



***openETCS* : Open Source Prinzipien für das Europäische Zugsicherungssystem**

DB Netz AG / Alstom Transport GmbH

Klaus-Rüdiger Hase / Jean Y. Koulischer

ETCS Onboard Programm

Graz, 14.09.2011

Signale & automatische Zugsicherung

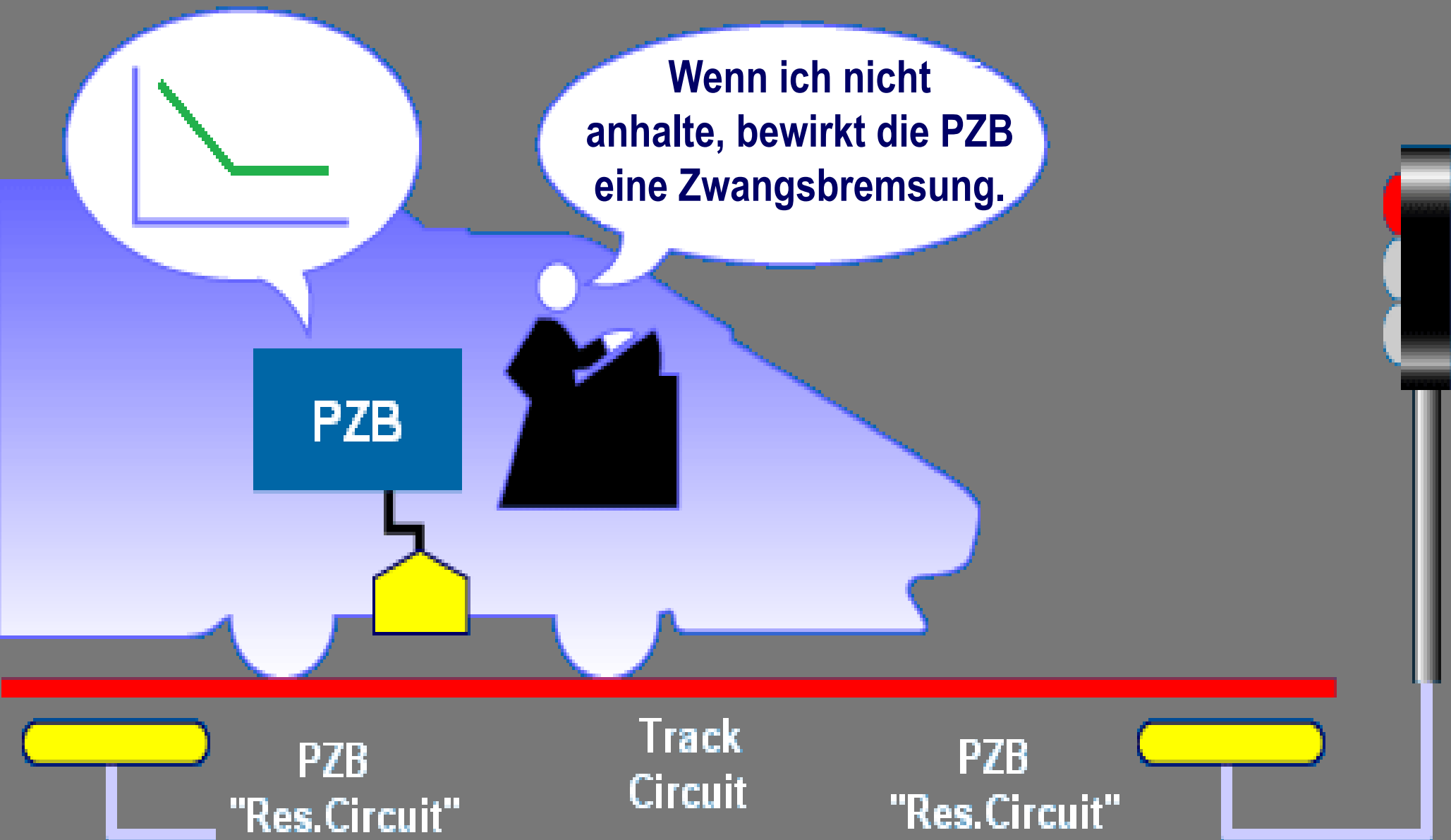


Quelle: Wikipedia



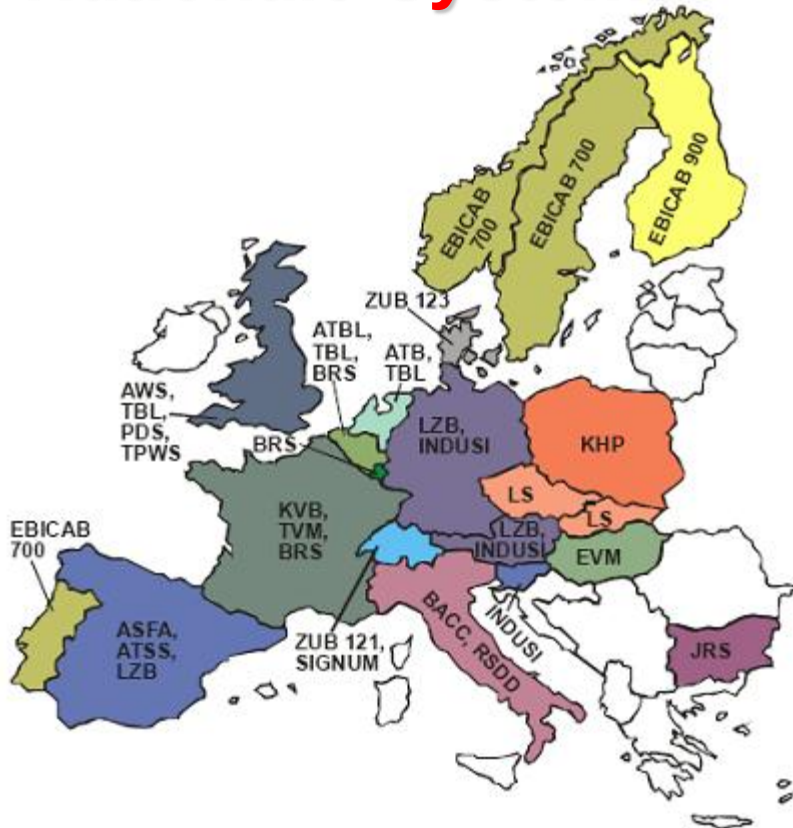
Quelle: Deutsche Bahn AG

Automatische Zugsicherung (PZB seit 1934)

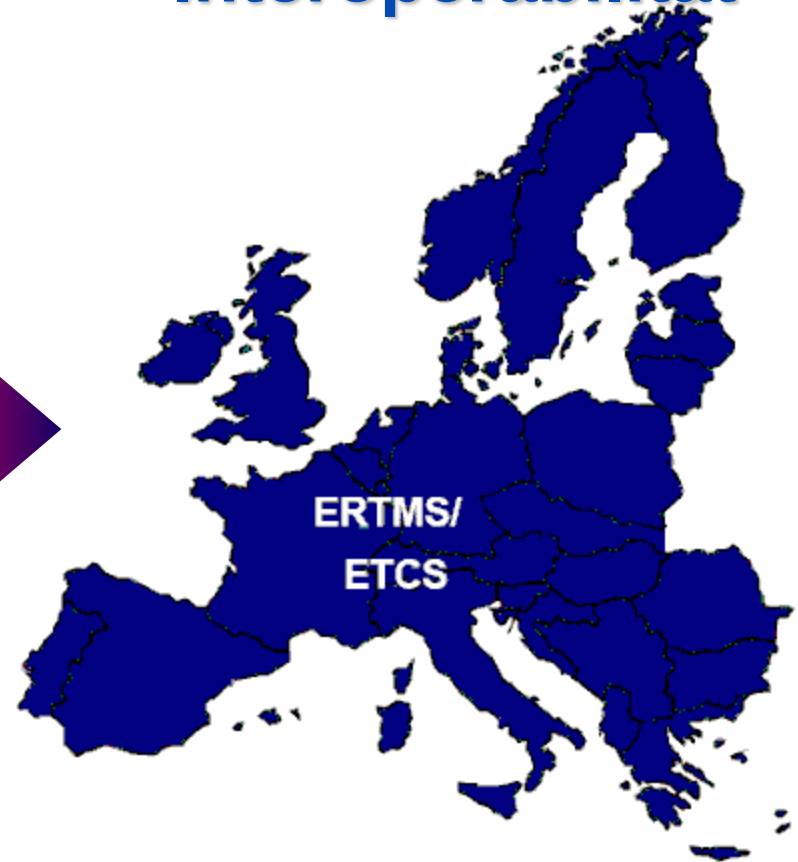


Historisch bedingte Vielfalt

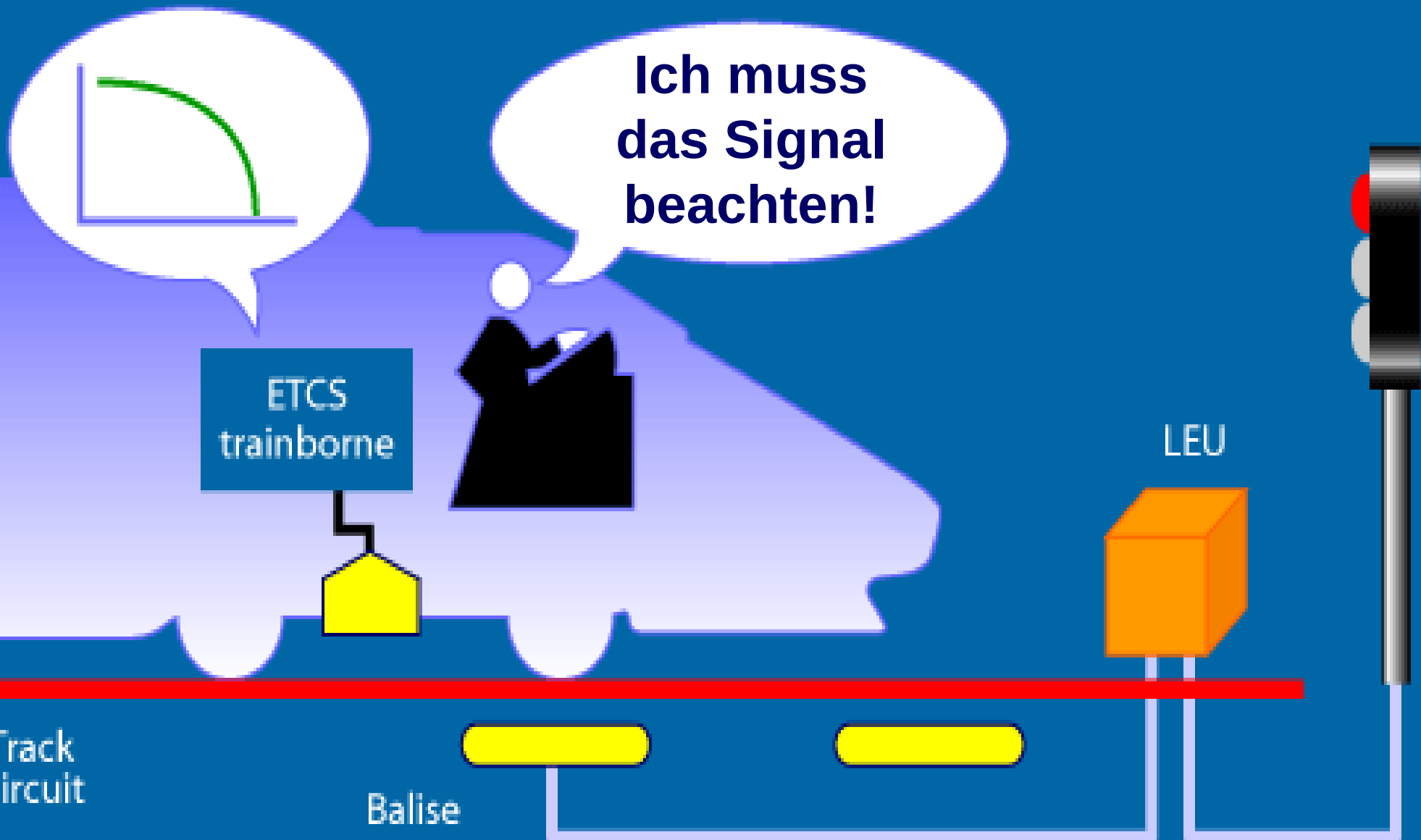
**Bis heute:
Nationale Systeme**



**Zukunft: Europäische
Interoperabilität**



ETCS Level 1



ETCS Level 2

**European
Vital
Computer**

EVC

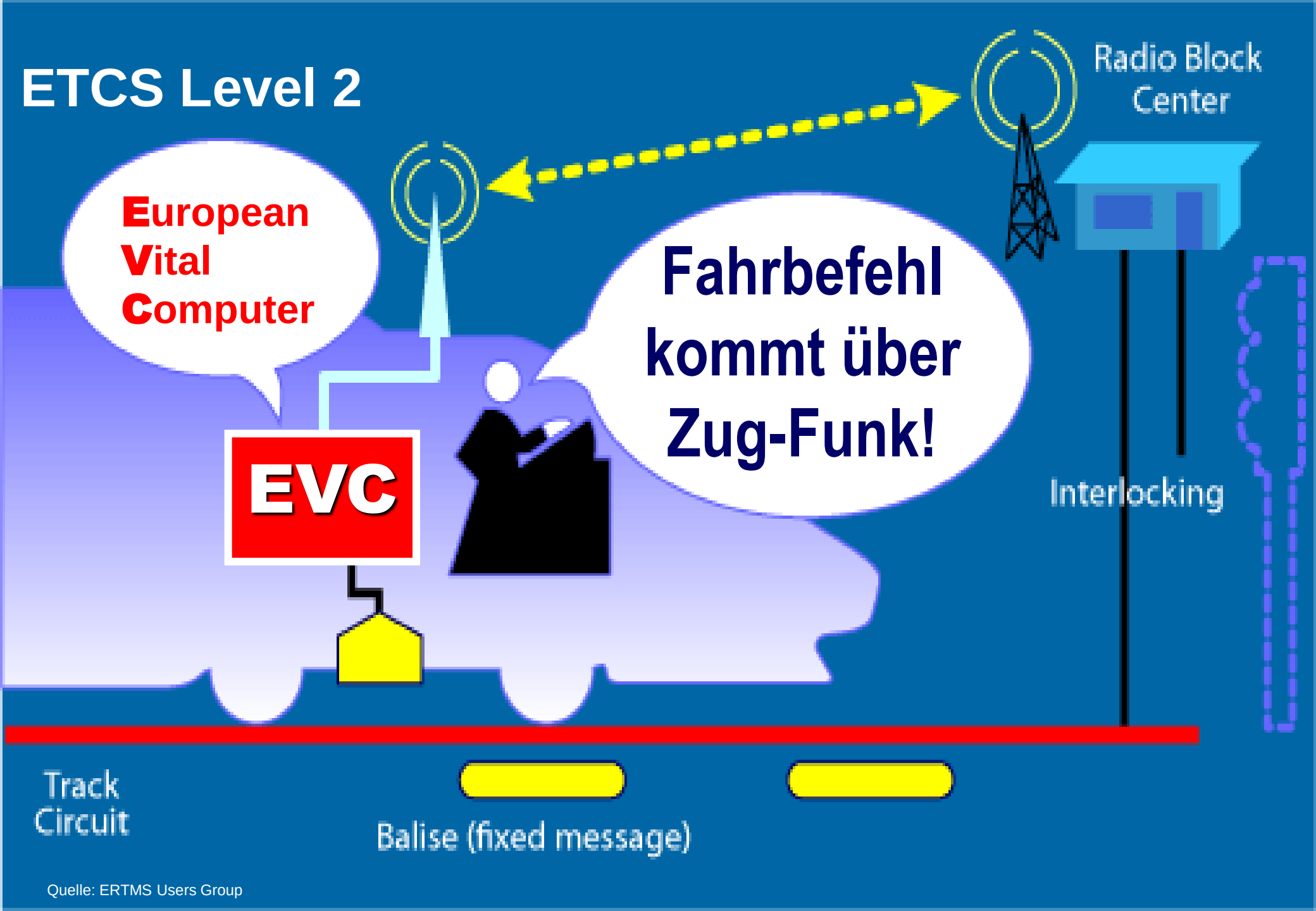
**Fahrbefehl
kommt über
Zug-Funk!**

Radio Block
Center

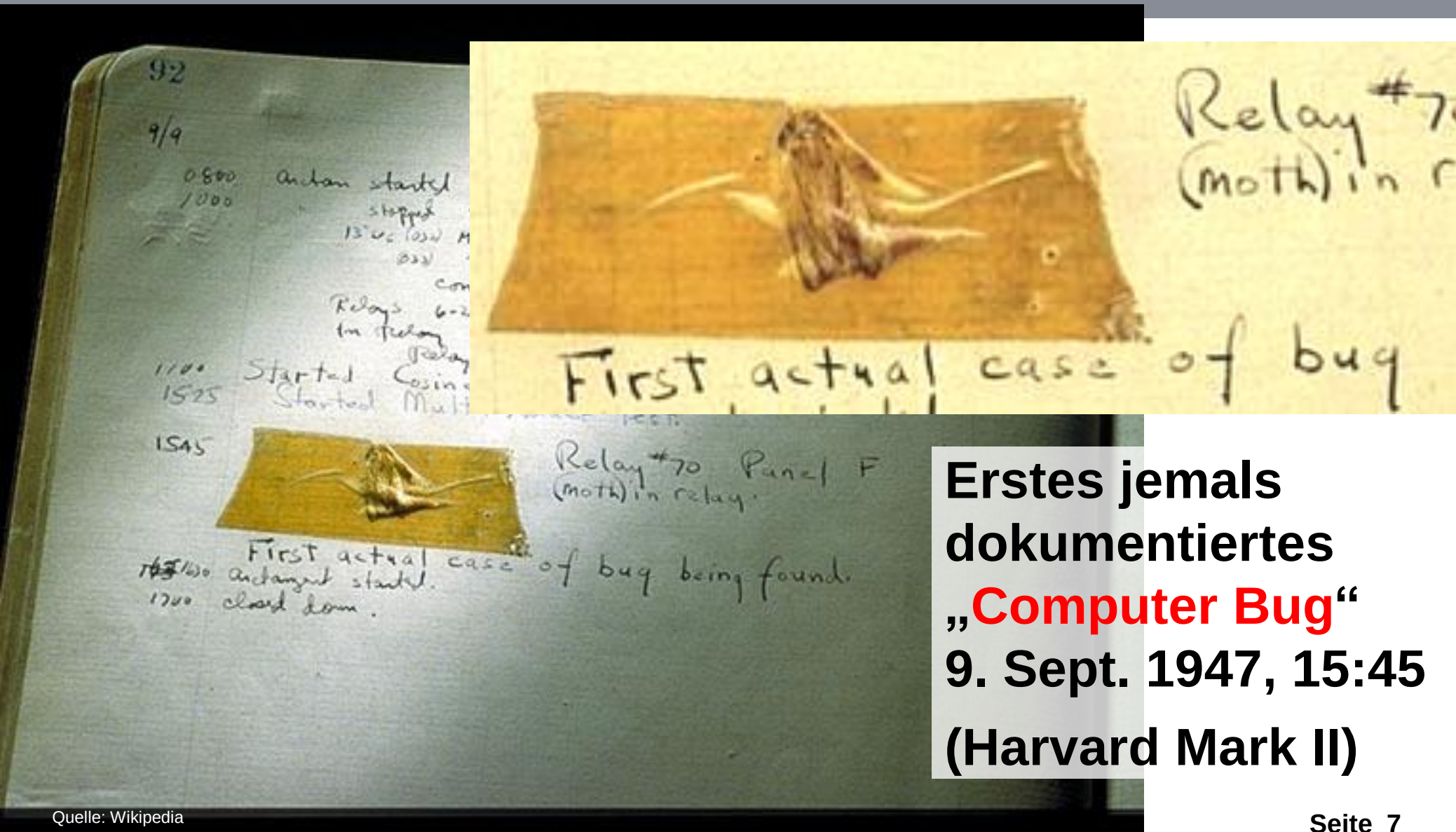
Interlocking

Track
Circuit

Balise (fixed message)



Computer für “SAFETY” ? ... haben „Bugs“ !



Erstes jemals
dokumentiertes
„**Computer Bug**“
9. Sept. 1947, 15:45
(Harvard Mark II)

Computer-Bugs: Ärgerlich, störend, gefährlich !

Foto 2



Foto 3



Entgleiste Lok Re 465 007-3

16. Oktober 2007: Entgleisung an der Lötschberg-Basislinie bei Frutigen wegen eines Softwarefehlers im ETCS Radio Block Center (RBC) *)

*) aus Unfallbericht, Quelle: http://www.uus.admin.ch/pdf/07101601_SB.pdf

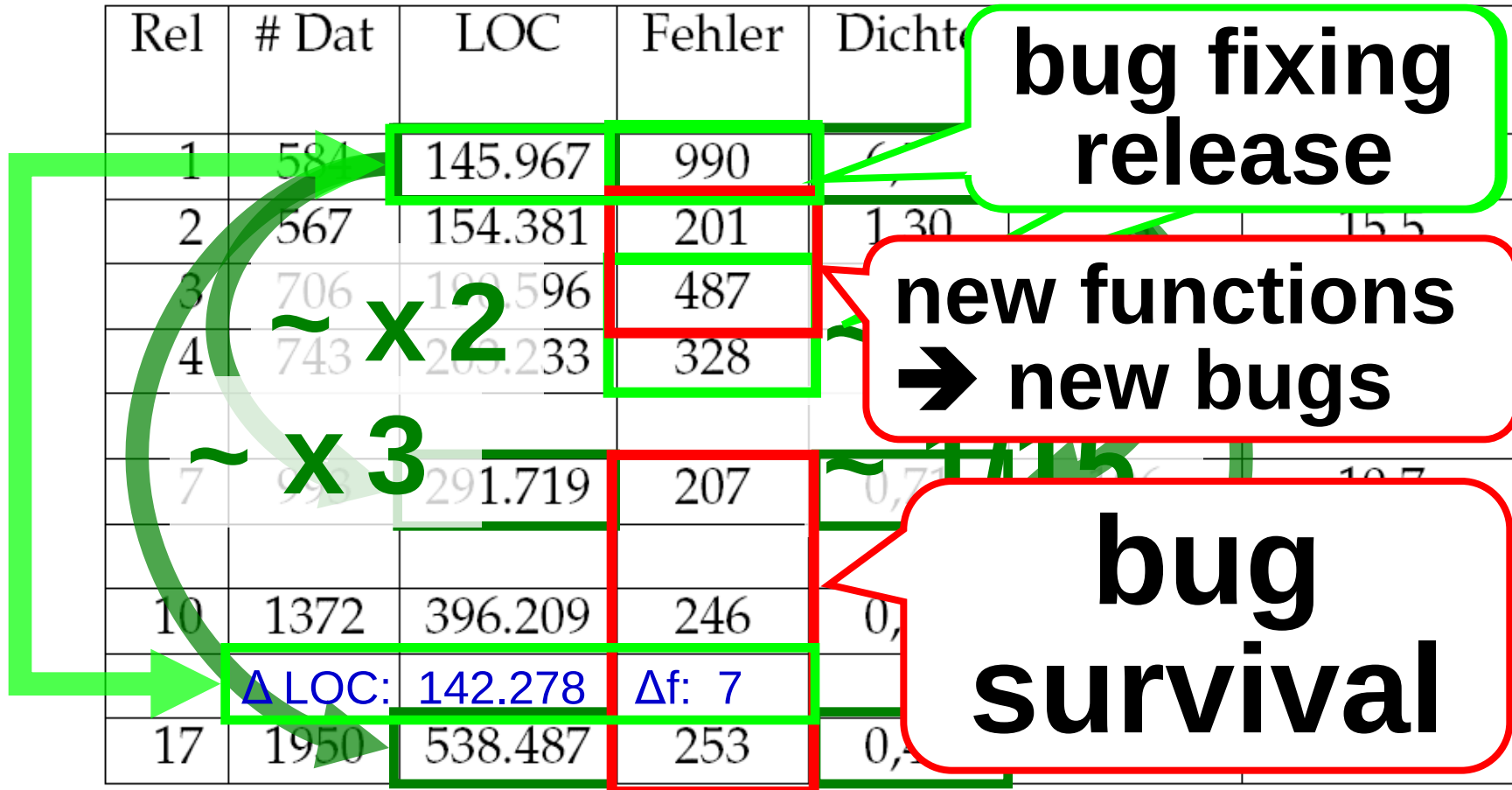
Wie viele „Bugs“?

- Typische Qualitäts-SW: **1 - 10 Bugs je 1.000 lines of code (TLOC)**
- Sehr ausgereifte, weit verbreitete SW: **0,5 Bugs per TLOC**
- Höchste Softwarequalität:
 - *< 1 Fehler auf 10 TLOC*
 - Kosten mehr als 1.000 US\$ je LOC (1977)
 - *US Space Shuttle mit 3 Mio. LOC zu 3 Mrd. US\$*

➔ Kostenniveau untypisch für Bahnsektor (< 100€/LOC)
- Typische ETCS Kern-Softwaregröße: 100 ... 350 TLOC
 - Das bedeutet: 100 ... 1.000 unentdeckte Fehler je EVC
 - Wie und wann findet man die „Bugs“?

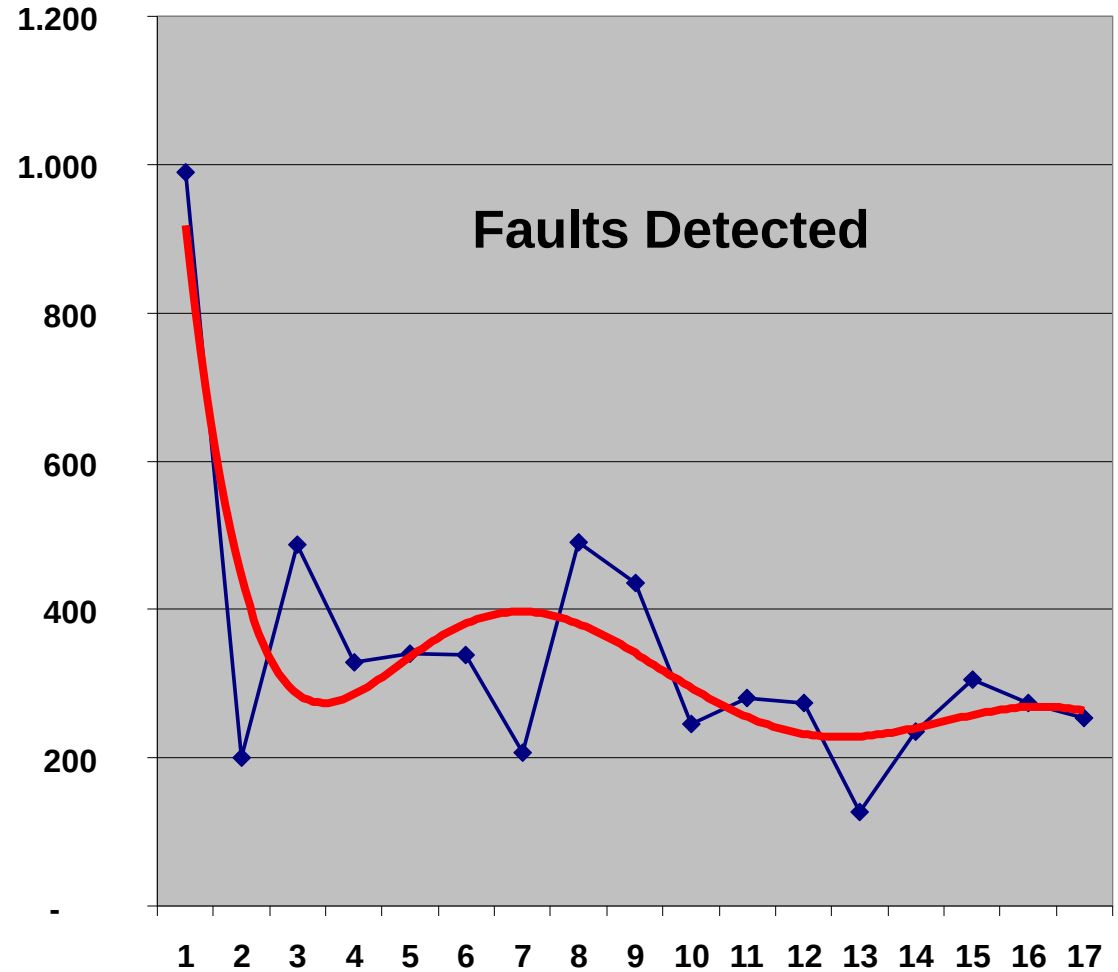
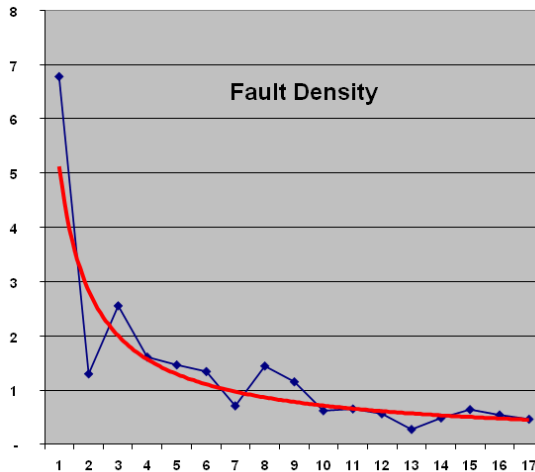
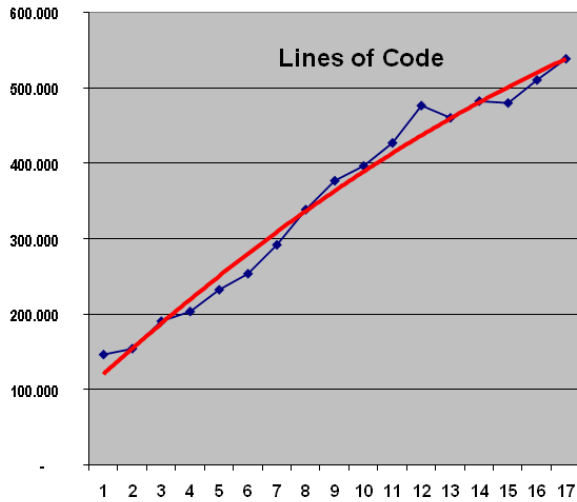


Fehler in komplexer Software



OSTRAND, Thomas J. ; u.a.: "Where the Bugs Are", In: ROTHERMEL, Gregg (Hrsg.): Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis, Bd. 29, 2004, S. 86–96

Lebenszyklen komplexer Software



Lebenszyklen komplexer Software

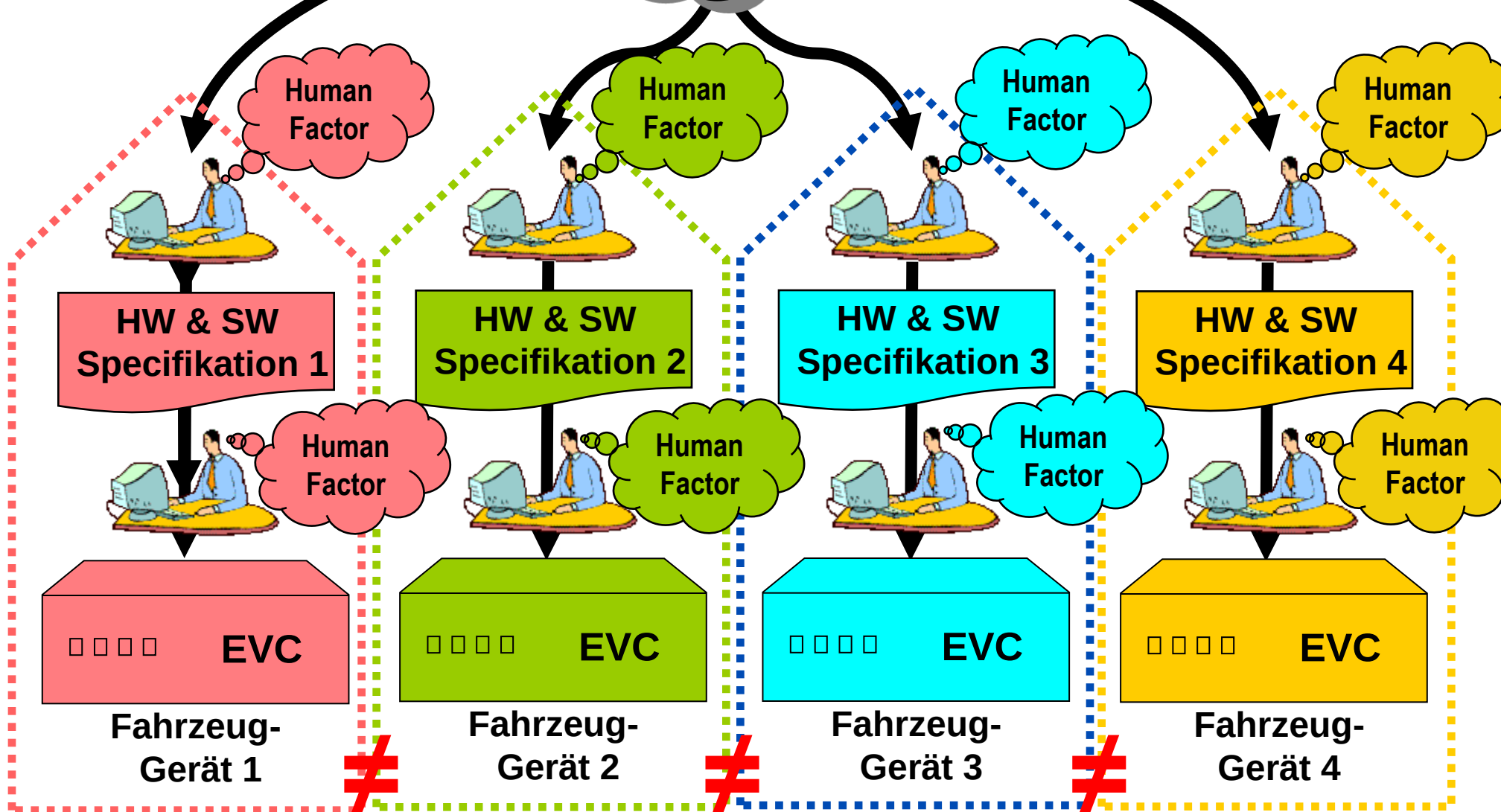
Das Beispiel zeigt:

Software wächst unaufhörlich → Updates sind unvermeidbar

Komplexe Software braucht dauerhafte Pflege.

ETCS Geräte-Entwicklung heute:

ETCS
SRS 3.0.0
"Prosa"



Abhängigkeit vom Lieferanten

Software wächst unaufhörlich → Updates sind unvermeidbar

Komplexe Software braucht dauerhafte Pflege.

Für Kunden proprietärer Software gibt es ein Problem:

- Sie sind völlig vom Originalhersteller abhängig.
- Für die Softwarepflege gibt es heute keinen Wettbewerb !

... und das für 15, 20 oder 30 Jahre ???

Wie besser machen?

- | | | |
|-------------------------|---|----------------------------|
| Komplexität | ➔ | 1. Standardisierung |
| Mehrdeutigkeiten | ➔ | 2. Formale Methoden |
| Software-Fehler | ➔ | 3. Langzeit-Service |
| Abhängigkeit | ➔ | 4. “Open Proofs” |



“Open proof” idea

- “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)



ERA's
Responsibility

Get it
right !

SRS 3.2.0
"Prosa"

Human
Factor

Formal System
Requirement Spec.

Human
Factor

Human
Factor

Formal Language
Functional Vehicle
Specification

Safety
Case
Docs

openETCS
Tools

Synthetic
test cases &
response pattern

openETCS
Project

SW Code
Generator

Parameters

openETCS

API

HW

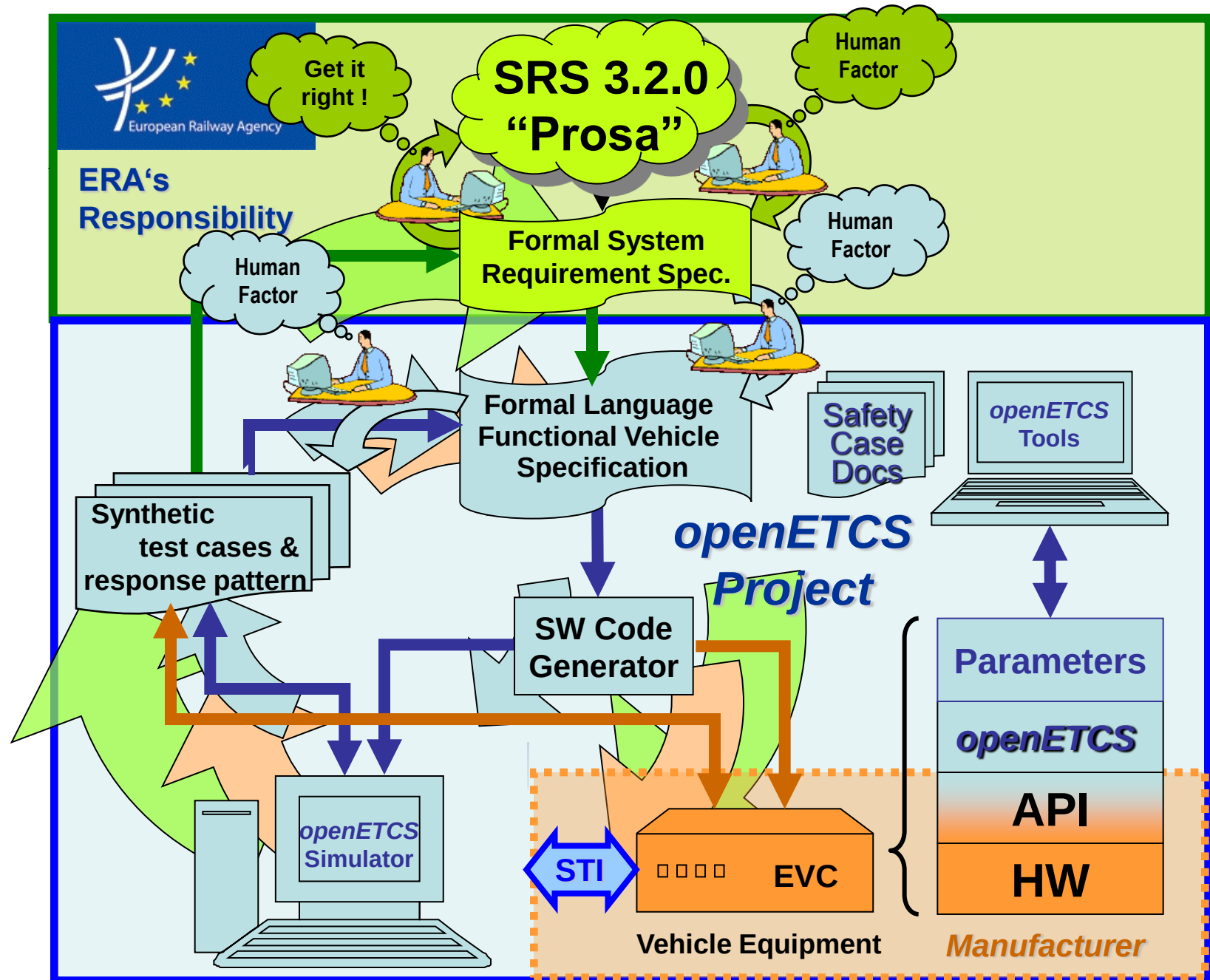
openETCS
Simulator

STI

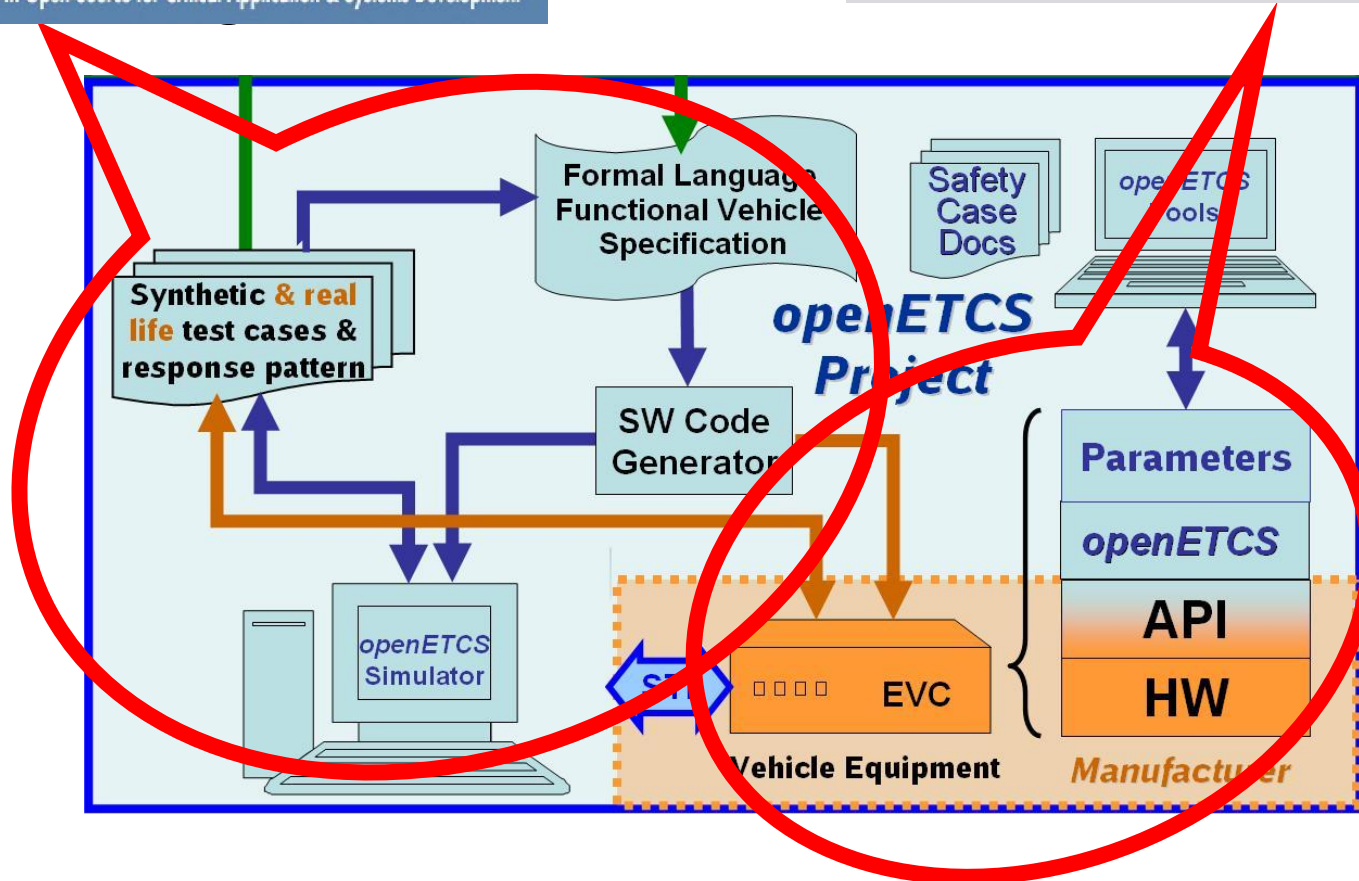
EVC

Vehicle Equipment

Manufacturer



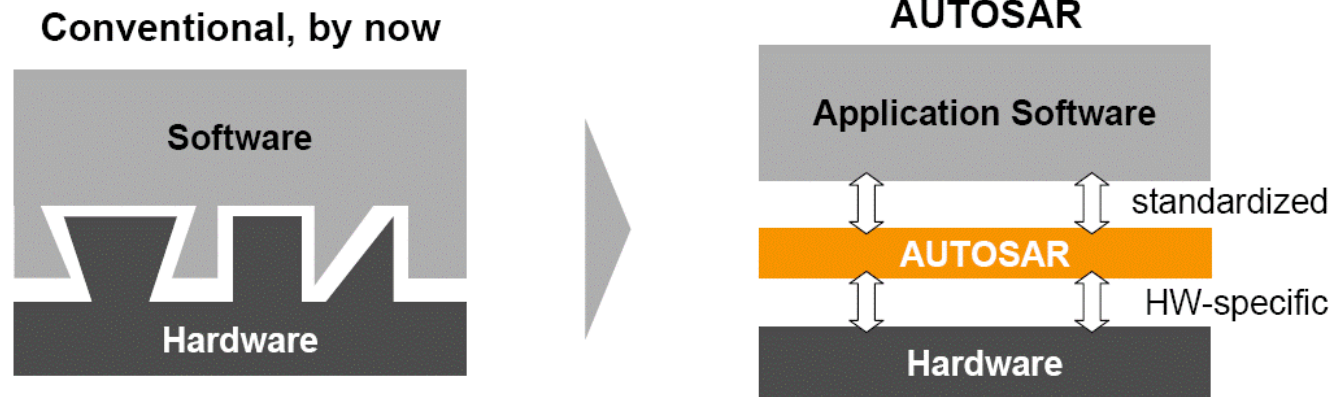
Umfang von openETCS



API in der Automobil-industrie



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.

AUTOSAR – Core Partners and Members

Status: 30th September 2009

9 Core Partner



10 Development Member



86 Associate Member
16 Attendees

56 Premium Member



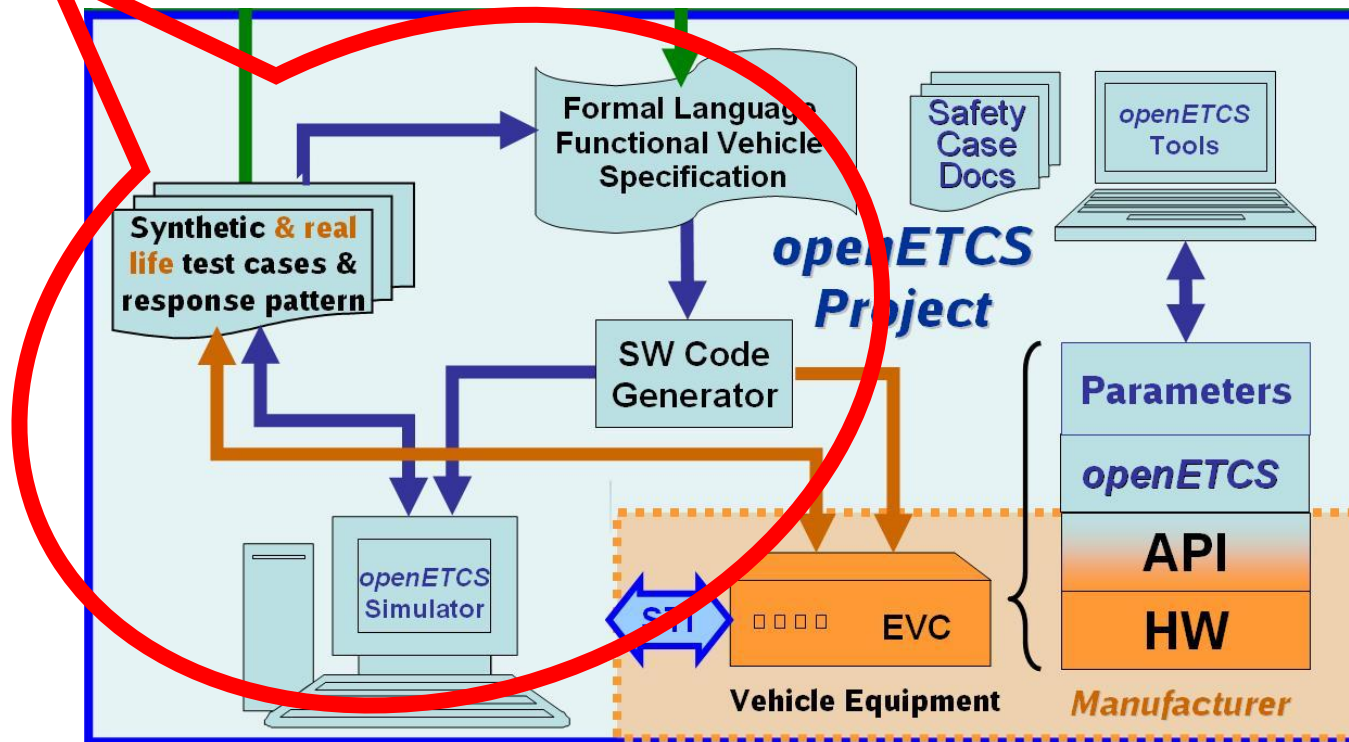
Up-to-date status see: <http://www.autosar.org>

- AUTOSAR Confidential -

Courtesy of

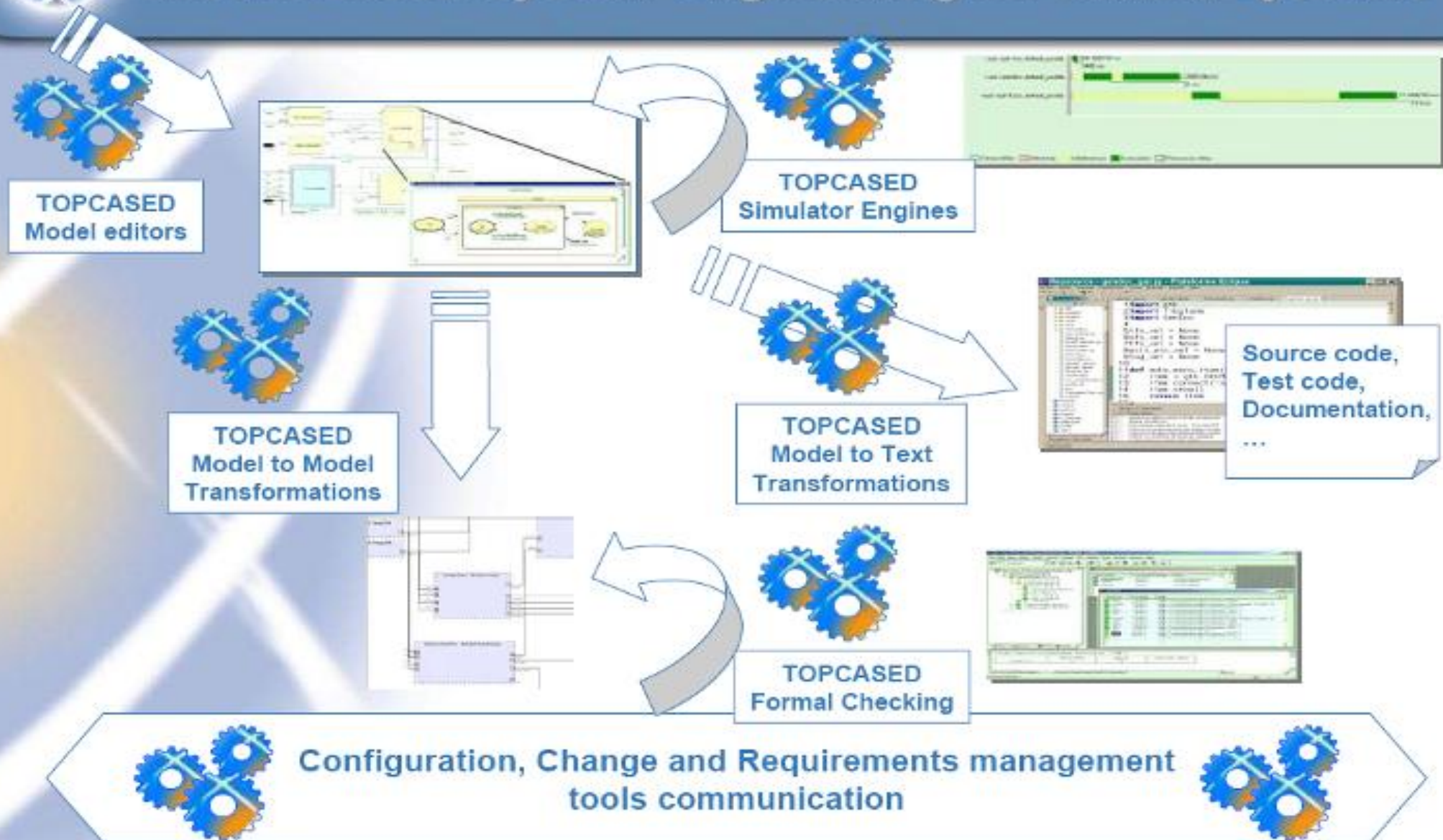
AUTOSAR

Umfang von openETCS



TOPCASED overview

Model Based System Engineering for critical systems





TOPCASED project – initial members

Industries

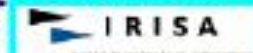


SMEs

Tectosages



School/Universities

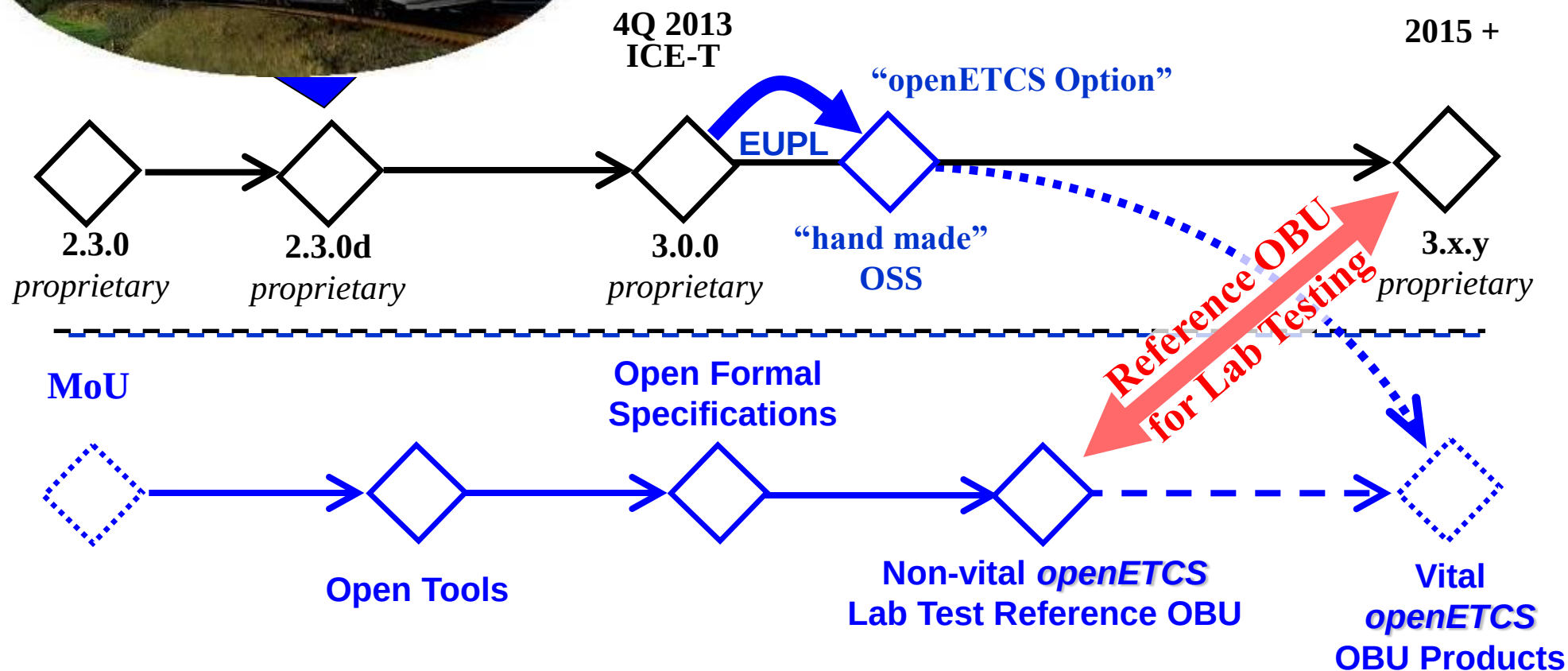


Laboratories

openETCS Produkteinführung



R&D and Product Launching Schedule



openETCS-Project implementing “Open Proofs”

Kommerzieller Kontext

Ausschreibung DB Fernverkehr im Frühjahr 2010 für Nachrüstung der ICE-T und ICE3-Baureihen mit ETCS Bordgeräten (121 Fahrzeuge)

Darin enthalten erstmals zwei neue Forderungen aus „*openETCS*“:

- „Muss-Option“ für einen Software-Service-Vertrag (6 Jahre Laufzeit)
- „Soll-Option“ für ein Open Source Software Angebot

Alstom hat ein *openETCS*-Konzept entwickelt und angeboten

- Alstom hat mit diesem Konzept den Zuschlag erhalten.

Motivation

Hauptmotivation eines Herstellers sich der **openETCS**-Initiative anzuschließen:

- Beschleunigung der ETCS-Migration in Europa

Haupthindernis für ETCS aus Sicht der Infrastrukturbetreiber:

- Problemen mit der Interoperabilität
- Eine offene Referenzsoftware könnte hier den Prozess der Harmonisierung beschleunigen helfen

Haupthindernis für ETCS aus Sicht der Fahrzeughalter:

- Noch deutlich höhere Kosten als für die meisten Class B-Systeme
- **openETCS** könnte hier Kosten senken helfen

Kostensenkung durch openETCS

Kosten werden durch Einmalkosten und wiederkehrende Kosten bestimmt:

Einmalkosten: Hier arbeitet Alstom aktiv an der Schnittstellenstandardisierung.

Wiederkehrende Kosten:

- **Software-Upgrades** nach Einschätzung von Alstom **mindestens alle zwei Jahre**
- **Kontinuierliche Weiterentwicklung der ETCS-Software:**
- **Erfahrung Alstom:** Ca. alle neun Monate entsteht eine neue „Baseline“, für
 1. *Integration offizieller „Change Requests“*
 2. *Spezifische Funktionen einzelner Länder.*

Die Idee einer konsolidierten ETCS-Softwareentwicklung als „Basisprodukt“ für alle Hersteller könnte dem ganzen Sektor erhebliche Kosten sparen.

Um die ETCS-Standardisierung und Kostensenkung zu beschleunigen, hat sich Alstom entschlossen, seinen Softwarekern, gemäß UNISIG Subset 026, aufgrund der derzeit umfassendsten Erfahrung und dem damit erreichten hohen Reifegrad, im Rahmen des ICE-T/ICE3-Angebotes als Open Source Software unter die EUPL v.1.1 zu lizenzieren.

Herausforderungen

Alstom sieht zwei wesentliche Herausforderungen für *openETCS*:

➤ **Technische Herausforderung:**

➤ *Sicherheitsmanagement*

➤ *Sicherheitsnachweis*

➤ **Kommerzielle bzw. juristischer Herausforderung:**

➤ *Gewährleistung*

➤ *Zivilrechtlicher Haftung*

➤ **Diese Themen sollen in einem übergreifenden Projekt bearbeitet werden.**

➤ **Liefervertrag ICE-T/ICE3 besagt:**

Offenlegung der ETCS-Kernfunktionalität bis zum 31.12.2016

Zwischenperiode

Was passiert in der Zwischenzeit?

Die **openETCS**-Initiative kommt gerade rechtzeitig vor Einführung der Baseline 3

Fragestellungen können an der noch gültigen SRS Vers. 2.x studiert werden

Bis Ende 2011 werden ca. 50 Mio. km im kommerziellen Betriebseinsatz erreicht

Alstom prüft die Möglichkeit, das Konzept einer Lizenzierung schon mit der aktuellen Softwareversion zu erproben, um

- Reibungslosen Übergang für **openETCS** mit Baseline 3 zu garantieren
- Eine breite Akzeptanz zu erreichen

Top Level Vision:

- Offenes System → Volle Transparenz
- Wahlfreiheit beim Service

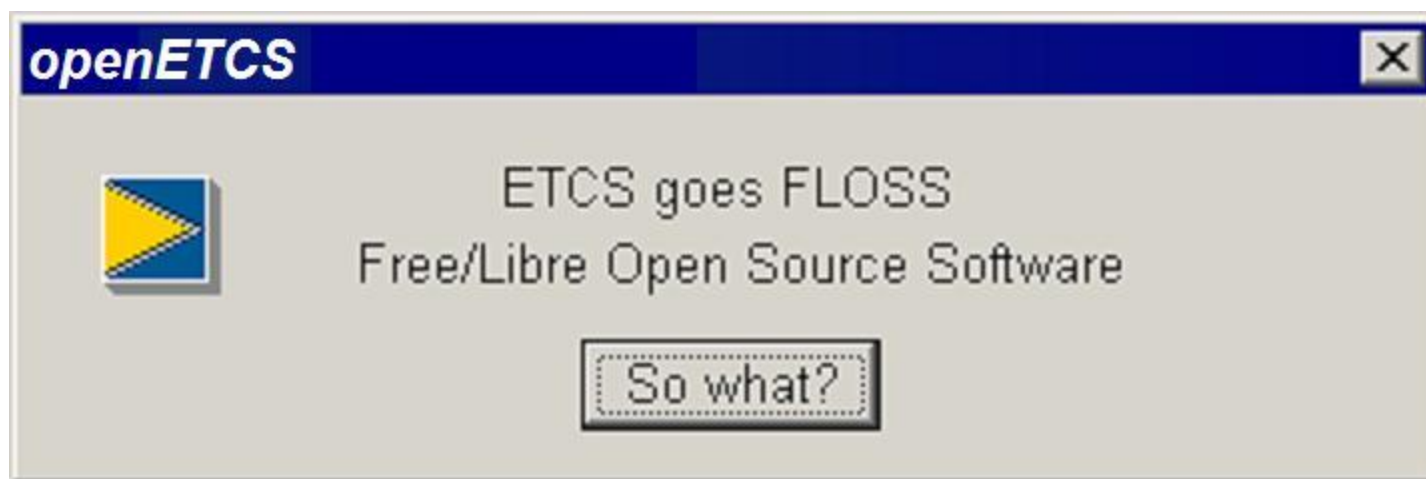
Technischer Level:

- Offene formale Spezifikation & Modell → Eindeutigkeit
- Open Source Software, Tools & Proofs → Nachhaltigkeit
- Offenes Referenzsystem → Interoperabilität

↪ ... auf existierende Technologien zurückgreifen:
TOPCASED, AUTOSAR Prinzipien, vorhandene OBU HW & SW design, ...

Was **openETCS** nicht ist:

- Es ist keine neue “Version” von ETCS !
- Es erfordert keine komplette Neuentwicklung! → Nur neue Lizenzen.



Vielen Dank für Ihre Aufmerksamkeit.