MES
MODEL ENGINEERING SOLUTIONS

LATEST ISO 26262 UPDATE
Focusing on Concurrency

Heiko Doerr

MGI Group, 06. December 2016

STARTING POINT

- ISO 26262 released in November 2011
- Second edition available for review as ISO/DIS 26262:2018
  - Final publication scheduled for 2018
- Impact on model-based development – Changes of part 6?
  - 1) Use cases of model-based development
  - 2) Evolution of best practices
  - 3) Handling of concurrency

UPDATE TO ANNEX B – USE CASES OF MODELS

MES
MODEL ENGINEERING SOLUTIONS

- Specification of software safety requirements:
  Models capture corresponding functionality in addition to requirements
- Representation of software architectural design:
  Models capture the static and dynamic aspects of software
- Design and implementation of software units:
  Most prominent use of models in automotive - model based software development
- Integration of software components:
  Models for the integration of software units
- Verification of software:
  Models serve as reference implementation, e.g. for generation of test cases - most likely known as model-based testing

UPDATE DUE TO EVOLUTION OF TECHNOLOGY

- Table 5 Mechanisms for error handling:
  - Measure 1c) Independent parallel redundancy split into a) homogeneous and b) diverse redundancy
- Table 9 Methods for software unit verification
  - Pair-programming added
  - Notion "Semantic code analysis" refined to "Static analyses based on abstract interpretation"
- Table 12 Methods for verification of software integration
  - Verification techniques also applicable to integrated software, e.g. analyses on control or data flow, static code analysis as well as abstract interpretation
- Table 16 Methods for deriving test cases
  - Additional methods: analysis of functional dependencies and operational use cases

MINOR UPDATES TO RECOMMENDATIONS

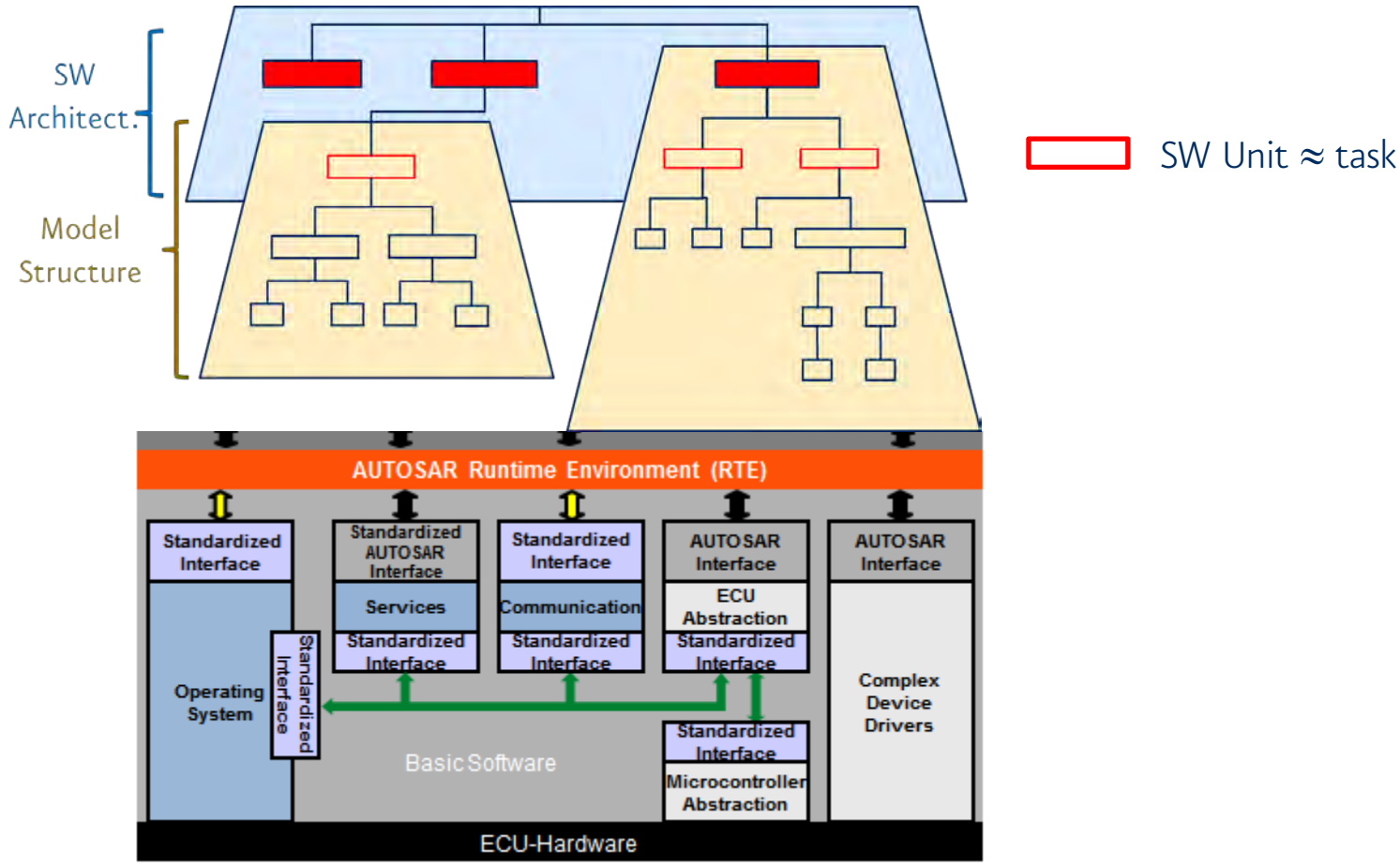
- Changes to level recommendation:
  - “o” → “+”
  - “+” ↔ “++”

    in various tables

MAJOR UPDATE – HANDLING OF CONCURRENCY

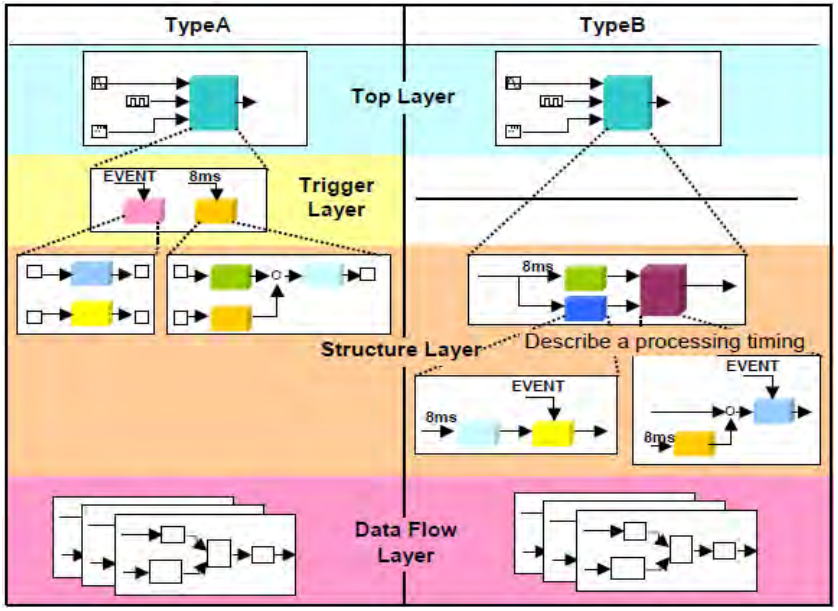
- Table 1 Modelling and Coding guidelines
  - New section of guidelines on the "Representation of concurrency aspects"
- Table 3 Principles for software architectural design
  - Software components of any ASIL shall use only priority-based interrupts
  - Concurrency aspects as processes or tasks shall be expressed
  - Appropriate management of shared resources
- Table 4 Mechanisms for error detection
  - Generalizes the recommended safety measure "Control flow monitoring" to "temporal monitoring of program execution"
  - Active access permission control mechanisms to ensure that safety related resources are not corrupted during execution
- Table 6 Methods for the verification of the software architectural design
  - Recommends scheduling analysis which becomes very important for multi-core of concurrent software system

CONCURRENCY IN MODEL-BASED DEVELOPMENT



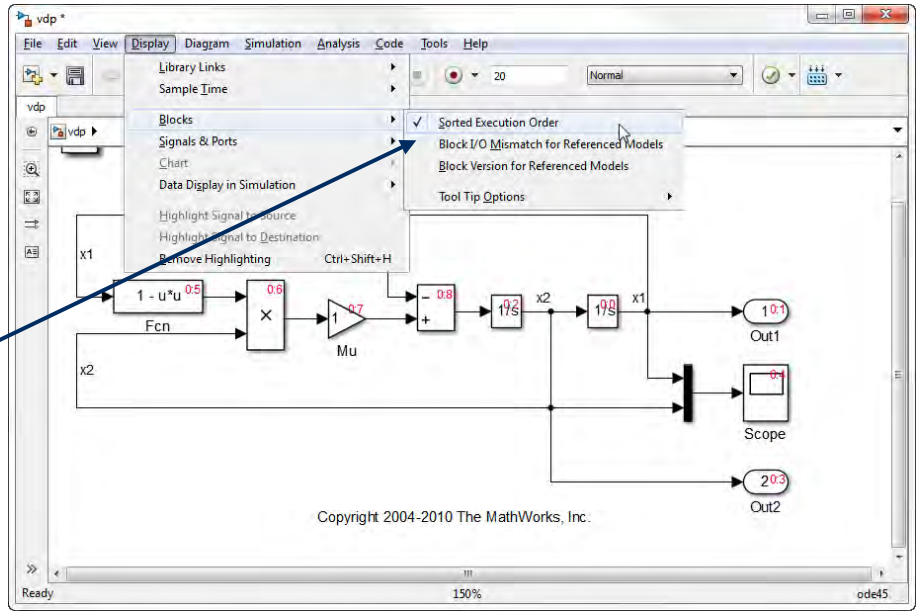
- Mapping of logical units to run-time tasks
- Define threads within processes according to execution model of run time environment (e.g. statically scheduled OS, AUTOSAR RTE, …)

- jc_0301: Controller model:
  Control models are organized using the following hierarchical structure:
  - Top layer / root level
  - Trigger layer (optional)
  - Structure layer
  - Data flow layer



MULTITASKING IN THE MODEL

- Which scheduling aspects can be handled in the model?
  - Definition of tasks / processes
  - When and how tasks will be triggered



- Priorities
  - Model priorities explicitly in Simulink
  - See misra_slsf_009_b:
    You must not enforce explicit statement of execution order of blocks.
  - misra_slsf_009_c:
    Block execution order must be specified by either data flow or function calls
  - misra_slsf_009_d:
    Explicitly state sample times in the model

MULTITASKING IN THE MODEL

- At present, SW systems generated from models are already concurrently executed.

- Which are current approaches to design and documentation of concurrency, if any?
- Which are obstacles to successful creation of concurrent tasks from a software model?
- Which mistakes shall be avoided?

- Proposals for modelling guidelines welcome

MGIGROUP – NEXT ONLINE MEETING

- **Tuesday, March 7, 2017**
  3:00 pm CET (Berlin)
  9:00 am EST (Detroit)
  7:30 pm IST (Bangalore)
  10:00 pm CST (Beijing)
  11:00 pm JST (Tokyo)

- **Link to Event:**
  https://model-engineers-event-en.webex.com/model-engineers-event-en/onstage/g.php?MTID=ee8b1c35a236a00933b6895ab5fa07a4c

MODEL ENGINEERING SOLUTIONS GMBH

Mauerstraße 79
10117 Berlin

T: +49 30 2091 6463-0
F: +49 30 2091 6463-33

info@model-engineers.com
www.model-engineers.com