS D'AVENIR

Région de Bruxelles-Capitale

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

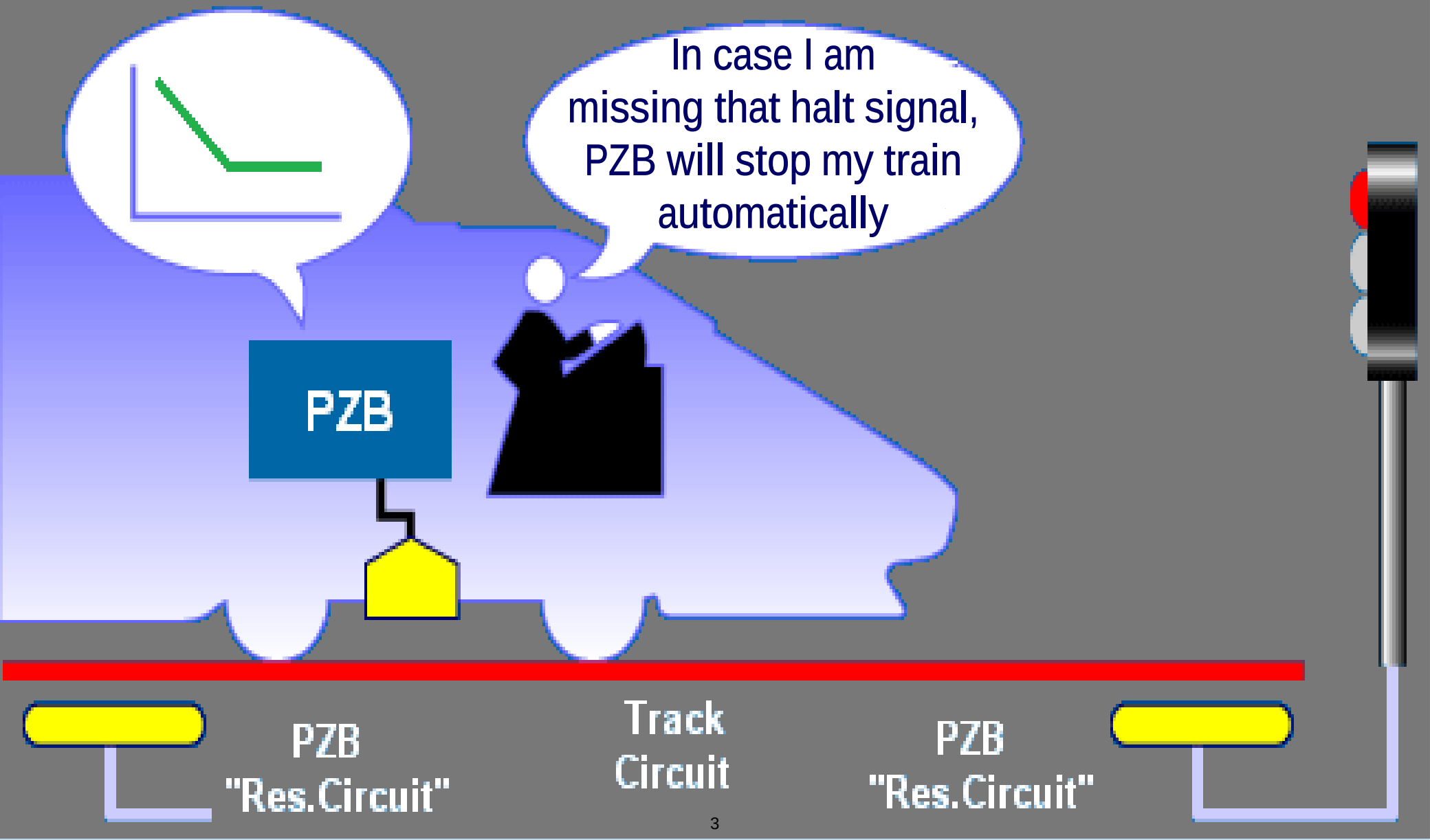
openETCS@ITEA2 Project

Klaus-Rüdiger Hase

Paris, 03.07.2013

Signals need ATP: Drivers can make mistakes

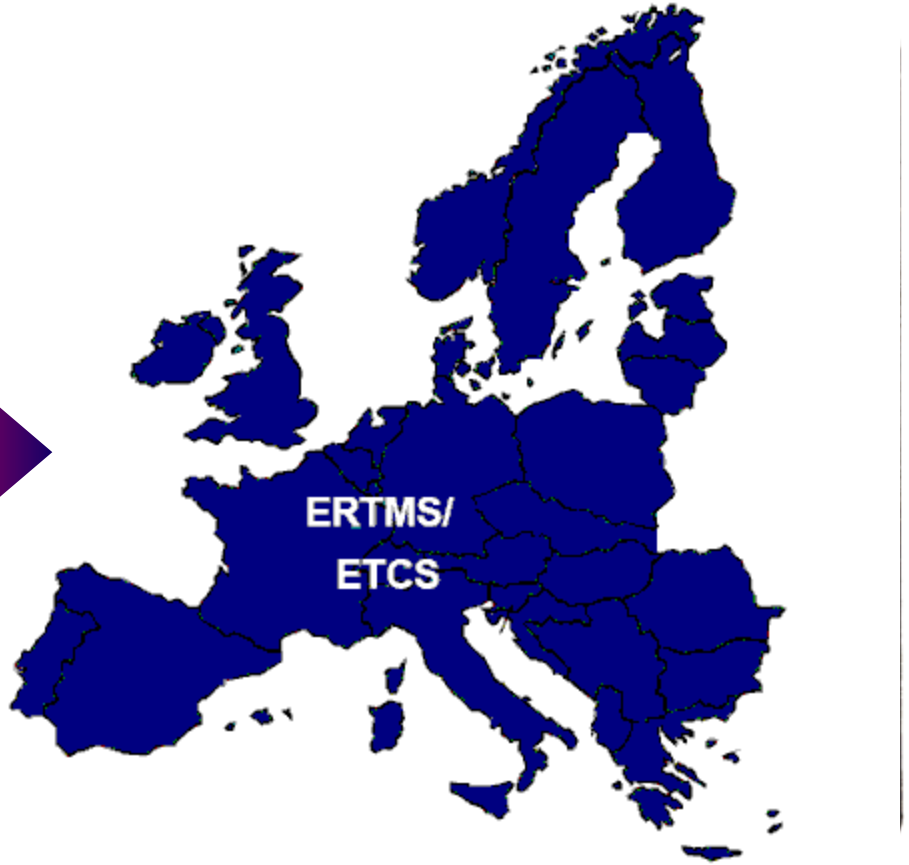
Automatic Train Protection (e.g. PZB since 1934)



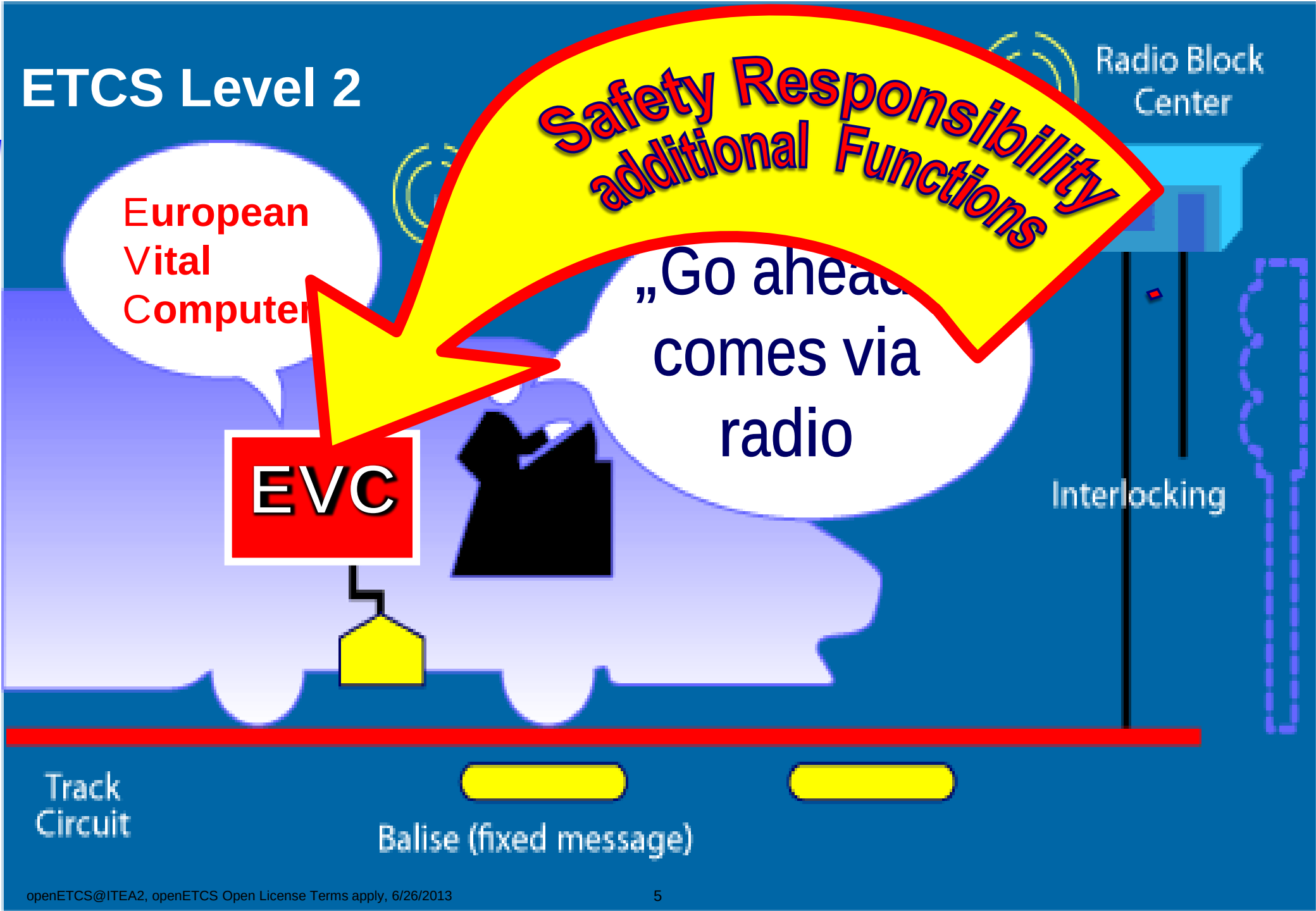
European Signaling Diversity due to History

Today: Diversity

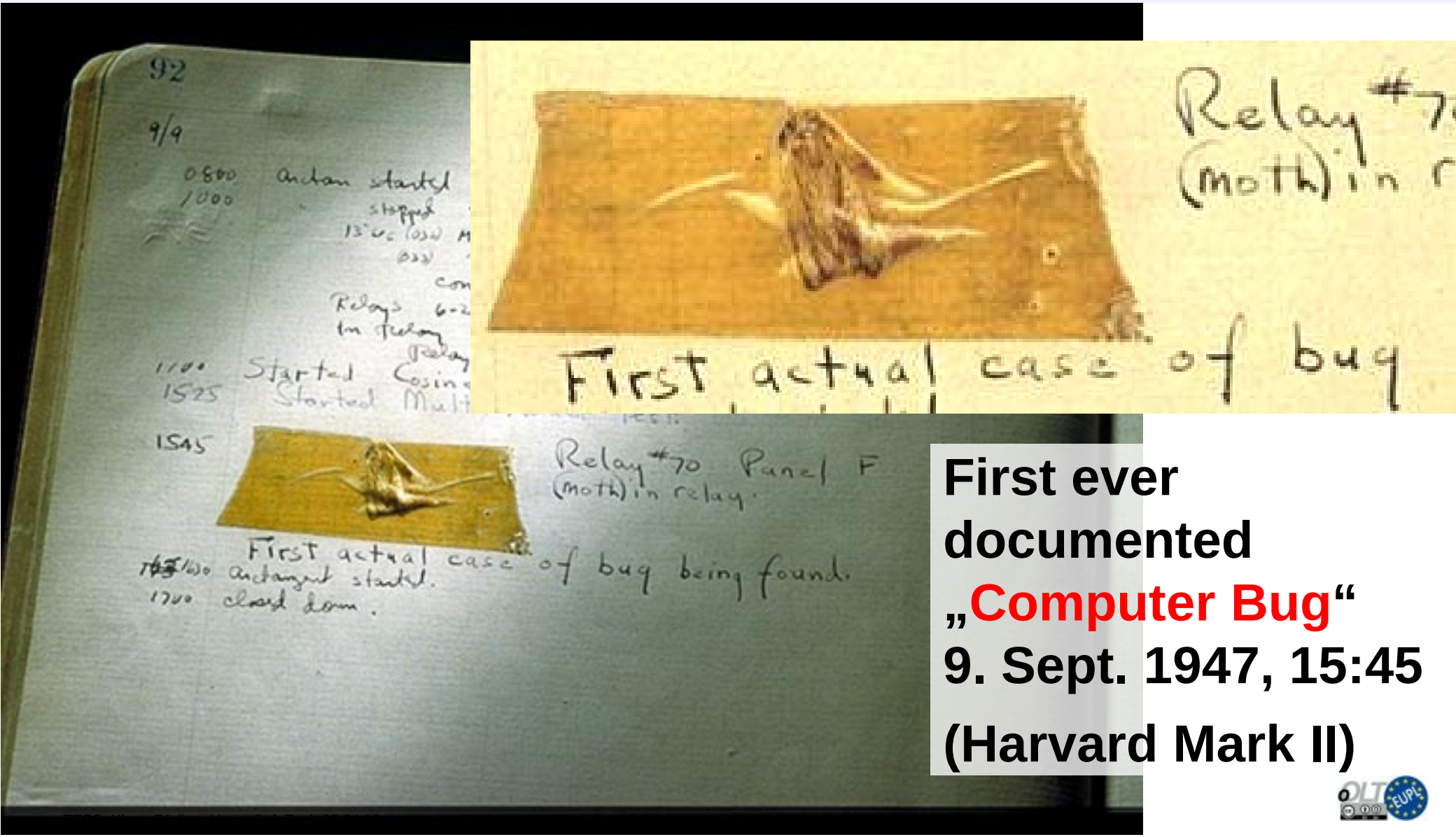
Future: Unity



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)

Computer for “SAFETY” ? … have „Bugs“ !



First ever documented „Computer Bug“
9. Sept. 1947, 15:45
(Harvard Mark II)

Computer Bugs

Foto 2

Foto 3

Entgleiste Lok Re 465 007-3

October 16, 2007: Derailment at the Lötschberg Baseline near Frutigen (CH) due to a software bug in the ETCS Radio Block Center (RBC) *)

***) published at: http://www.uus.admin.ch//pdf/07101601_SB.pdf**

How many „Bugs“ to expect?

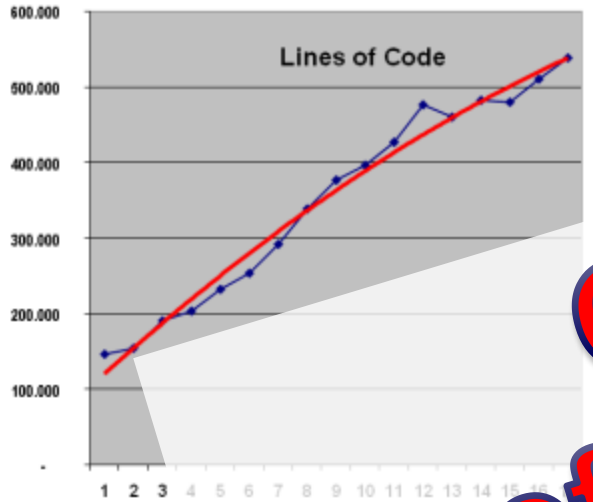
- **Typical quality SW: 1 … 10 bugs per 1.000 lines of code (TLOC).**
- **Very mature, long-term, well proven SW: 0,5 bugs per TLOC**
- **Highest software quality ever reported :**
  - ***Less than 1 bug per 10 TLOC***
  - **At cost of more than 1.000 US$ per LOC *(1977)***
  - ***US Space Shuttle with 3m LOC* costing 3b US$ (out of 12b$ total R&D)**

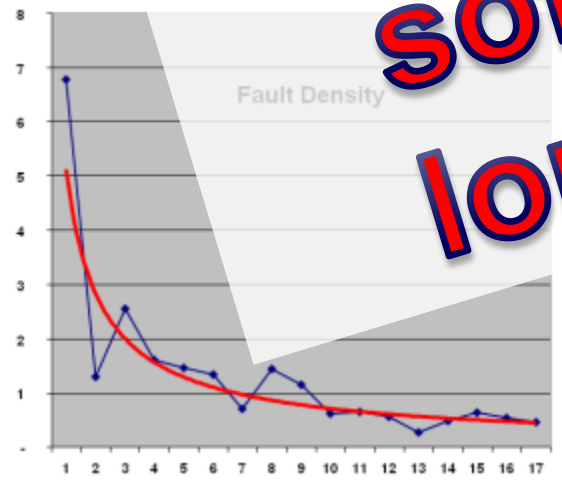
➔ **Cost level not typical for the railway sector (< 100€/LOC)**

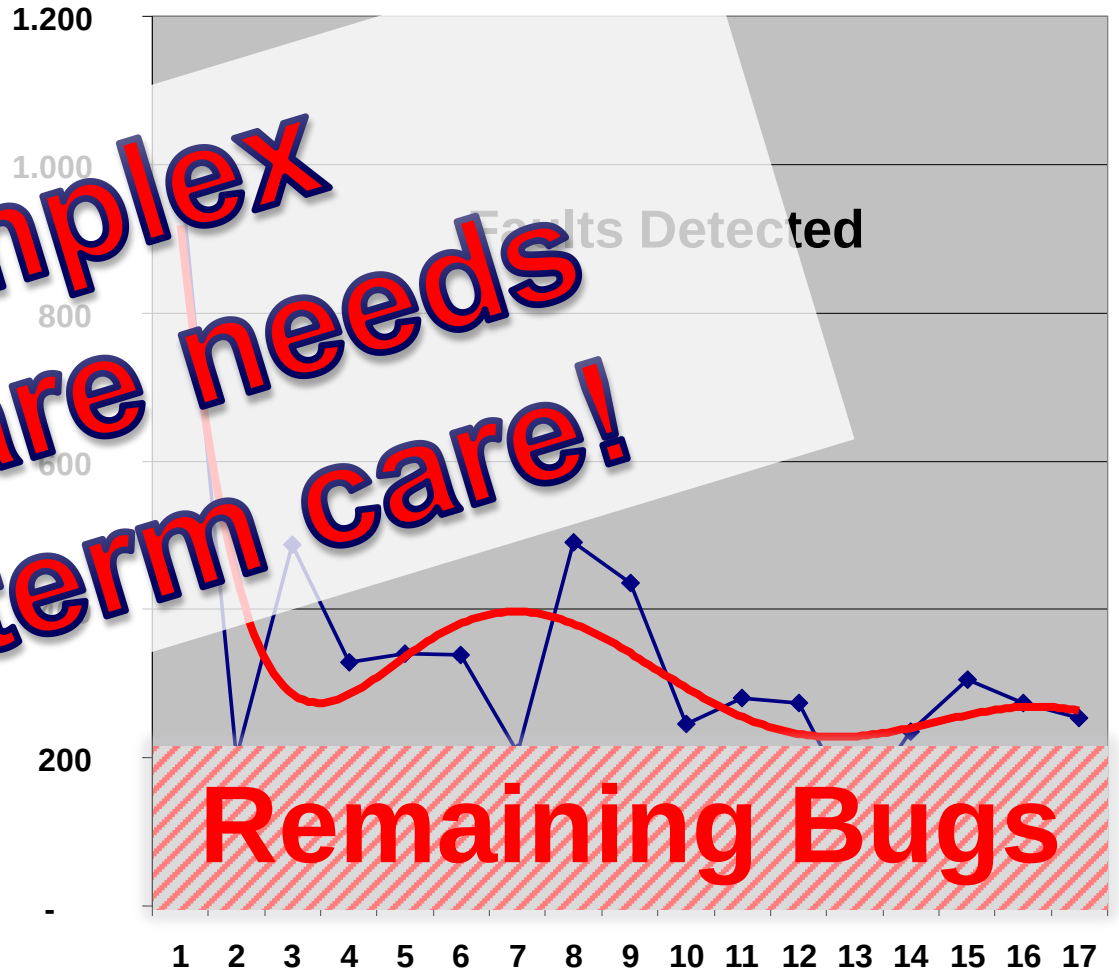
- **Typical ETCS Kernel software size from 100 to 500 TLOC**

  ↳ **That means: 100 … 1.000 undisclosed BUGS per EVC**

Characteristics of Complex Software

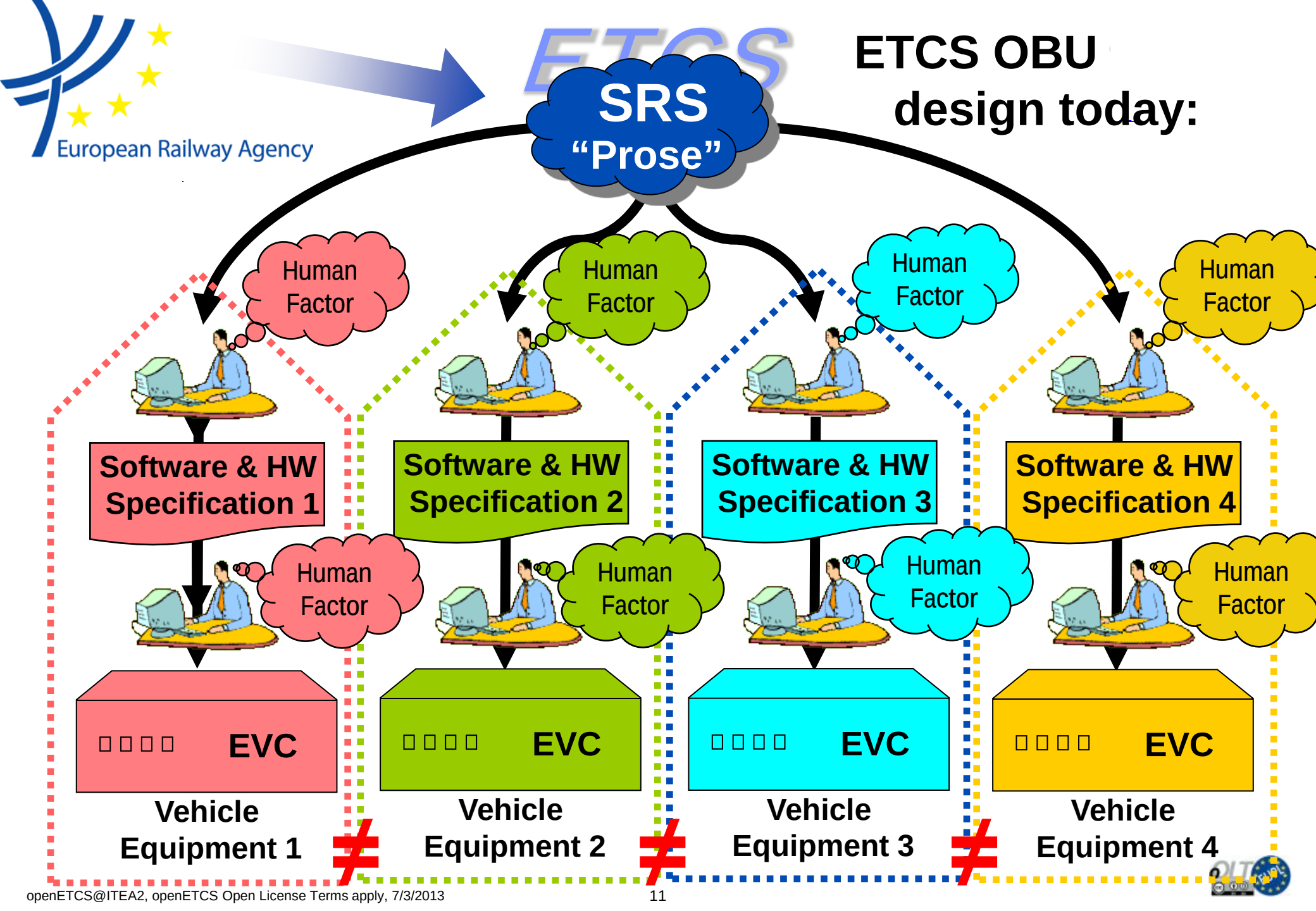






Complex software needs long-term care!

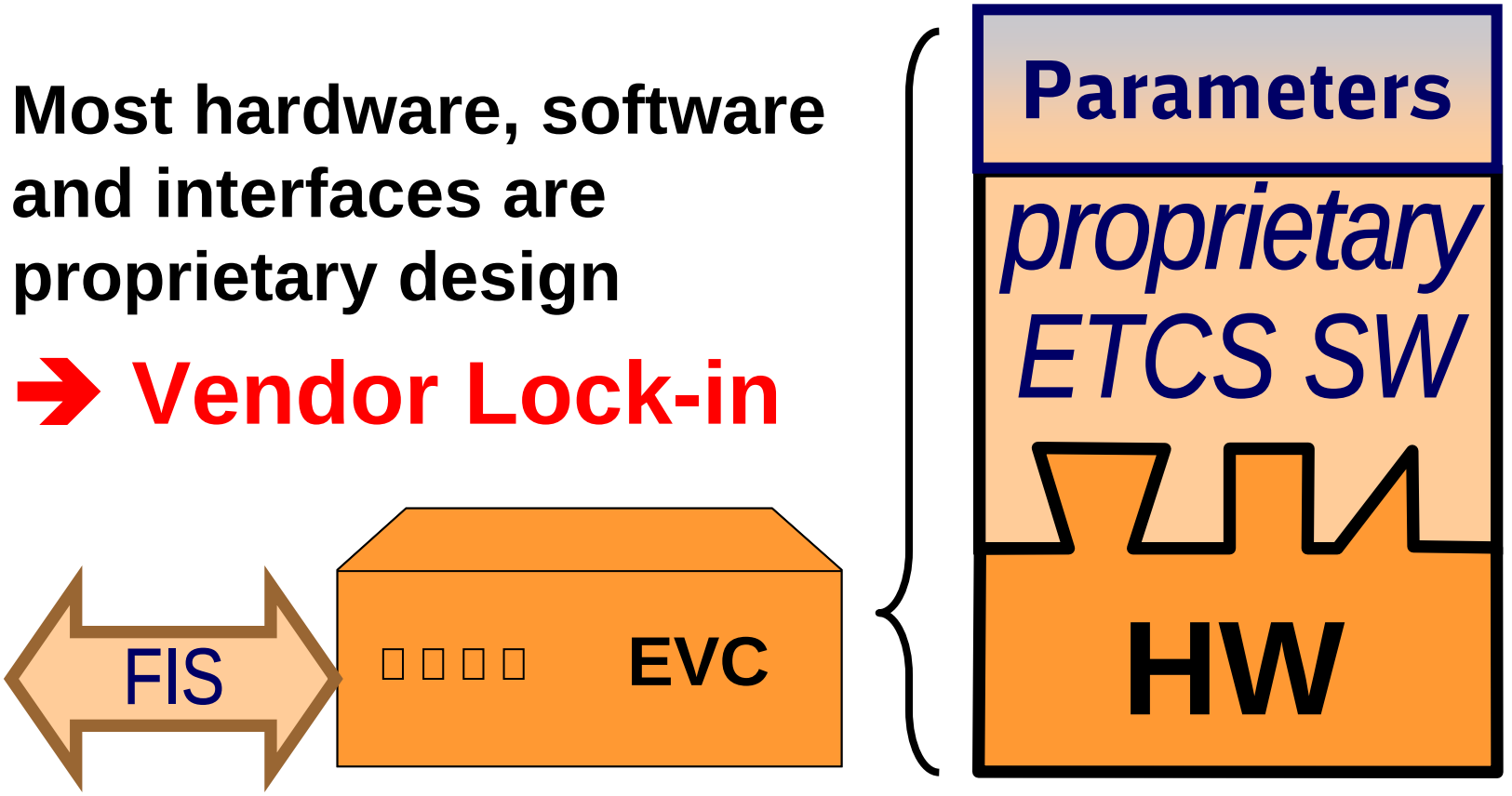
ETCS OBU design today:



Low Level of Standardization Today

Most hardware, software and interfaces are proprietary design

➔ Vendor Lock-in



Vehicle Equipment

What means „Vendor Lock-in“?

How to improve?

Lower Complexity	➔	**1. Standardization**
Reduce Ambiguities	➔	**2. Make it “Formal”**
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 required tools: OSS
- Anyone can examine/critique, improve upon, collaborate with others for improvements
  - Not just software, but what's proved & tools
  - Example for training, or as useful component
- Extends OSS idea for high assurance
  - 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)

EUROPEAN PARLIAMENT

1999 2004

REPORT

11 July 2001

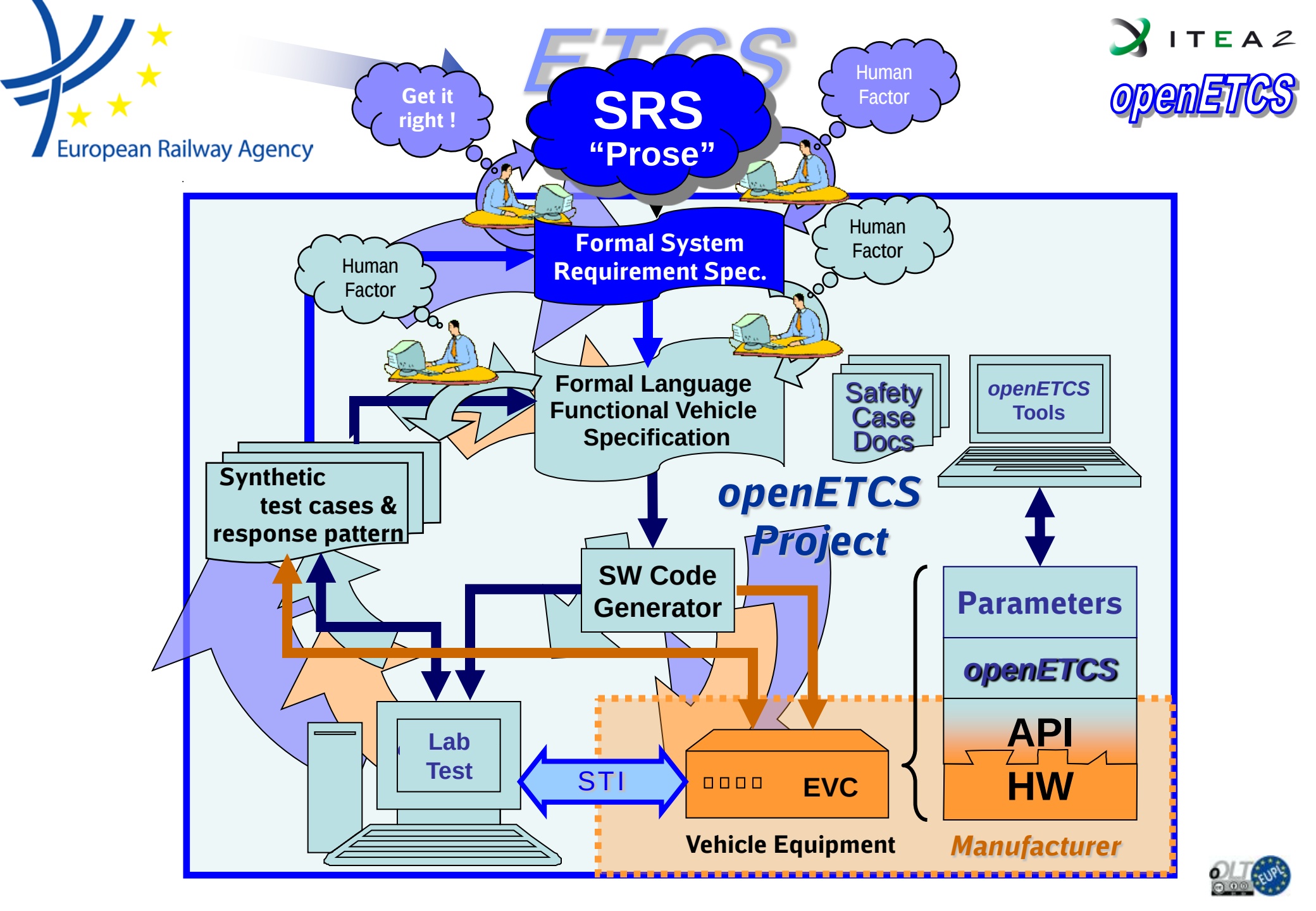
FINAL
A5-0264/2001
PAR1

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))

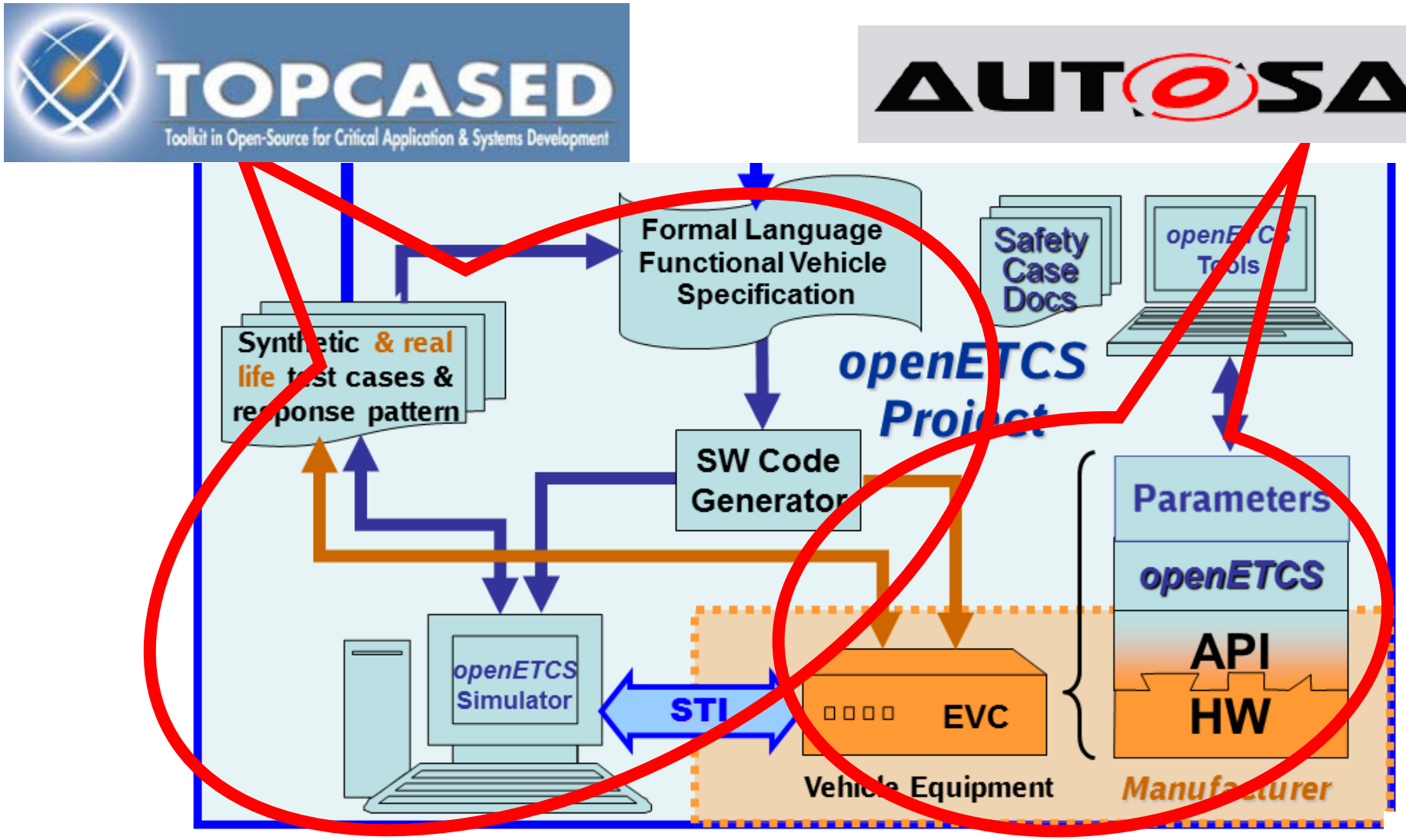
Measures to encourage self-protection by citizens and firms

30. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;

31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category;

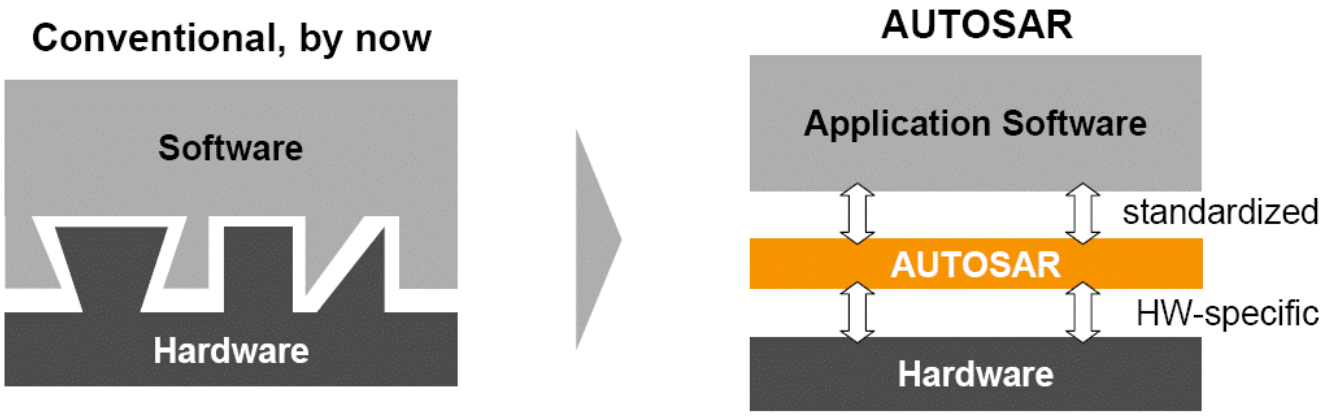

European Railway Agency
ITEA 2
openETCS
ETCS
Get it right !
SRS "Prose"
Human Factor
Human Factor
Human Factor
Formal System Requirement Spec.
Formal Language Functional Vehicle Specification
Safety Case Docs
openETCS Tools
Synthetic test cases & response pattern
openETCS Project
SW Code Generator
Parameters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

Scope of openETCS



API in AUTOSAR

Automotive Software Development will change.



- **Hardware- and software** will be **widely independent** of each other.
- **Development processes** will be **simplified**.
  This **reduces development time** and **costs**.
- **Reuse** of **software increases** at OEM as well as at suppliers.
  This **enhances** also **quality** and **efficiency**.

Automotive Software will become a product.

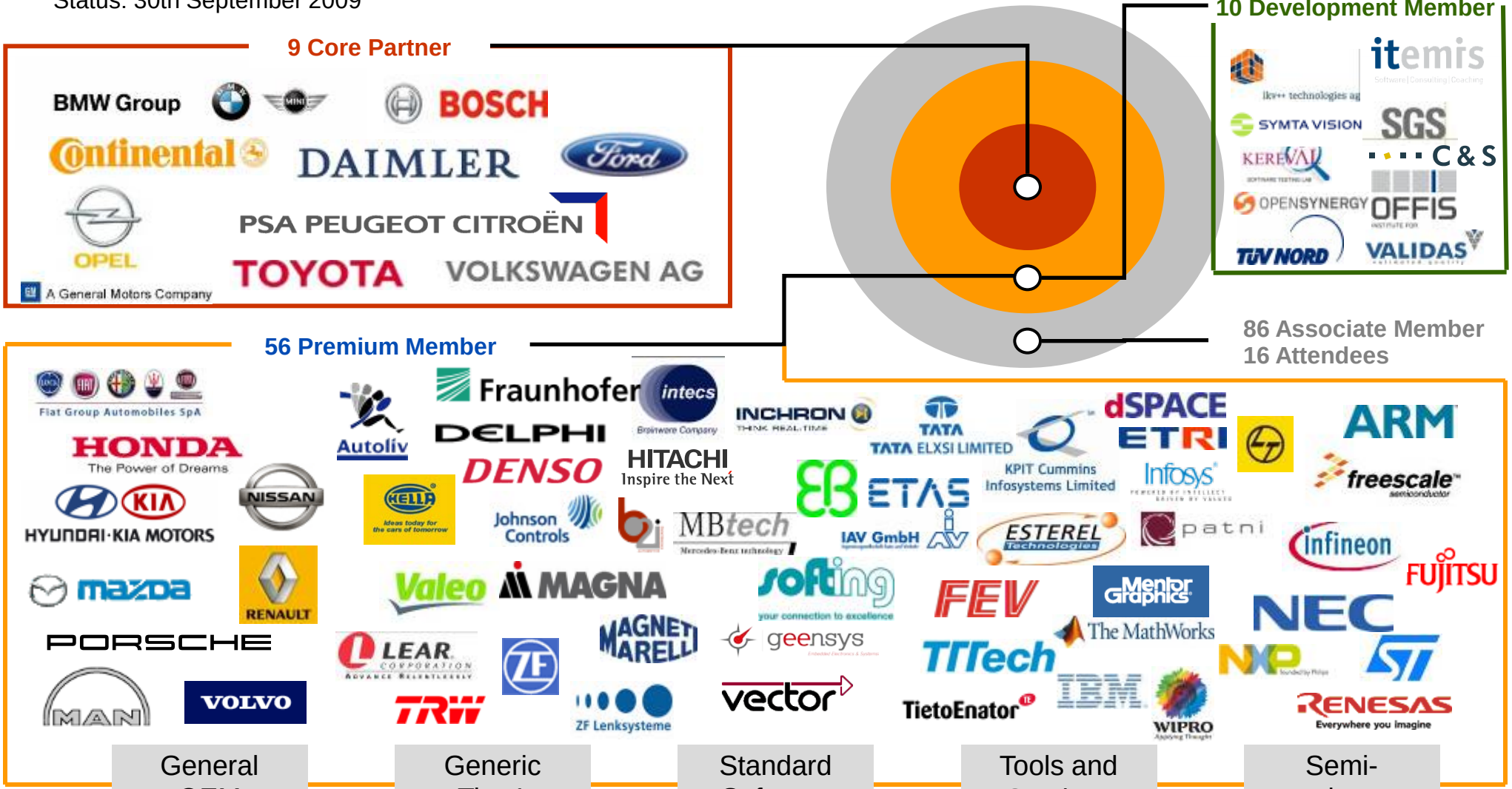
Referenz: www.autosar.org

AUTOSAR Roll-Out
Final Step of Migration

Reference: www.autosar.org

AUTOSAR – Core Partners and Members

Status: 30th September 2009

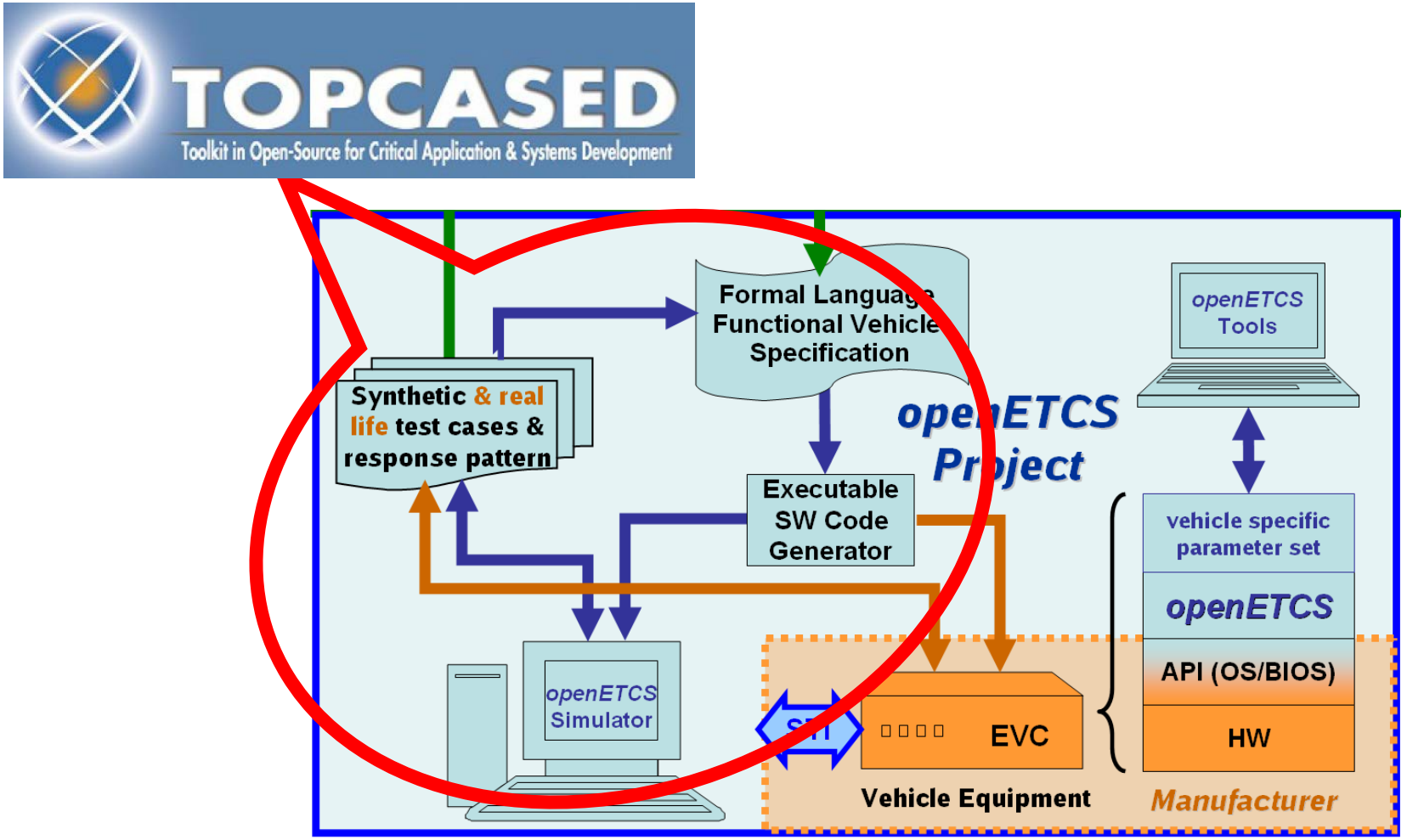


Up-to-date status see: http://www.autosar.org

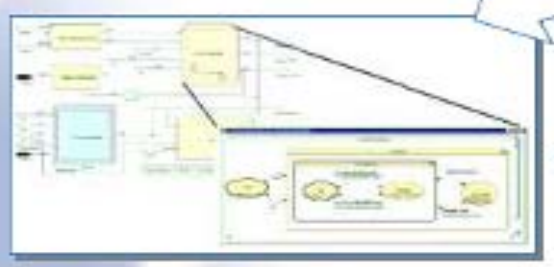
Courtesy of

Overview on AUTOSAR Members

Scope of openETCS



TOPCASED overview
Model Based System Engineering for critical systems



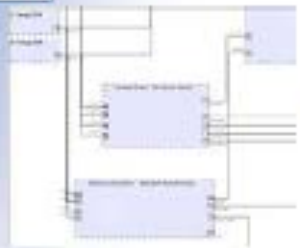
TOPCASED
Model editors

TOPCASED
Simulator Engines

TOPCASED
Model to Model
Transformations

TOPCASED
Model to Text
Transformations

Source code,
Test code,
Documentation,
...



TOPCASED
Formal Checking

Configuration, Change and Requirements management
tools communication

Reference: www.topcased.org

TOPCASED project – initial members

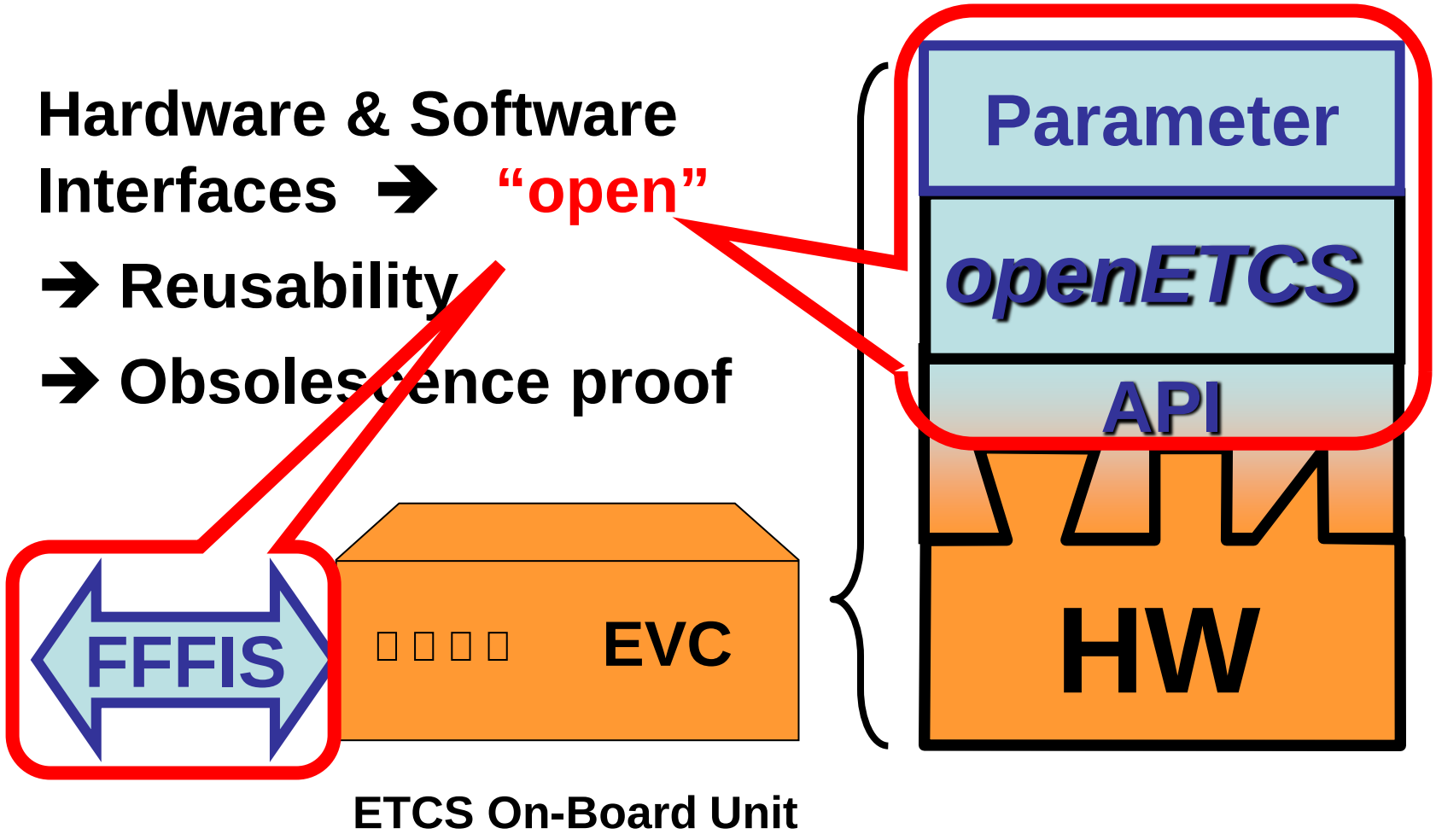
Reference: www.topcased.org

openETCS - Architecture

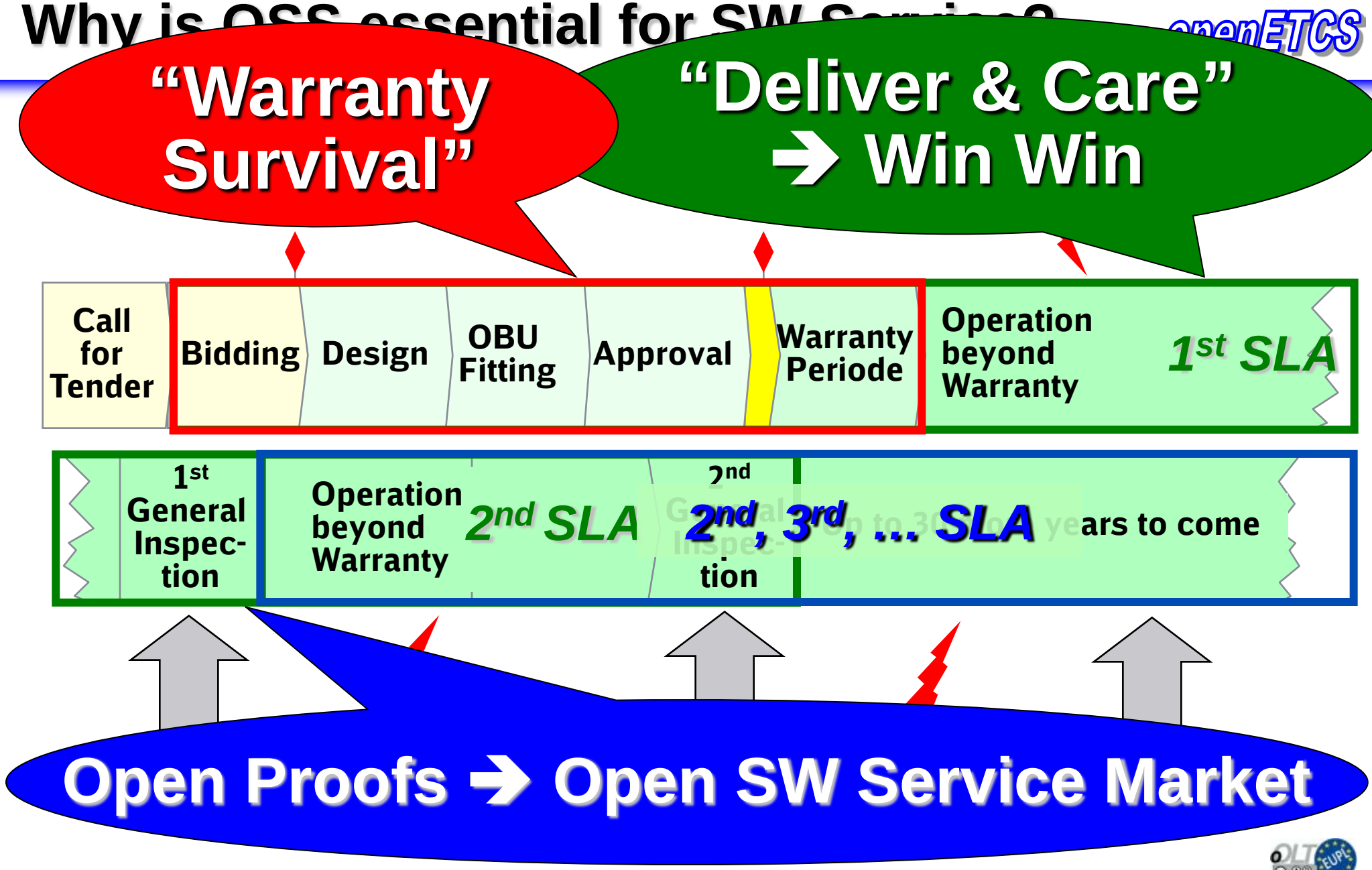
Hardware & Software Interfaces ➔ “open”

➔ Reusability

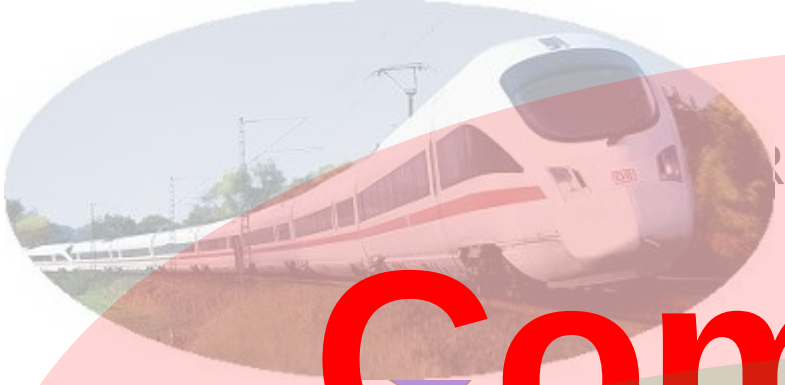
➔ Obsolescence proof



Why is OSS essential for SW Service?



openETCS Implementation Time Line



DB's ICE-T /3 ETCS retrofit program requesting OSS

R&D and Produc

4Q 2013

2015 +

EUPL

2.3.0 proprietary

2.3.0d proprietary

3.0.0

"hand made"

3.x.y proprietary

MoU

Open Tools

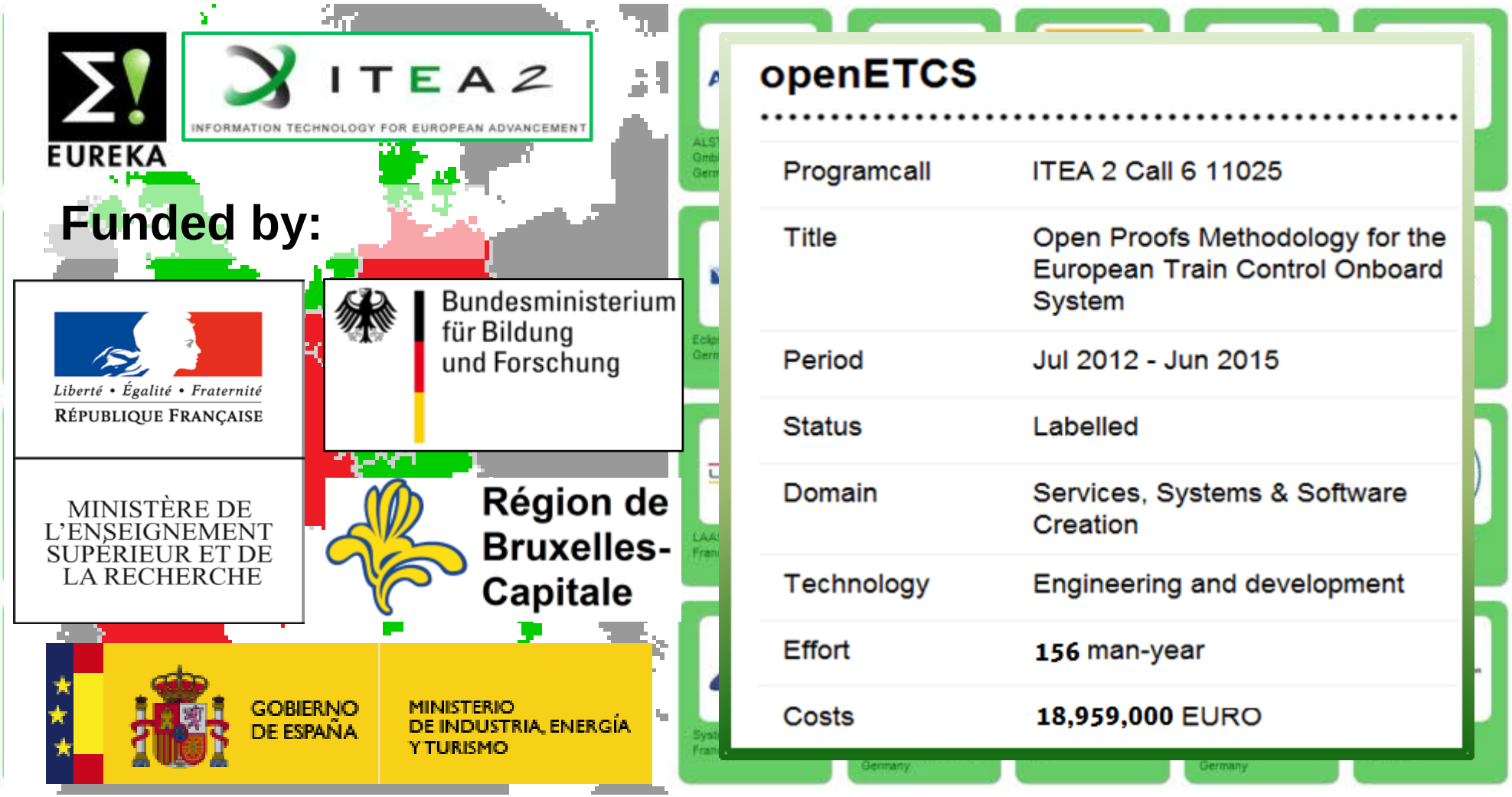
Lab Test Reference OBU

Vital openETCS OBU Products

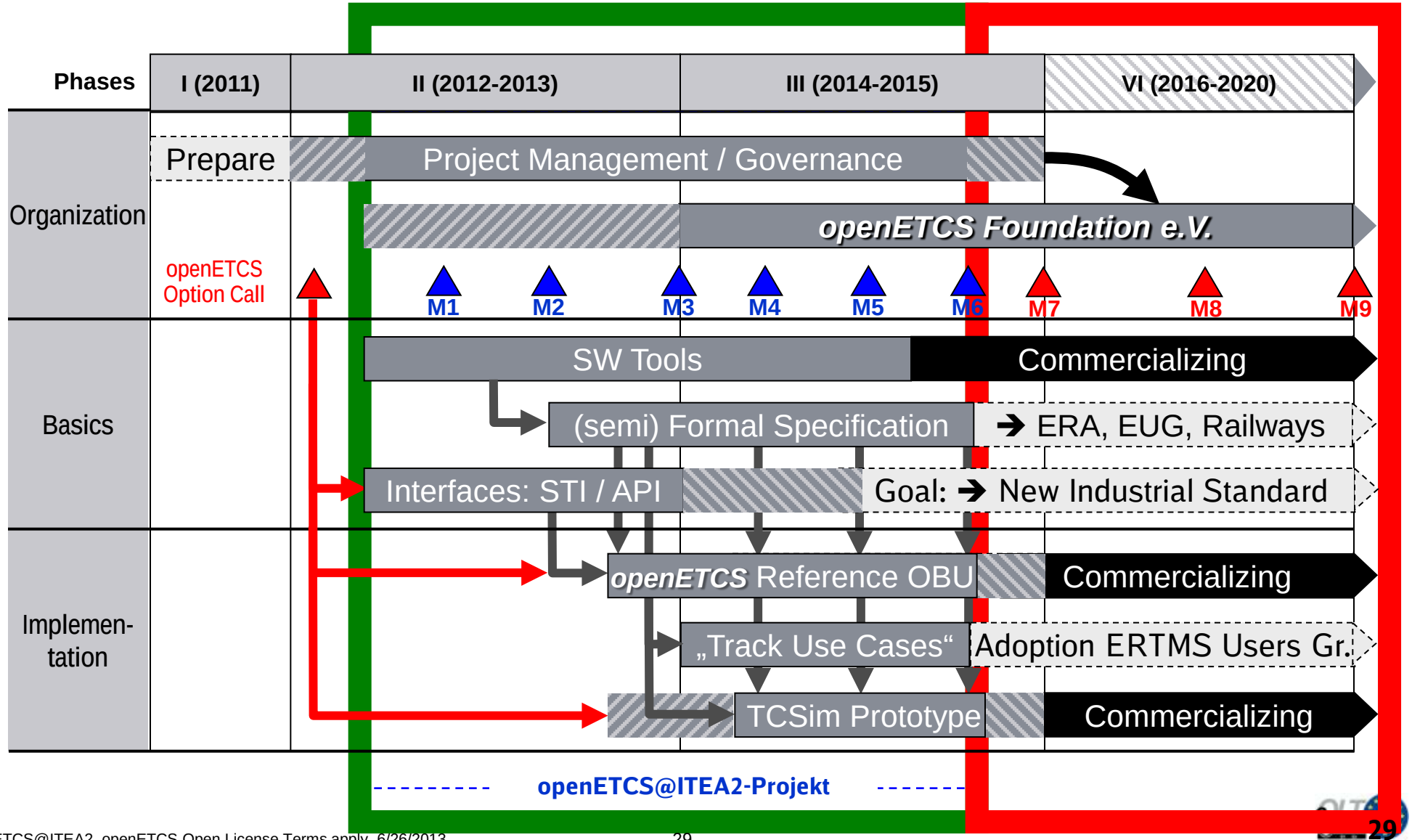
openETCS-Project implementing "Open Proofs"

Commercial Project ITEA2

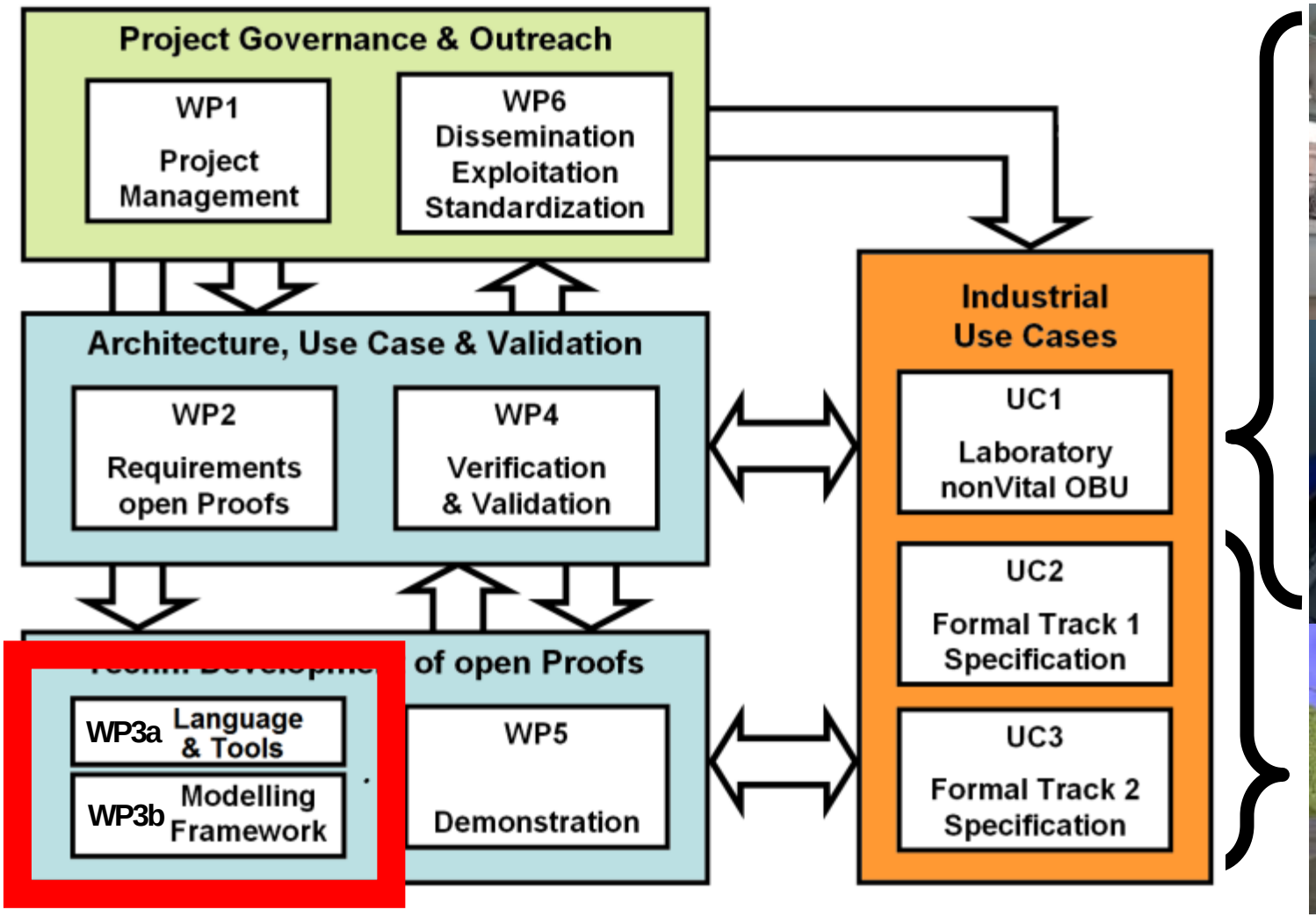
openETCS @ ITEA2 Project



openETCS Project Schedule Overview



Project Structure and Proof of Concept utilizing *TCSim* at DB



Split of WP3 ➔ Work Packages WP3a + WP3b

WP3 Objectives		
Date	**Deliverable**	**Description**
T0+6	**D3.1:** Tool chain architecture definition, openETCS language definition and System specification model	Set of proposals for the tool chain architecture (including requirement elicitation technique, modelling languages, modelling tools, transformation tools and V&V tools). Model of the overall signalling system including ETCS
T0+9	**D3.2:** openETCS tool chain development plan	Selection of tool chain architecture. Development tasks description Development tasks planning.
T0+15	**D3.3:** openETCS open-source ecosystem	Open source ecosystem for the openETCS tool chain.
T0+36	**D3.4:** openETCS tool chain and openETCS source code	openETCS tool chain including its documentation and on-board unit software code.
T0+18	**D3.5:** openETCS functional model	Models of the ETCS system specifications (SRS).
T0+30	**D3.6:** openETCS architecture description openETCS platform API specification	The architecture model(s) of ETCS system. Specification of the API of the platform on which openETCS code runs.

WP3a ➔ WP7 (new)
New WP-Leader :
Formal Mind GmbH
(Partly self funded and subcontracted by Deutsche Bahn AG)

WP3b ➔ WP3 (new)
WP-Leader:
Alstom (Belgium)

http://www.openETCS.org

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

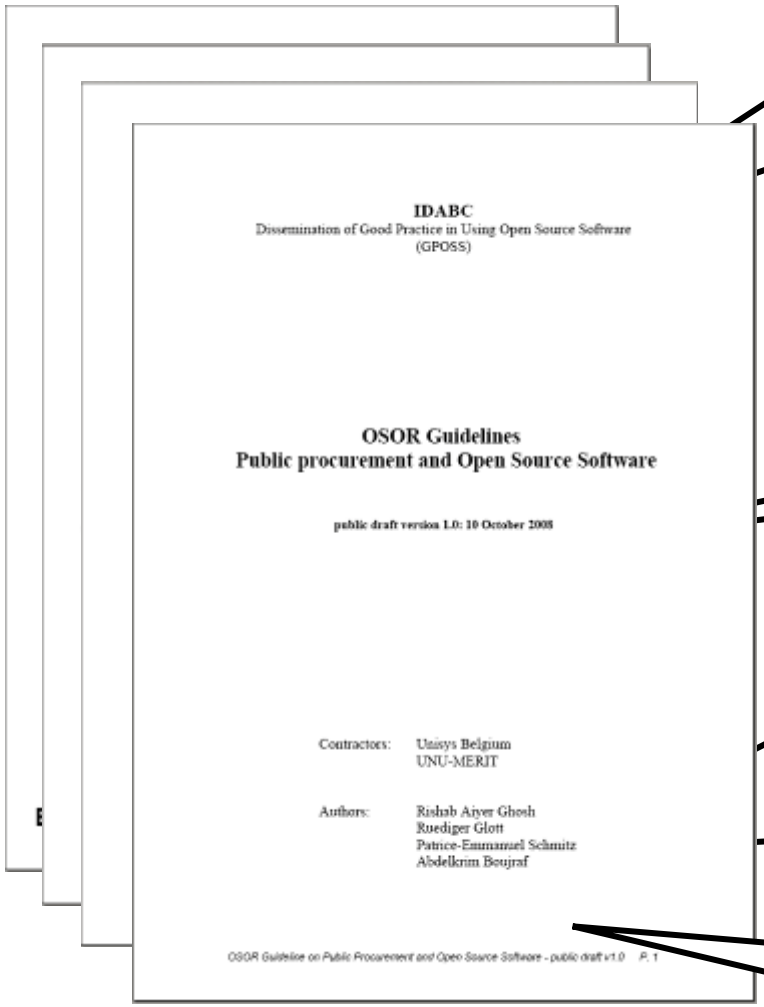
FormalMethod Conference
Date: April 15th and 16th

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

What is new? What is the innovation?

- ✓ First industrial implementation of „open Proofs“
- ✓ First technical system using EUPL
- ✓ First open project in the railway safety domain
- ✓ First attempt to combine CENELEC EN50128 with:
  - ✓ Open source software production scheme
  - ✓ Agile methods
- ✓ First training simulator with formal approach
- ✓ First open source reference device in railway sector

EU supports FLOSS


IDABC
Dissemination of Good Practice in Using Open Source Software
(GPOSS)

OSOR Guidelines
Public procurement and Open Source Software

public draft version 1.0: 10 October 2008

Contractors: Unisys Belgium
UNU-MERIT

Authors: Rishab Aiyer Ghosh
Ruediger Glott
Patrice-Emmanuel Schmitz
Abdelkrim Boujraf

OSOR Guideline on Public Procurement and Open Source Software - public draft v1.0 P. 1

EU Parliament Report A5-0264/2001:
*"Calls … source code **not** made public to be… in … **'least reliable'** category;"*

UNU-MERIT Study 2007: *"Study on the economic impact … of FLOSS"*

European Union Public License
Compatible with popular OSS:
GNU GPL v.2 , OSL, CPL, EPL, Cecill
In line with the EU legal system:
22 EU Languages & Copyright & Liability

OSOR FLOSS Procurement Guide

What has been accomplished so far?

DB's ICE-T /3 ETCS retrofit program

DB's contract with Alstom to OSS ICE-T ETCS OBU Software

Tools evaluation: 9 "Candidates" too chose from.

ICE-T

2015 +

EUPL

"openETCS Option"

3.0.0 proprietary

"hand made" OSS

3.x.y proprietary

Reference OBU for Lab Testing

MoU

Open Formal Specifications

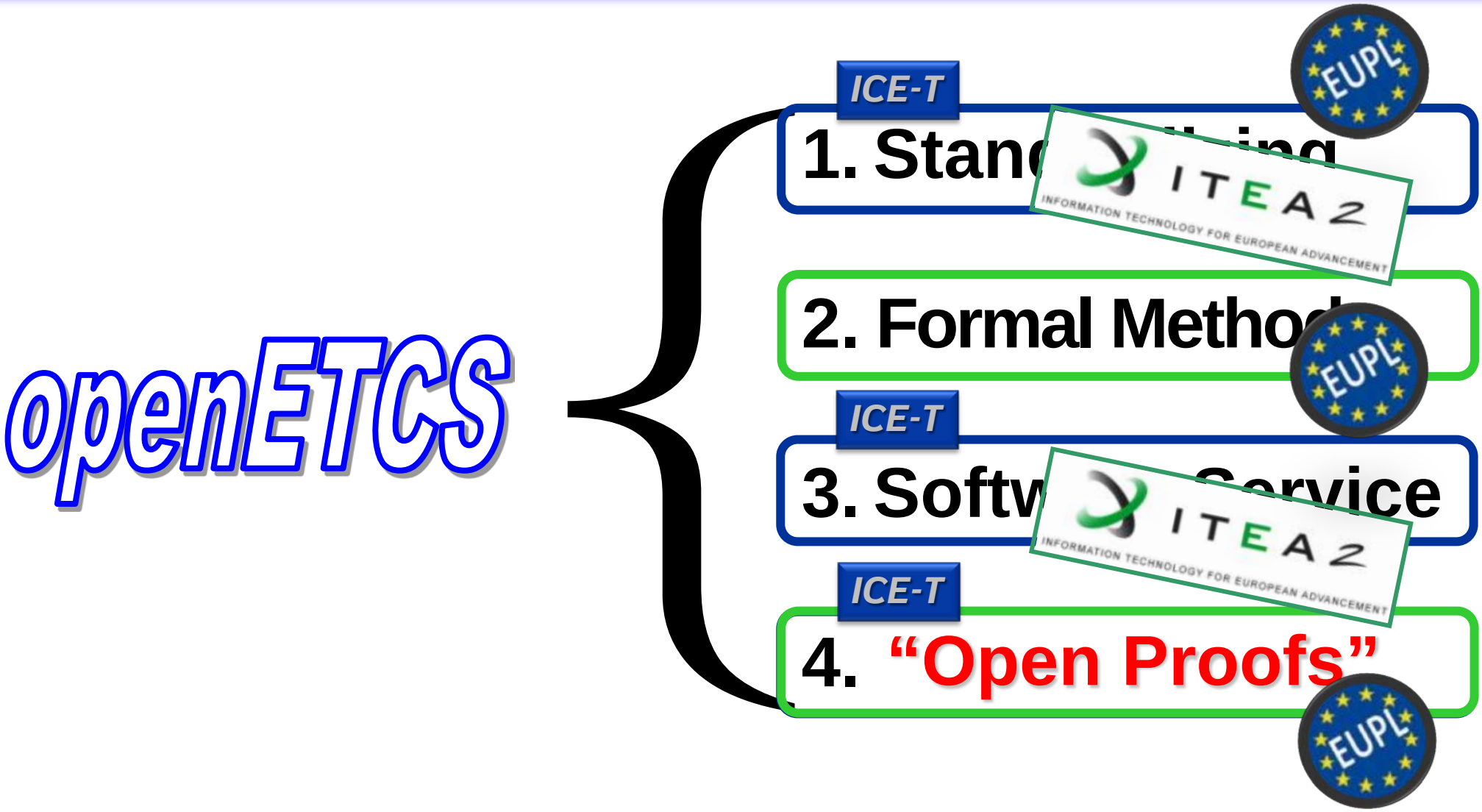
Non-vit... openETCS ...nce OBU

Vital openE...

ERTMS Formal Specs® licensed under EULP

ERSA ETCS OBU TCSim Software under EUPL

What is the status so far?



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.

New WP 7: “open ETCS Tools Chain”

Date	Deliverable	Description
T0+13	D7.1 (Systerel)	Report on the final choice(s) for the primary tool chain (means of description, tool and platform)
T0+15	D7.2 (Systerel)	Report on all aspects of secondary tooling (results of T7.2)
T0+19	D7.3 (Systerel)	Tool chain qualification process description
T0+20	D7.4 (Universität Bremen)	Tool chain first release
T0+36	D7.5 (Eclipse Source)	Ecosystem Artefacts: Proposed Terms of use, Proposed Committer Agreements, Proposed IP Policy, Proposed Development Process Description, Development Process Guidelines, Infrastructure Documentation, Infrastructure Template, Evolution Report of previous Deliverables

New WP 3: “Modeling – Code Generation”

Date	Deliverable	Description
T0 + 21	D3.5: System Specification Model (ERTMS Solution)	Development of a semi-formal model of the Subset 26. This task might be performed in parallel on several fragments of Subset 26 by various contributors, provided the tooling enables us to merge the obtained model together
T0 + 27	D3.6: Functional Model, (ERTMS Solution)	Definition of a function model as defined in previous table and of the corresponding functional API
T0 + 30 {T0 + 24} {first version}	D3.7: System architecture model with physical allocation (Alstom)	Definition of an hardware architecture compliant with the safety, availability and real-time requirements, Allocation of the functional blocks to and/or splitting of the functional blocks between the processors
T0 + 36 {T0 + 27} {first version}	D3.8: Open Source Code (PiEM) (Fraunhofer)	Generation of the Open Code Source (PiEM: Platform Independent Execution Model)