10 recommendations for successful implementation of ISO 26262 and Automotive SPICE

Summary

The Safety Standard ISO 26262 and the Process Maturity Standard Automotive SPICE (ASPICE) are both extensive standards that cover large parts of the system and software development organization. Implementing both these standards can provide significant advantages, but also poses significant challenges. In this whitepaper Addalot offers advice on how to combine and implement these standards.

ISO 26262 and ASPICE

This paper is intended for organizations facing the challenge of simultaneously implementation the safety standard ISO 26262 and the general process maturity standard Automotive SPICE (ASPICE). Even if we focus here on ISO 26262 and ASPICE, most of the content is also applicable for other safety standards (e.g. ISO 61508) and maturity standards (e.g. CMM-I).

Typical situations where this paper can be useful are:

- As a supplier you have a new contract with customer requirements on compliance with ISO 26262 and ASPICE. You have not worked in depth with these standards before.
- You are an OEM using ASPICE, and are about to introduce 26262.

The recommendations focus on reducing the risk for diverging, inefficient or overly complex processes with increased cost. This risk can be the consequence if we are not careful when implementing these standards.

This paper describes an implementation strategy for a specific product/project where you have market requirements to comply with these standards. The recommendations can also be used for gradual implementation of the standards over several products with some adaptation.

The implementation of the two standards is not a simple task, it requires commitment, planning and effort from the whole organization. As with most organizational changes, the updating of the process documentation is just a small fraction of the total effort.

The 10 recommendations do not address the importance of product architecture for safety, i.e. the ability to properly isolate safety critical functions, and providing an architecture where safety mechanisms can be efficiently and effectively implemented which is key to a safe and cost efficient system. The architectural aspects are something that we assume that all organizations have high on their agenda with or without these standards.

*First published in 2011 the **ISO 26262** standard is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.*

*In 2005 the industry-specific standard **Automotive SPICE®**, derived from the new ISO 15504 International Standard (IS) for software process assessments, was published by the Special Interest Group Automotive.*

Why is implementation not that simple? The main reason is that the standards are not synchronized. They partly overlap, and they also use different terminologies and different general view of the system and software development processes. Along with adapting to the organizations own development process, this makes interpretation and implementation complex.

Awareness

All involved parties need to have good understanding of both standards. People must understand that these are standards that need to be adapted to both products and organization.

1. Demystify the standard as much as possible. Ensure that people have read the parts of the standard that are relevant for them, and arrange for them to present their interpretation of that particular part.
2. Discuss examples of why the different techniques are there, and discuss their relevance for your products, project and organization.
3. If everyone can understand that these are mainly just good engineering practices it is much simpler to implement them.
4. Clearly understand the differences in scope between ISO 26262 and ASPICE.
    a. ISO 26262 is "life critical" – ASPICE is about project cost, time and general quality.
    b. ISO 26262 also covers lifecycle activities taking place later in the process.
    c. ISO 26262 is more technical.
    d. ASPICE is more detailed regarding organizational processes.
    e. ASPICE covers more management practices.
    f. ISO 26262's hazard analysis is a special form of requirements elicitation leading to functional safety requirements, i.e. new product requirements, with a focus that these are correct and complete. ASPICE requirements elicitation is generic.
    g. ASPICE is a "maturity" standard where activities depend on capability level, ISO 26262 is a "mandatory" standard depending on ASIL level.
    h. ISO 26262 is a standard only addressing the safety product quality attribute, ASPICE addresses the capability/maturity of the organization and its projects.

Hint: Let people pick out the 3 most "difficult" parts of each standard and discuss them

ASPICE requirements and benefits increase with maturity, 26262 requirements and safety increase with ASIL level

Existing way of work as a basis

Implementation should be based on your current processes to which necessary activities are added or improved.

1. Do not assign separate ISO 26262 and ASPICE implementation responsibility to different people; base the implementation on the existing process management structure, e.g. improvement drivers, line responsibility etc.
2. Make a concrete list of changes/improvements that shall be implemented including responsible roles, effort and consequences.
3. Follow up progress of implementation as clearly and visibly as possible, e.g. training (people trained, effectiveness of training), effort planned and used, efficiency rating.
4. Have a light weight improvement project at the organizational level that follows up activities across target projects, but focus the majority of the activities on supporting the target projects.

ISO 26262 and ASPICE are improvements and extensions to your own process

Focus on the projects

Focus more on project activities and plans and less on organizational processes, but ensure that results can be reused by other projects. This item is especially applicable for a gradual implementation

1. Focus on the actual project that shall deliver a product with ASPICE or ISO 26262 requirements – they need to comply with these requirements.
2. Ensure that competence build up is planned and synchronized with the other project activities.
3. Ensure time and resources are available to support, implement and evaluate the necessary changes that are planned for the project.
4. Good practices are best transferred through people. Ensure that the buildup of competence and transfer of knowledge from the project is planned and performed.
5. Provide regular insight into the projects for the whole organization so that others can learn as those involved learn. Provide overview presentations about the whole project, or more in depth presentations about specific techniques.

Effort increase with ASIL level. Numbers reported are
ASIL A 15 - 25 %
ASIL B 20 - 40 %
ASIL C 30 – 60 %
ASIL D 50 – 100 %

Safety culture

Focus on a Safety culture – it will also lift the general quality culture

1. Update the goals and incentives in the organization so they support safety, or at least are not working against safety.
2. An important part of the safety culture is to establish a general value in the organization that safety is taken seriously. Ensure

that everyone understand that the company is dealing with systems with risk for personal injury and possibly death.
3. Ensure that all relevant parts of the organization are informed, involved and responsible.
4. Even if there is a safety manager, safety must be everyone's concern.
5. Discuss the impact of safety for each role, and follow up so that all roles can handle the responsibilities.
6. On regular basis evaluate the progress and effectiveness of your safety work and general safety culture.
7. Consider using a safety culture questionnaire to probe the organizations awareness and adherence to safety.
8. Discuss any deviations or problems related to safety work, e.g. conflicts of time/cost/functionality and safety, difficulties in applying specific safety methods or doubts about the methods effectiveness.

Pro-active use of Quality Assurance

Take advantage of quality assurance (QA) role and involve the assessor/certifier early

1. Use the QA role to support work with both ASPICE and ISO 26262.
2. Involve QA in planning and implementation of the changes.
3. Ensure that QA is knowledgeable about the specific practices so the role can provide concrete support to the project.
4. Synchronize and if possible integrate the necessary compliance activities with the normal QA work.
5. Use the QA role to help extract good practices and spread knowledge about the target project to the rest of the organization.
6. Involve the assessor/certifier early, by presenting plans, selection of methods, intermediate results etc., and get feedback during the work.
7. Let the assessor select which intermediate activities and documents to follow, and do not focus only on the final documents.

For further reading about proactive Quality Assurance read our QA whitepaper

Management of legacy

Analyze what to do with legacy artefacts, e.g. code, tools, models, and hardware. Develop a legacy strategy – bringing legacy artefacts up to the necessary ASIL level is probably the most difficult task when introducing

safety into an existing system. Use necessary time and effort to understand your options.

1. If possible identify and classify the legacy into different safety risk levels as input to the strategy.
2. To select which safety design and test practices to apply, classify them in terms of impact and effort.
3. Use ASIL decomposition to manage legacy code.
4. Test different alternatives on smaller pieces of the code, e.g. lift part of the code to the necessary ASIL level by doing the necessary design and test activities or isolate legacy code through the operating system. Use this experience and-effort estimates as input to the strategy – sometimes it is not as difficult as one might think.
5. As for all safety activities clearly document the analysis and rational for the decision. This is even more important in areas for which you must rely on your own interpretation of the standard, or where you feel that the standard is unclear.

Why is handling of legacy complex?

- *Legacy code tends to be comprehensive, monolithic and unstructured.*
- *The requirements and design are often not properly documented.*
- *Often there is a lack of traceability.*
- *Tests are not carried out according to safety standard*
- *Hazard analysis is not done*
- *Complete verification is likely needed after system changes.*

Management of suppliers

Work proactively with suppliers. Suppliers with limited experience in using these standards can be greatly helped by a pro-active OEM, which results in a win-win situation.

1. Suppliers need to be involved early.
2. Clearly state expectations in the supplier contract. This is covered to a large extent by 26262.
3. Together with the supplier assess the gaps in the supplier's processes.
4. Ensure that suppliers get all necessary information about what you have planned, and what you expect from them.
5. Plan if and how they can be involved in the competence development activities that you are doing.
6. Assign dedicated persons to follow up the activities in the standards with suppliers.
7. Perform safety audits and assessment of the supplier and evaluate the result together with the supplier. Use the result from the audit and assessment as benchmarking of your own process and methods.

Expectations cover more than functional requirements, cost and delivery time. ASPICE and 26262 requirements need to be clearly stated

Key supplier roles:
QA and Safety Manager

Planning of changes

Based on our experience we recommend analyzing and planning these changes in four steps or building blocks. The last two building blocks are optional, but can lead to a better implementation.

1. Ensure that basic ASPICE management practices are in place to handle requirements, estimates, plans, tracking, configuration management and quality assurance. This will give a solid foundation for proper planning, execution and follow up of projects. Remember: "You can't build anything on sand".
2. Focus on required safety related activities from ISO 26262 based on ASIL level. These activities are mandatory to meet the certification requirements.
3. Check whether any of the ISO 26262 practices shall be extended beyond safety to meet other business goals. These could be additional unit testing methods, or using formal models independent of ASIL level. The ISO 26262 activities will generally improve the quality of the product.
4. Select synergetic and complementary ASPICE practices focusing on other business goals or OEM ASPICE requirements. These may be practices related to reuse. The complementary ASPICE activities can provide improvement in predictability, lead time and cost.

ISO 26262 practices generally improve product quality

The complementary ASPICE activities can provide improvement in predictability, lead time and cost

Training and support

Provide good training and support for the safety methods

1. The safety methods are concrete and will give tangible results. It is easy to check that the organization is doing what is required and that it is changing its behavior.
2. Proficiency in the methods is important for their effective use.
3. Focusing on these methods will probably not only lead to better safety, but also to better design and overall quality – evaluate whether this is the case.
4. Establish a good understanding of the effort needed for each of the methods, who needs to be involved, and the results.
5. Ensure that appropriate support and follow up are provided when everyone starts to use the safety methods.
6. Perform product safety audits and process assessment to check the efficiency and correctness of performed methods
7. Standardize and improve methods continuously, based on feedback from practitioners and projects.

Consider different training techniques, self-study, webinar, courses, mentoring

Organizational change management

Take change management seriously. There is some overlap between the recommendations here and previous sections, but they deserve to be repeated:

1. As with all changes success requires management commitment and clear project goals.
2. Ensure that everyone understands what is in it for them, and that they know why they need to do this.
3. Ensure success by planning concrete activities that are clearly connected to target projects.
4. Provide adequate resources and competence for on-site practical support to target projects, e.g. how to carry out and document safety activities.
5. Allocate enough time, and follow up that it is really used.
6. Visualize progress clearly, in e.g. wall charts with status for different activities, best practice stories.
7. Be aware that there are three steps to implementing a new practice: training, first time use and continuous use. The effort required for first time use is greater than in continuous use.
8. Distinguish differences. Safety is more concrete than ASPICE, i.e. there are concrete new activities that shall be done, and everyone can understand that your organization can't deliver a system where only 95% of the identified necessary safety activities are completed. ASPICE is more "general" improvement of existing practices, and you can "pass" without 100% compliance. Note that for both standards identifying the necessary level for many activities is not trivial, and subject to professional judgment.
9. Understanding that deployment of a new process is more than definition. It is not enough to document a new standard process, and assume that the projects will use it. It is generally much better to define the process through a plan together with the target project and then abstract it later to a generic process.
10. Focus on results in the projects, e.g. documents and plans, and then abstract the templates and processes from there.

Change management is difficult, 2/3 of all improvements fail or do not meet their objectives

Summary

These 10 recommendations address the challenge of successful implementation. Within your organization and operational context you will most likely encounter additional challenges, but we hope that these 10 recommendations can serve as a basis for developing your implementation strategies.

References:
ISO 26262,
http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1499

Automotive SPICE,
http://www.automotivespice.com/

About Addalot

Background

Addalot Consulting has over 25 years' experience of system and software process improvement. The company started in 1989 as Q-Labs, a spin-off from Ericsson, and became in Europa the leading provider for services related to improvement of software companies. Q-Labs was bought in 2006 by DNV and then in 2011 transferred to the newly established company Addalot Consulting.

Addalot helps organizations to improve results and reduce risks by improving their way to develop and maintain software.

Philosophy

Our core belief is that the process, current way of working, strongly impacts the quality and lead time of the products developed. Many companies focus on the result and desire improvements (faster, cheaper, better) without thinking of what abilities that needs to be addressed in order to make this happen.

Efficient processes give better software

Addalot's services

Process Improvement - better, faster and more reliable processes
Product Quality- Quality of requirements, design, code and verification
Software safety – Management of safety critical software

Clients

Addalot helps large and small companies in several domains: ABB, AkerSolutions, Atlas Copco Autoliv, BAE Systems, BMW, BorgWarner, Bosch, DNV, EADS, Emric, Ericsson, GM, FMC, FMV, Hoerbiger, Ikea, Ikano, Kockums, Kongsberg, Lawson, Mecel, Nokia, Nucletron, Nordstedt Juridik, Qliktech, Palette, Point, Readsoft, Saab, Sony, ST-Ericsson, SEB, Statoil, Stoneridge, Telia, Telenor, Terma, Thales, Tieto, UIQ, Visma, Visteon, Volvo.

Contact

We are today active in Göteborg, Malmö och Stockholm, with main office at Gråbrödersgatan in Malmö.

Addalot Consulting AB
Gråbrödersgatan 8
211 21 Malmö
www.addalot.se
040-972400