Safety Methodology – CENELEC and Safety PoC – Radio Communication

1. Introduction
2. CENELEC Assessment
3. SSRS CENELEC compliance
4. System Safety Analysis PoC
5. Conclusion

Introduction

- Activity in the frame of WP4 V&V
- CENELEC Assessment activities
- SSRS compliance with CENELEC requirements
- SSRS based System Safety Analysis

CENELEC Assessment

- Main CENELEC activity: Quality Assurance
  - Activity drived by SQS
  - Documentation :
    - QA Plan
    - Review process
    - Software Configuration Management Plan
    - Competencies matrix
  - Consider the Quality assurance application to the field
- Quality and Safety Assessment: Internal Assessment
  - Activity performed by CENELEC recognize experts (N. Schäfer, F. Vallée, J.L. Boulanger)
  - Documentation:
    - Internal DoW
    - Internal Assessment Plan
  - START after first QA Plan release

SSRS CENELEC compliance

- EN50128:2011 – Software for Railway control and protection system, applied to SSRS model
- Application on concrete case: Uwe’s Manage Radio Communication model
- Different parts of the standard concerned for the model:
  - So far, V&V is not considered for the evaluation
  - 7.2 – Software requirements
  - § 7.3 Architecture and Design
    - § 7.3.1 Interface
    - § 7.3.2 Design
  - § 7.4 Component design
- Address Safety requirements for CENELECs not fulfilled
  - These requirements will have to be closely considered

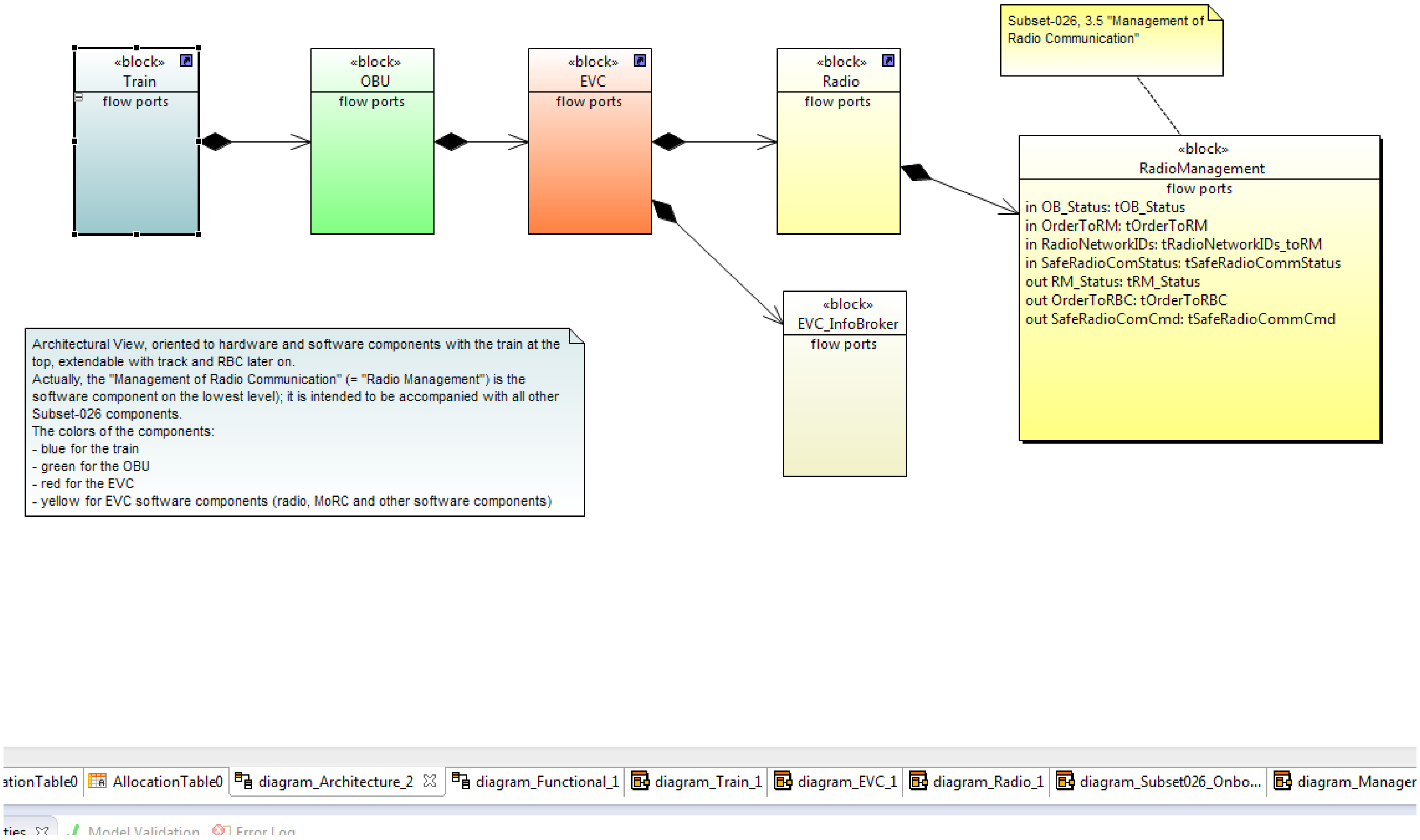
SSRS CENELEC compliance

- Main features and concerns to consider:
  - New field of application for CENELEC : Model Driven Engineering
  - Necessity to generate required documentation for CENELEC compliance
  - Separation between SSRS text, and SSRS model
  - Potential discrepancy between SCADE System model and SysML Papyrus model ➔ need of methodology defined
  - Expression of HW and SW functional and safety constraints
  - Consider the requirements traceability matter
    - Inputs: Subset26, subset76, FIS,…
    - SCADE System facility certifiable
    - Using PRoR with SysML model
    - Ensure connection between both
  - Implement software components properties in the model

System Safety Analysis PoC

- Inputs
  - SRS Subset26, subset88 & subset91
  - Uwe's Radio Management SCADE System model
    - Functional Interoperability Specification
    - Functional and Organic architecture
    - Data structure
    - Considered as SSRS model sample
- System Safety Methodology
  - EVC Functional description and breakdown (SSRS – Top-Down)
  - Defined a HW environment and structure (Organic Architecture)
  - Connect with Train level SRS System Analysis (Basic Events)
  - Define the feared events at the considered Level
  - Realize Safety Analysis at bottom level (Bottom-Up)

System Safety Analysis PoC

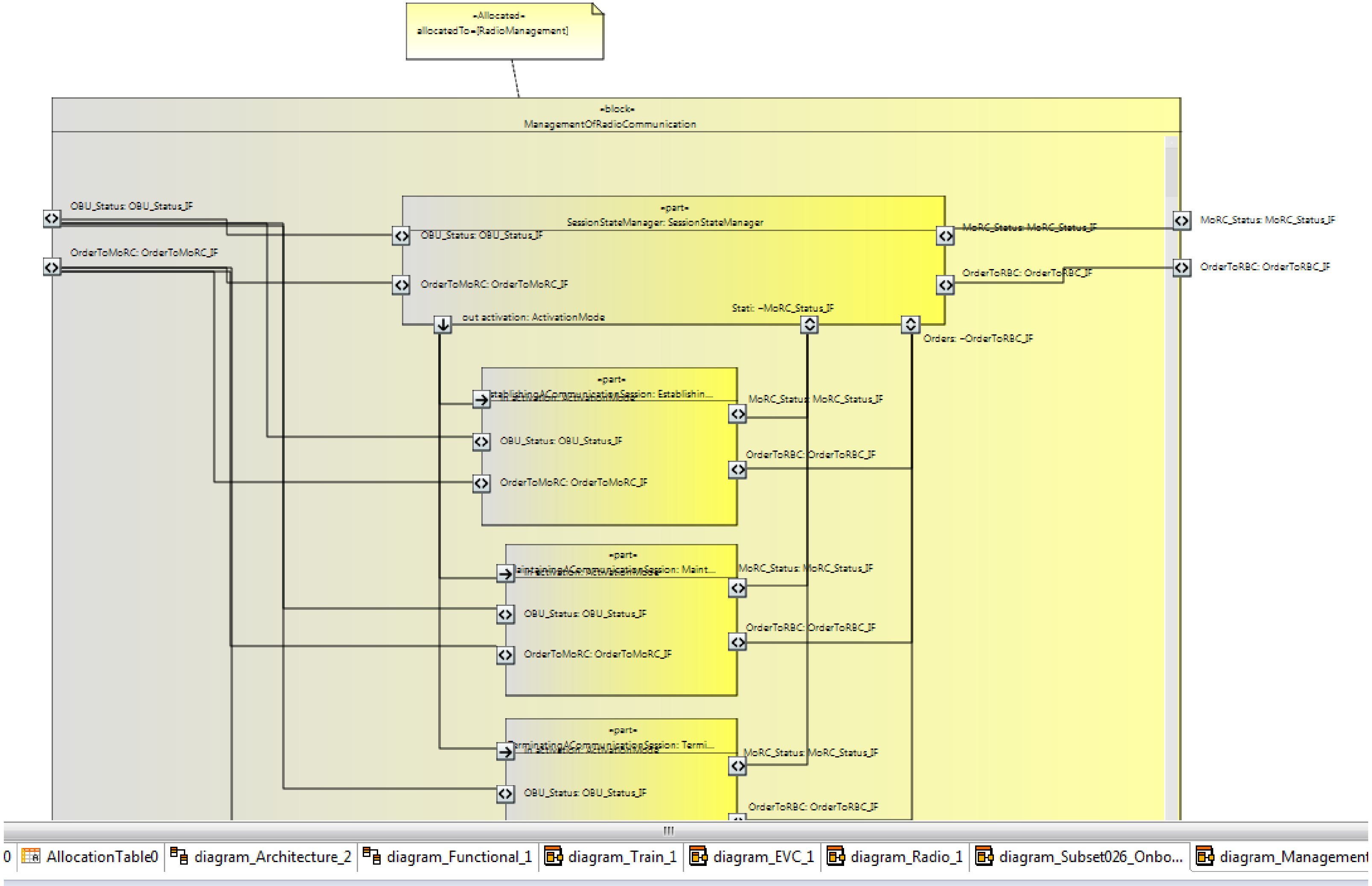


Subset-026, 3.5 "Management of Radio Communication"

in OB_Status: tOB_Status
in OrderToRM: tOrderToRM
in RadioNetworkIDs: tRadioNetworkIDs_toRM
in SafeRadioComStatus: tSafeRadioCommStatus
out RM_Status: tRM_Status
out OrderToRBC: tOrderToRBC
out SafeRadioComCmd: tSafeRadioCommCmd

Architectural View, oriented to hardware and software components with the train at the top, extendable with track and RBC later on.
Actually, the "Management of Radio Communication" (= "Radio Management") is the software component on the lowest level); it is intended to be accompanied with all other Subset-026 components.
The colors of the components:
- blue for the train
- green for the OBU
- red for the EVC
- yellow for EVC software components (radio, MoRC and other software components)

System Safety Analysis PoC


«Allocated»
allocatedTo=[RadioManagement]
«block»
ManagementOfRadioCommunication
OBU_Status: OBU_Status_IF
OrderToMoRC: OrderToMoRC_IF
«part»
SessionStateManager: SessionStateManager
OBU_Status: OBU_Status_IF
OrderToMoRC: OrderToMoRC_IF
out activation: ActivationMode
Stati: ~MoRC_Status_IF
Orders: ~OrderToRBC_IF
MoRC_Status: MoRC_Status_IF
OrderToRBC: OrderToRBC_IF
MoRC_Status: MoRC_Status_IF
OrderToRBC: OrderToRBC_IF
«part»
stablishingACommunicationSession: Establishin...
in activation: ActivationMode
OBU_Status: OBU_Status_IF
OrderToMoRC: OrderToMoRC_IF
MoRC_Status: MoRC_Status_IF
OrderToRBC: OrderToRBC_IF
«part»
aintainingACommunicationSession: Maint...
in activation: ActivationMode
OBU_Status: OBU_Status_IF
OrderToMoRC: OrderToMoRC_IF
MoRC_Status: MoRC_Status_IF
OrderToRBC: OrderToRBC_IF
«part»
erminatingACommunicationSession: Termi...
in activation: ActivationMode
OBU_Status: OBU_Status_IF
MoRC_Status: MoRC_Status_IF
OrderToRBC: OrderToRBC_IF
0
AllocationTable0
diagram_Architecture_2
diagram_Functional_1
diagram_Train_1
diagram_EVC_1
diagram_Radio_1
diagram_Subset026_Onbo...
diagram_Management

System Safety Analysis PoC – Subset88

- ETCS Application Levels 1 &2 – Safety analysis

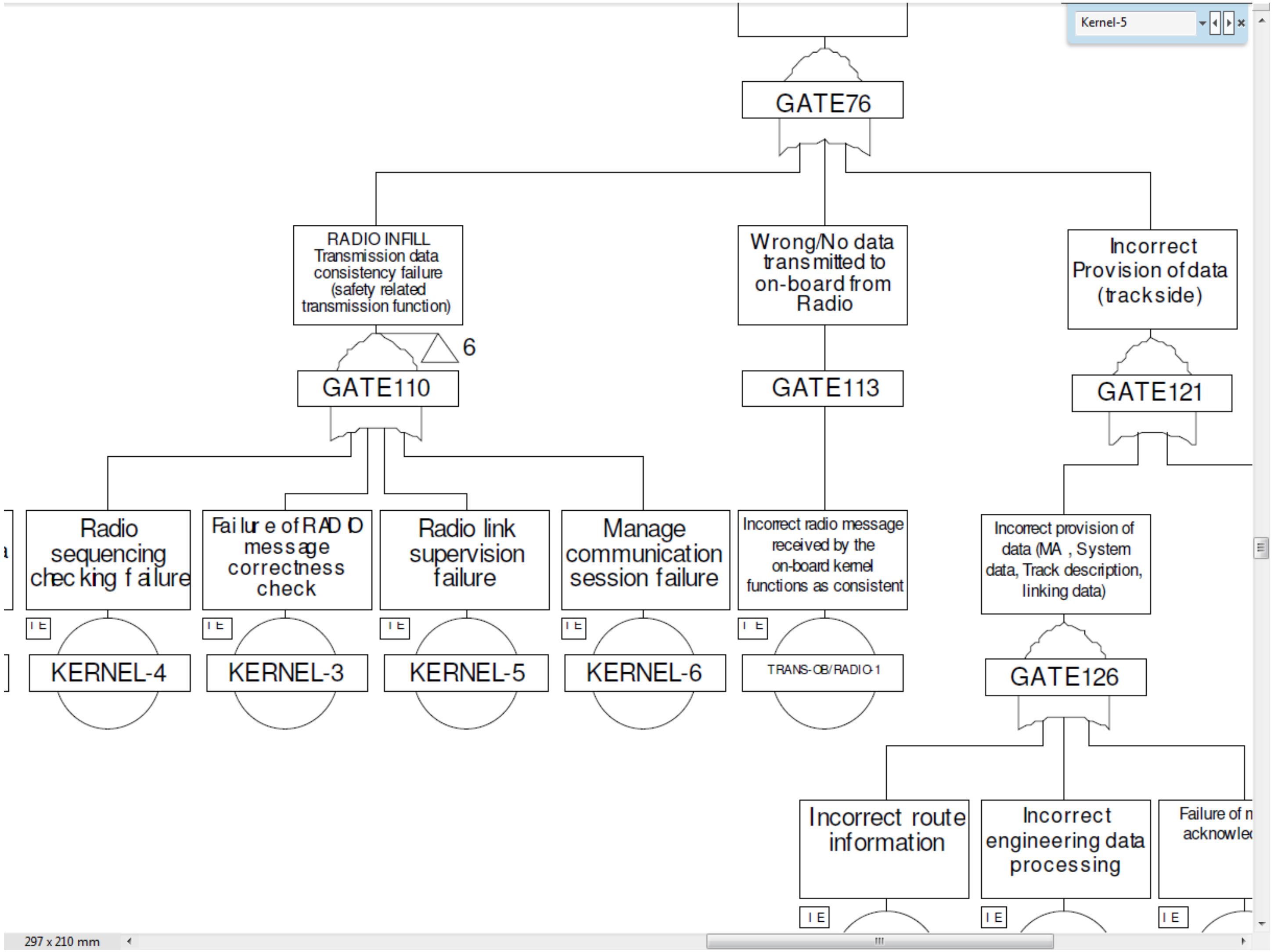
Provides the Safety Analysis at train system level

- Content:
  - Fault Tree Analysis, based on functional analysis (according to ETCS level and mode). ➔ in part 1

  WARNING: FTA = Dysfunctional Analysis (different from a Reliability Bloc Diagram (BDD) = Functional Analysis

  - Failure Mode, Effects and Criticality Analysis (according to ETCS level and mode).➔ in part 2
- Basic Event (FTA) considered
  - Kernel 5
  - Kernel 6

System Safety Analysis PoC - Subset88


Kernel-5
GATE76
RADIO INFILL Transmission data consistency failure (safety related transmission function)
Wrong/No data transmitted to on-board from Radio
Incorrect Provision of data (trackside)
6
GATE110
GATE113
GATE121
Radio sequencing checking failure
Failure of RADIO message correctness check
Radio link supervision failure
Manage communication session failure
Incorrect radio message received by the on-board kernel functions as consistent
Incorrect provision of data (MA , System data, Track description, linking data)
IE
KERNEL-4
KERNEL-3
KERNEL-5
KERNEL-6
TRANS-OB/RADIO-1
GATE126
Incorrect route information
Incorrect engineering data processing
Failure of n
acknowle
297 x 210 mm

System Safety Analysis PoC – Application

- **Focusing on Kernel-6 System Basic Event: Manage communication session failure**
  - ➔ **Considered as EVC feared event (Top Tree for FTA)**
- **Functional Breakdown (from the Model)**
  - SessionStateManager
  - EstablishingACommunicationSession
  - MaintainingACommunicationSession
  - TerminatingACommunicationSession
  - RegisteringToTheRadioNetwork
- **Link the functional Blocks to the Feared Events**
  - **Functional analysis at the bottom level (signals)**
  - **Define concerned IO signal at different levels**

System Safety Analysis PoC – Application

- Propagate the local component failure to the system

- Need of:
  - Funtional meaning and role of each signal
  - Components functional description
  - Data Dictionnary (interprete the model properly)

- Proof Of Concept based on Safety Architect tool
  - Interface with SysML in the box
  - Fitted for Safety Analysis on Model Based Design for Rail Software

5 - Conclusion

- CENELEC activities already started through quality assurance
- Quality Assessment on the starting blocks (after first QA Plan release)
- Safety Activities linked to the CENELEC AND the V&V tools
  - Need of concrete proof on concept on Safety (to be finished for end of october)
  - Need on stable scope and method for SSRS (on going activities driven by PF Jauquet)
  - Need of choices on tools (SysML is defined, need of clarify SCADE System or Papyrus, so far both are acceptable)

- Thank you – Questions?