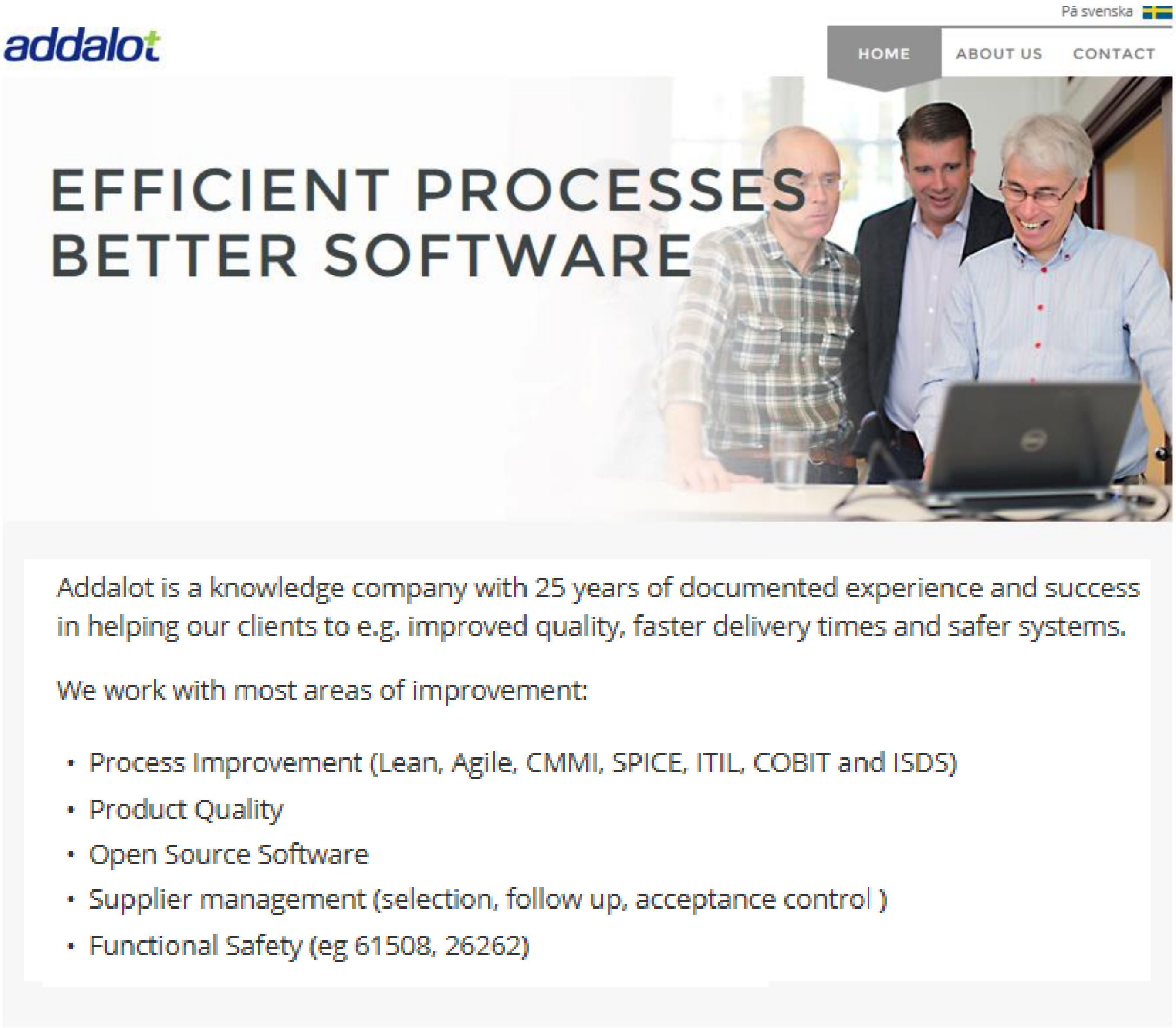
Supplier follow up related to ISO26262

Tord Wullt 2016

addalot
QUALITY IMPROVEMENT



EFFICIENT PROCESSES BETTER SOFTWARE

Addalot is a knowledge company with 25 years of documented experience and success in helping our clients to e.g. improved quality, faster delivery times and safer systems.

We work with most areas of improvement:

- Process Improvement (Lean, Agile, CMMI, SPICE, ITIL, COBIT and ISDS)
- Product Quality
- Open Source Software
- Supplier management (selection, follow up, acceptance control)
- Functional Safety (eg 61508, 26262)

Tord Wullt addalot partner

- Master of Science, applied physics LTH
  - **TUV Rheinland certified FSE Automotive ISO26262**
    - Scrum Master
- System and SW development

- **Functional safety related work**

  - **Automotive 5 yrs, Volvo Cars and Volvo trucks**

    Active safety, Power train, Certification to EU regulations

    -

  - **Offshore energy and Maritime 7yrs: Det Norske Veritas**
    - Quality and safety of controls systems
    - Offshore standard DNV OS d203

  - **Defense industry Telub, Toyota (BT), SAAB Aircrafts, Airport Technology..**
    - Automation, Functional Safety

Supplier follow up under ISO26262

Workshop purpose

- To discuss how to manage suppliers with gaps in their ISO26262 capability
- ...or how to supply projects for automotive OEM if you don´t have ISO experience

Supplier follow up under ISO26262

Weaknesses can be..

- Processes
  - Processes not in place at all, or not practiced
  - Insufficient guidelines to support efficient implementation of the standard
- Tools
  - Traceability not supported
  - Tools not qualified
  - Tools to support safety analysis missing
- Design legacy
  - No proven patterns or design from previous projects
  - Safety designs introduces a ”new” design challenge
- Competence and experience
  - Not available within the company, or on very few individuals
- Management
  - Don´t understand the efforts needed
  - This is the most important factor

Supplier follow up under ISO26262

ISO26262 capability

Does a supplier need to be experienced and mature?

- In mass production, the driving cost is production, not development
  - Added costs for developing safety capability within the project may be small in relation.
- The competition is about the best total offer
  - Procurement and project may need to manage supplier gaps in capability with respect to ISO26262
- **Low maturity can be mitigated with the right actions.**
  - Will add costs, can be substantial part of the development cost

Supplier follow up under ISO26262

Scenario to avoid with a supplier that have gaps!

- Efforts for safety work are underestimated
- A pragmatic attitude is taken to requirements in the standard as many are not understood and there is no time in the budget to consider to much.
- The focus for the time plan will be on delivery of the normal functionality as this is most visible, thus deciding the schedule.
- Education will be planned for to few people, to short trainings and to late.
- As safety competence is on very few people, the safety work and development of normal functionality will not be integrated creating inefficiency and risks.
- The safety work will have a slow start, making the safety work lag after normal development.
- It takes time to change/update tools to support safety traceability and work will be done without sufficient traceability. Often the need is understood quite late.
- The need to follow the delivery plan for normal functionality will force delivery of safety solutions without proper safety analysis, traceability, reviews for completeness etc.

addalot
QUALITY IMPROVEMENT

Supplier follow up under ISO26262

Scenario to avoid with a supplier that have gaps!

- The low integration of safety work and normal work, will create ”misunderstandings” and design/implementation decisions not in line with the standard and safety concept.
- The lack of competence will be evident and external support will be looked for, however the process of creating budget and finding someone takes long time .
- There are no resources or processes for ver/conf reviews, work will be based on drafts
- Safety assessment is seen as something performed in the end, ”when all documentation is fixed”, creating an atmosphere where ”formalities” can be dealt with later.
- As safety mechanisms are a new design element, lack of experience will create impact on reliability. As safety work is late, this will be evident very late
- The need to use simple safety solutions will impact reliability.
- At the end when the project should be finalized there will be very substantial work still to be done.

Supplier follow up under ISO26262

Actions before contract

- Assessment of the supplier capability
  - Processes, tools, people, experience
  - Safety and Quality Management
  - Understand and agree on the gaps and the actions needed to manage them
- Mitigating actions included in the contract
- When development-budget is frozen it can be hard and time consuming to add costs for e.g. training.

Assess capability and add mitigations to the contract

Gaps are OK if known and there is plan for mitigation!

Supplier follow up under ISO26262

Mitigations to agree on before contract

- Processes
  - Start process improvement
  - The standard can be followed directly with all work products etc.
    - Risk that safety is separated from the other development
  - Guidelines important

Start process improvement
Efforts and time has to be added. Detailed planning needed

Supplier follow up under ISO26262

Mitigations to agree on before contract

Tools

- Update or new tools
- Traceability and new configuration items, attributes etc.
- Document management
- Verification tools may not support fault injection.
- SW development tools. Qualification may be needed

Budget shall include efforts and planning to assure that capable support tools are available from start of the project. Plan to be shown before contract.

Supplier follow up under ISO26262

Mitigations to agree on before contract

Compliance Approach

Agree on an approach addressing compliance during the project

- It shall be agreed that strict compliance is required from start
- Each delivery shall have complete documentation and progress of safety activities and documentation shall comply to the project progress
- Agree on frequent compliance assessments and content reviews

Agree on compliance from start and an assessment schedule

Supplier follow up under ISO26262

Mitigations to agree on before contract

Competence

- Agree on having external support.
  - Can take time to find, letter of intent before contract
  - High integrity required
- Agree on a training plan
  - Can also take time to arrange, booking before contract
  - All: basic training
  - Lead engineers System, HW, SW, test and safety manager shall have extensive training and certification

Budget shall include external support and sufficient training.
Needs to be planned well ahead!

addalot
QUALITY IMPROVEMENT

Supplier follow up under ISO26262

Mitigations to agree on before contract

Design Legacy

- No carry over from previous projects
  - New design challenges to introduce safety mechanisms etc.
  - Reliability impact
- External support can help
- Plan for more time, expect late changes

Budget shall include external support
Plan for late changes due to problem with reliability

Supplier follow up under ISO26262

Mitigations to agree on before contract

Safety Assessor

- External assessor from independent organization
  - Assessor need very high integrity
- Iterative assessment, at least one pre assessment.
- It can be quite difficult to find an assessor, takes time.

Include External assessor and pre-assessment in the budget.
Letter of intent before contract.

Supplier follow up under ISO26262

Mitigations to agree on before contract

Management

- Management does not understand the effort needed
- Make an effort to make top management understand the efforts of developing safety
- Make sure that you will have frequent top management meetings during the project

Make top management understand efforts needed

Supplier follow up under ISO26262

Activities during project

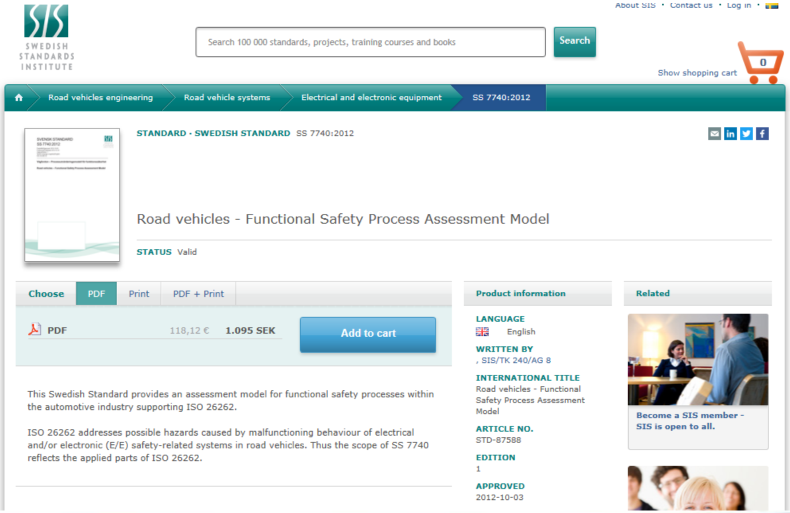
- Follow up all agreements and schedule
- Perform compliance assessments and content reviews
- Establish dialogue with top management, only way to impact budget

Supplier follow up under ISO26262

Follow up tool

- “ISO 26262 compliance matrix (Excel)”
  - Follow up of requirements in the standard
  - Action plans to mitigate insufficient compliance
  - Will drive competence and good knowledge of status

- Swedish Standard Institute, SIS SS7740
  - Standard to audit ISO26262 process compliance based on SPICE


SWEDISH STANDARDS INSTITUTE
About SIS • Contact us • Log in •
Search 100 000 standards, projects, training courses and books
Search
Show shopping cart
0
Road vehicles engineering
Road vehicle systems
Electrical and electronic equipment
SS 7740:2012
Choose
PDF
Print
PDF + Print
Add to cart
Become a SIS member - SIS is open to all.

STANDARD · SWEDISH STANDARD SS 7740:2012

Road vehicles - Functional Safety Process Assessment Model

STATUS Valid

PDF 118,12 € 1.095 SEK

This Swedish Standard provides an assessment model for functional safety processes within the automotive industry supporting ISO 26262.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of electrical and/or electronic (E/E) safety-related systems in road vehicles. Thus the scope of SS 7740 reflects the applied parts of ISO 26262.

Product information

LANGUAGE English

WRITTEN BY , SIS/TK 240/AG 8

INTERNATIONAL TITLE Road vehicles - Functional Safety Process Assessment Model

ARTICLE NO. STD-87588

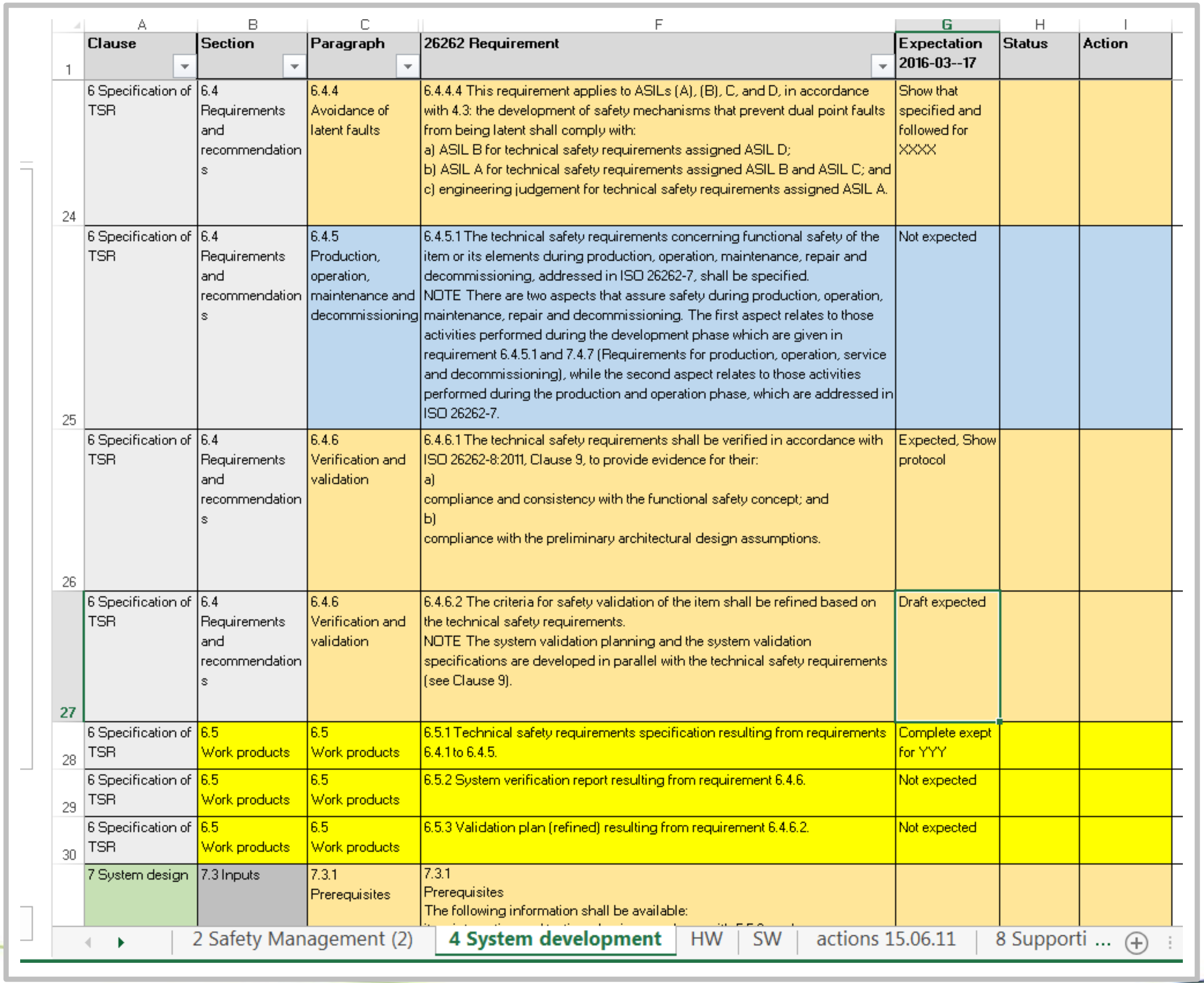
EDITION 1

APPROVED 2012-10-03

Related

Supplier follow up under ISO26262

“Compliance Matrix”



	A	B	C	F	G	H	I
1	Clause	Section	Paragraph	26262 Requirement	Expectation 2016-03--17	Status	Action
24	6 Specification of TSR	6.4 Requirements and recommendations	6.4.4 Avoidance of latent faults	6.4.4.4 This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: the development of safety mechanisms that prevent dual point faults from being latent shall comply with: a) ASIL B for technical safety requirements assigned ASIL D; b) ASIL A for technical safety requirements assigned ASIL B and ASIL C; and c) engineering judgement for technical safety requirements assigned ASIL A.	Show that specified and followed for XXXX		
25	6 Specification of TSR	6.4 Requirements and recommendations	6.4.5 Production, operation, maintenance and decommissioning	6.4.5.1 The technical safety requirements concerning functional safety of the item or its elements during production, operation, maintenance, repair and decommissioning, addressed in ISO 26262-7, shall be specified. NOTE There are two aspects that assure safety during production, operation, maintenance, repair and decommissioning. The first aspect relates to those activities performed during the development phase which are given in requirement 6.4.5.1 and 7.4.7 (Requirements for production, operation, service and decommissioning), while the second aspect relates to those activities performed during the production and operation phase, which are addressed in ISO 26262-7.	Not expected		
26	6 Specification of TSR	6.4 Requirements and recommendations	6.4.6 Verification and validation	6.4.6.1 The technical safety requirements shall be verified in accordance with ISO 26262-8:2011, Clause 9, to provide evidence for their: a) compliance and consistency with the functional safety concept; and b) compliance with the preliminary architectural design assumptions.	Expected, Show protocol		
27	6 Specification of TSR	6.4 Requirements and recommendations	6.4.6 Verification and validation	6.4.6.2 The criteria for safety validation of the item shall be refined based on the technical safety requirements. NOTE The system validation planning and the system validation specifications are developed in parallel with the technical safety requirements (see Clause 9).	Draft expected		
28	6 Specification of TSR	6.5 Work products	6.5 Work products	6.5.1 Technical safety requirements specification resulting from requirements 6.4.1 to 6.4.5.	Complete exept for YYY		
29	6 Specification of TSR	6.5 Work products	6.5 Work products	6.5.2 System verification report resulting from requirement 6.4.6.	Not expected		
30	6 Specification of TSR	6.5 Work products	6.5 Work products	6.5.3 Validation plan (refined) resulting from requirement 6.4.6.2.	Not expected		
	7 System design	7.3 Inputs	7.3.1 Prerequisites	7.3.1 Prerequisites The following information shall be available:			

addalot QUALITY IMPROVEMENT

Supplier follow up under ISO26262

Something to add?
Other experiences?