Automotive SPIN Italia

Application of ISO 26262 in Practice

who we are

ikv++ technologies ag key facts

- based in Berlin, Germany and Yokohama, Japan
- 30 employees
- support solutions for automotive software development
- AUTOSAR Development Member since June 2009

activities

- automation of analysis and development processes
- functional safety analysis consultancy and solutions
- tool and process integration, process traceability
- configuration and change management solutions and consultancy

experiences

- since 2006 working mainly for carmakers in functional safety

Intecs – key facts

- medium size consultancy company
- based in Rome, Pisa, Naples, Turin, Genoa, Milan, Cagliari, Toulouse
- 350 employees
- AUTOSAR Premium Member

activities

- software development
- software verification & validation
- processes and safety consultancy (SPICE, CMMI, ISO 26262)

experiences

- founded in 1974 working at the forefront of technology in the domains:
  - defense/avionics
  - air traffic control
  - automotive
  - space
  - railway/underground

current status of introduction of ISO DIS 26262

what can we observe?

- auto makers currently define and adapt their safety processes according to the ISO DIS 26262
- happening in Europe, US and Japan
- tier-1 suppliers still seem to be waiting and watching

how do they approach it?

- intensive study of ISO DIS 26262 regarding work products and requirements
- definition of process phases in conjunction with company development process and methods
- definition of document templates
- company specific tailoring of ISO 26262

why is it such a hot topic now?

- uncertainty about legal impacts
- lawyers* stated that they treat ISO DIS 26262 as published state of the art

  * Prof. Klindt, of Nörr Steinhofer Lutz
  * Andreas Reuter, Robert Bosch GmbH

- therefore auto makers and suppliers now have to integrate ISO DIS 26262 in their processes
- some Japanese companies consider the ISO 26262 as a trade barrier

legal aspects

legal aspect was a main discussion point at EUROFORUM ISO 26262 conference in Stuttgart, September 2009

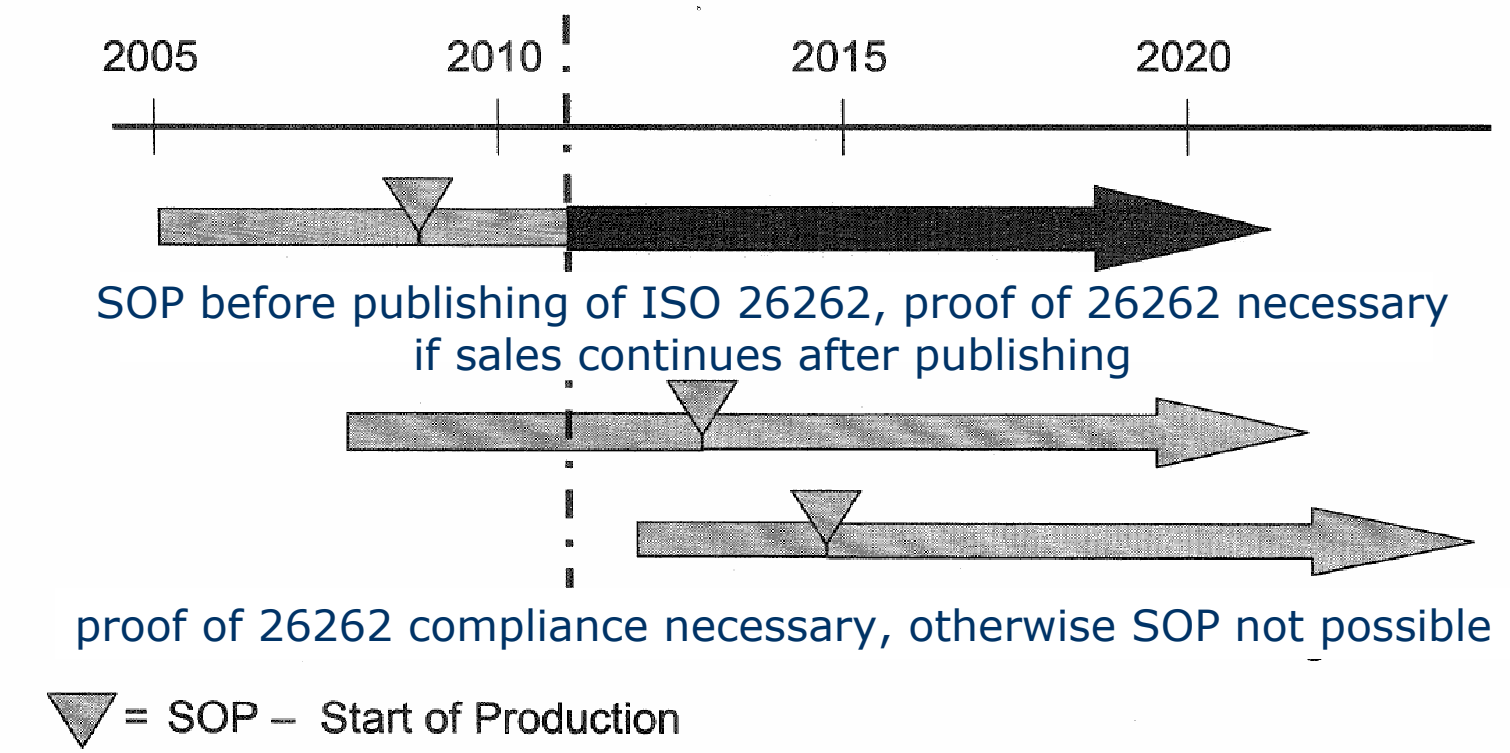
German law on product liability (§ 823 Abs. 1 BGB, § 1 ProdHaftG)

- similar in all EU countries
- car producers are generally liable for any damage to the health or death of a person caused by a malfunction of the product
- if the potential malfunction could not have been detected according to the technical state of the art at the time of placing the product on the market, the liability is excluded

→ *as ISO DIS 26262 is published, it is treated as **state of the art**,*

→ *therefore some lawyers strongly recommend that it has to be followed already now in order to exclude liability*

→ *important is the time of placing the product on the market (i.e. SOP), NOT the time of product development*



process definition

companies want to **keep their current approaches** and methods for functional safety

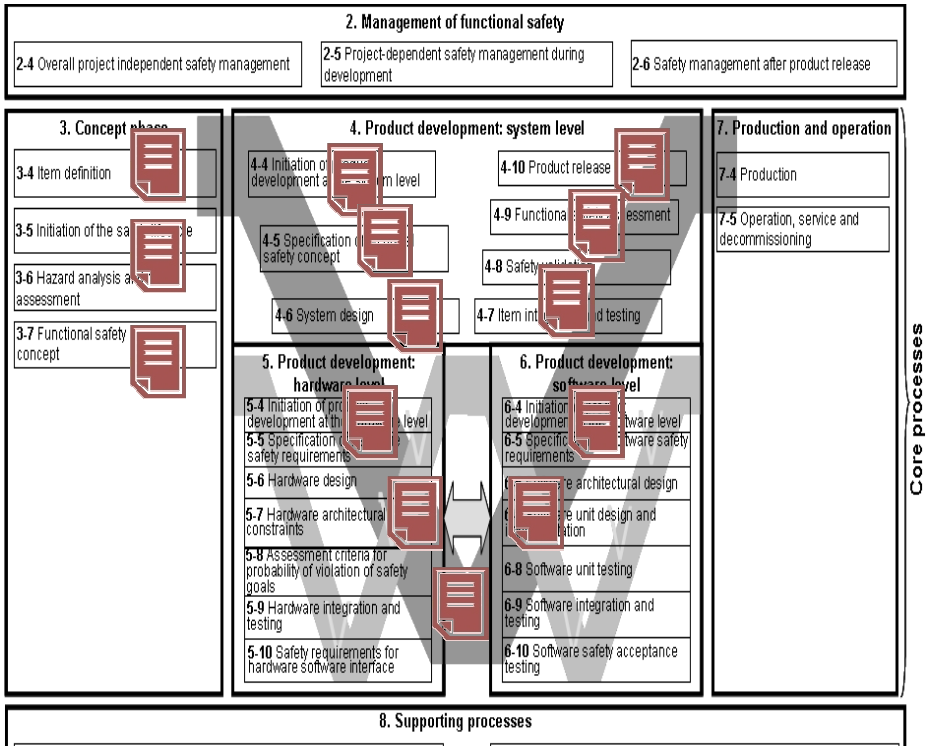
- established, assessed processes are important assets
- migrating their current processes towards ISO requirements
- they see provision of necessary documentation as key issue

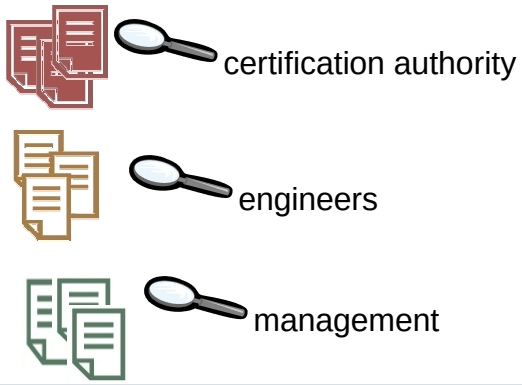
process improvements are done in a **document centric** way

- we observed already many Excel and Word templates
- one customer provided 21 different templates
- other customer adapts his .xls templates from company specific safety towards 26262 compliance

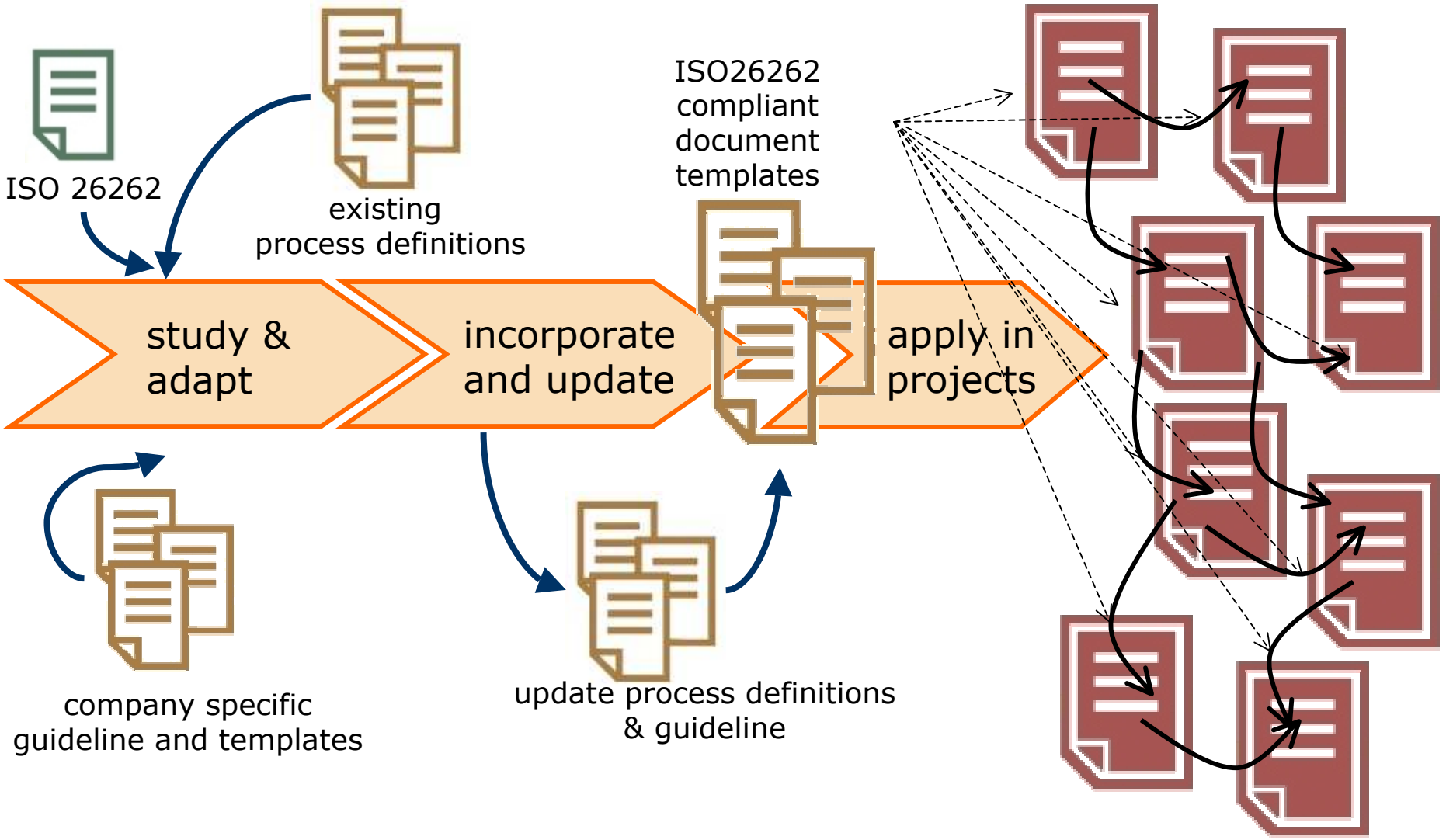
approach is similar to what we found in other domains

- INTECS experiences in railway, defense, space – also very document-centric





ISO 26262 integration in processes



problematic issues of document centric work

sources of dependent, related information are distributed over multiple documents

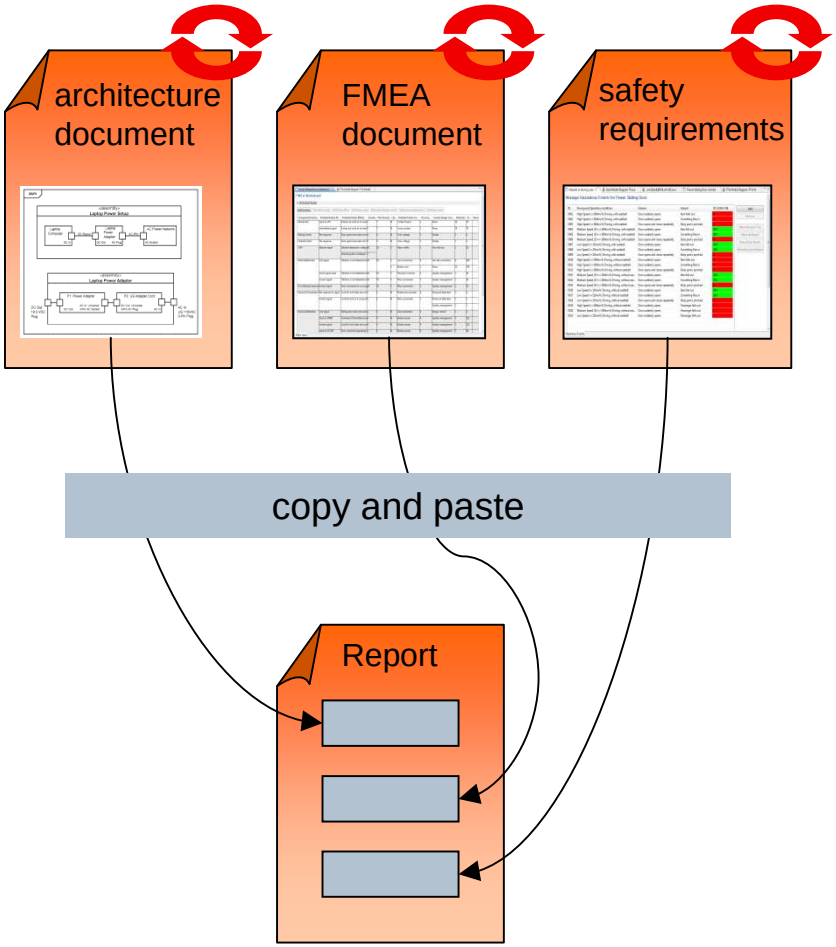
- re-use of information by copy-and-paste
- hard to manage consistency - changes in single artifacts lead to multiple updates in different documents (but how to find out which ones?)

iterative development and versioning

- changes in some documents may lead to the fact that other use of the information may become invalid
- in iterations and other change scenarios, it is not easy to determine effects

limited guidance for safety engineers

- the guidance can only be done based on documents, not by "context sensitive help"
- it's hard to identify the current state of the project by just analyzing document contents



problematic issues - traceability

traceability is a key requirement of ISO 26262

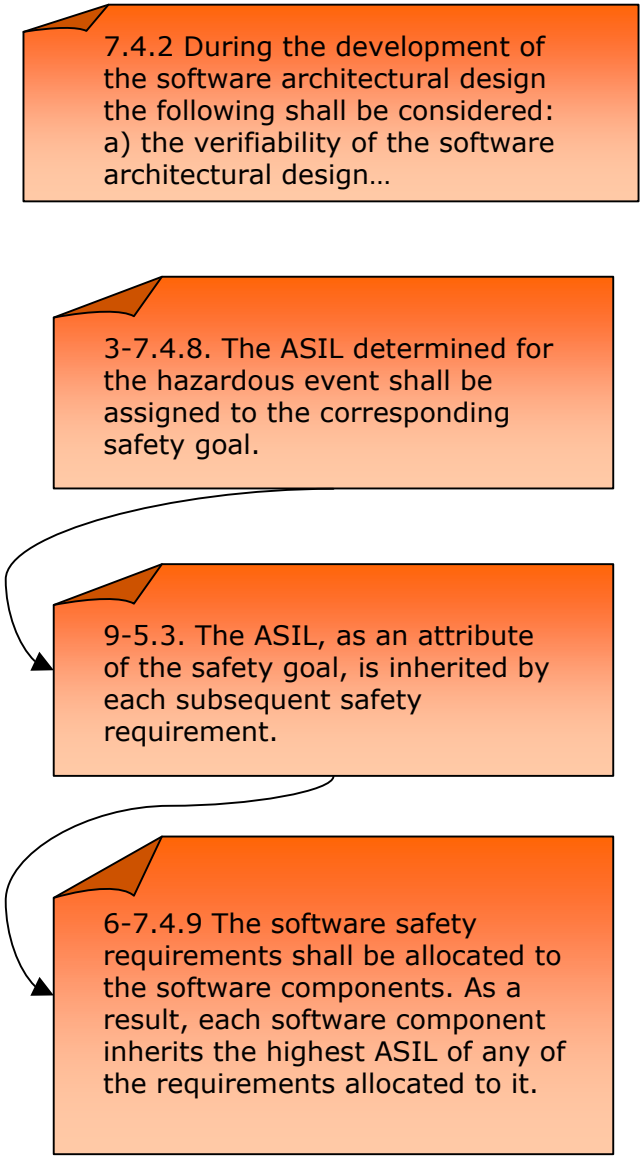
- it is necessary to show the relations between artifacts
- pre-condition for constraint checks (like ASIL "inheritance" rules)

traceability is established between documents in document-oriented approaches by cross-referencing

- artifacts are given IDs (reqID, testID, objectID, hazardID, etc.)
- in specific templates like tables, cross-references to other artifacts are made via ID's
- all traces are created manually

trace management is done manually or at most semi-automatically

- all ID's need to be continuously updated
- changes need to be incorporated in different documents



shift to a model-based approach

a model based approach offers the possibility to solve the problems

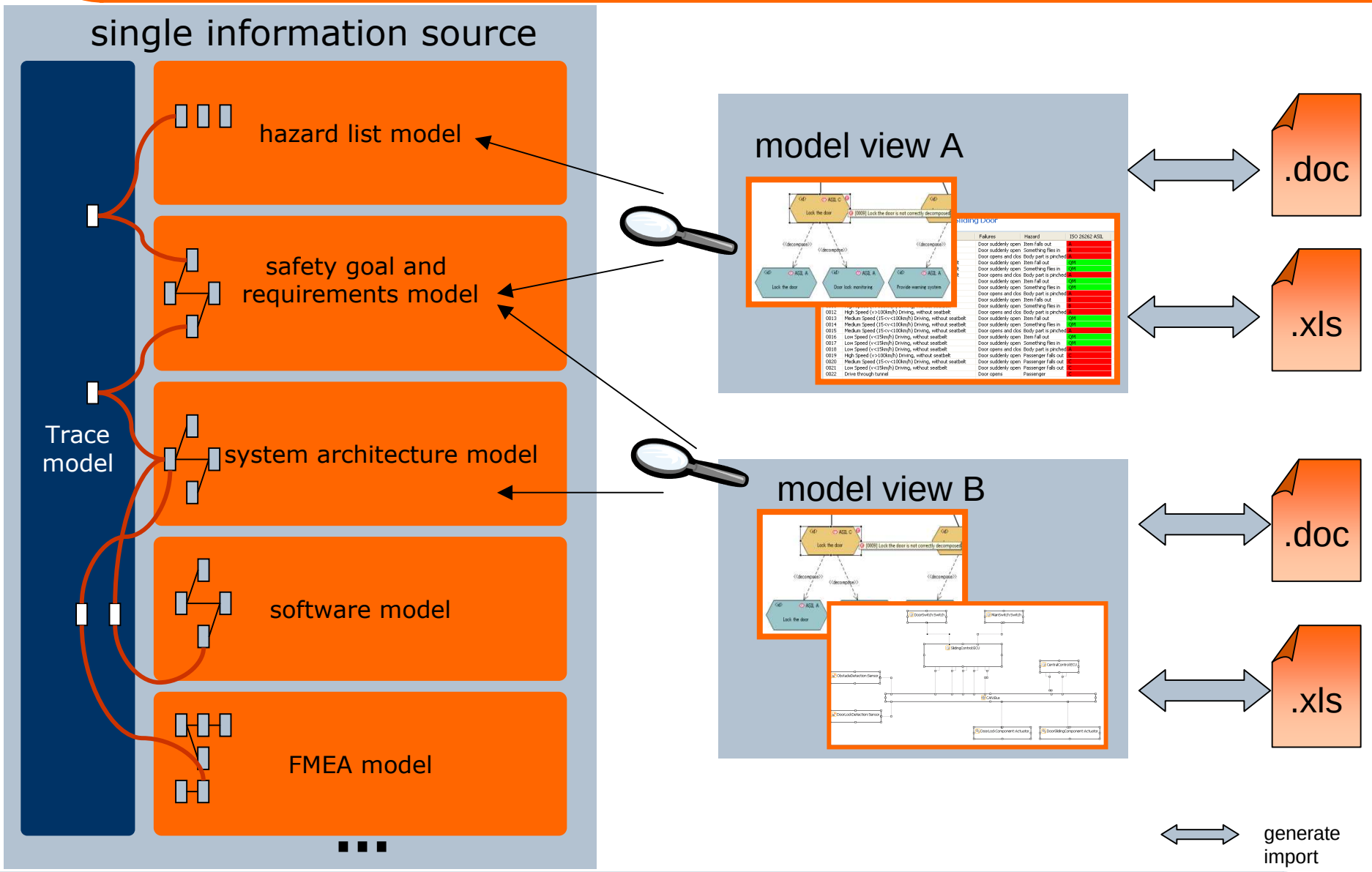
- note that ISO DIS 26262 contains many explicit provisions for the model based approach (in contrast to IEC 61508, which contains no mention) because of its growing acceptance in the automotive industry
- however, still necessary to obey the requirements of the customers for keeping their existing processes, methods, templates
  - simple proposal of replacing everything will not work

cornerstones of a model based approach

- everything is a model, even if it looks like Excel
- introduce a single information source principle
- establish fine-grained traces between model *elements*
- generate and import documents based on the defined templates

we have evaluated the model based approach vs. document centric approach with a German OEM

model-based approach overview



advantages of model-based approach

main advantages of model-centric approach to safety analysis (according to the German OEM)

- traceability maintenance support between related requirements across system decomposition levels
- consistency through referencing instead of repeating content (copy and paste)
- consistency through provision of standardized choices instead of prose text
- conservation of company know-how through acquisition and reuse of safety related artifacts (e.g. operational scenarios, safety measures, failure rates, etc.)
- semi-automated consistency checking within different system safety analyses (e.g. PHA, FTA, and FMEA)
- semi-automated consistency checking between system descriptions and system safety analysis artifacts
- semi-automated consistency checking between system safety analyses and corporate policy
- visualization support for identification of dependencies and change impact
- condition-depended process guidance for the safety engineer (workflow support)
- enable context sensitive help (process help, best practice documents, templates or reference documents)

conclusion

safety analysis according to ISO 26262 is about to be introduced

- driven by car-makers
- legal issues put strong requirements
- usually starting with document template definition

pure document-centric approach may cause problems

- consistency
- round-trip and change management
- fulfillment of traceability requirement

model-centric approach has potential to overcome problems

- well-supported by ISO 26262
- everything is a model
- single source principle
- manage traces on model level
- generate and import documents

we automate
system creation ...

ikv++ technologies ag
Dessauer Strasse 28/29
D-10963 Berlin

www.ikv.de

the brainware
company ...

Intecs SpA
Rome, Pisa, Naples,
Turin, Genoa, Milan,
Cagliari, Toulouse

www.intecs.it