Guide to the approval of systems with software on the railways

Version 2 of 22 March 2016
Foreword

1. General

Software (SW) is an important building block in railway subsystems. The safety functions of the subsystems are based largely on SW, and the subsystems often have complicated interfaces in themselves and with other subsystems, as is the case, for example, between fixed and mobile train control. SW therefore plays an important role in railway safety.

Whether we are talking about new SW that needs to be developed from scratch, or existing SW that needs to be changed, it is important to follow appropriate processes. This guide refers to standards EN50128:2011 and ISO/IEC 90003:2015, which describe just such recognised and appropriate processes. Other processes might be used to the extent that this is compatible with applicable legislation.

The SW development, change and approval process can be fairly complicated, and involve many different roles and competences, for example:

- The project management
- The SW designer
- The verifier, cf. EN50128
- The validator, cf. EN50128
- A notified body (NoBo)
- An independent assessor, cf. EN50128 (ASR)
- An independent assessor, cf. CSM RA (AsBo)
- An infrastructure manager or railway undertaking

This guide is primarily intended for use by railway undertakings and infrastructure managers, which, through their safety management system (SMS), must ensure that new subsystems are not commissioned without an authorisation for placing in service, and that subsequent changes are properly handled in accordance with the applicable legislation.

The guide supports the orders on authorisation for placing into service for subsystems in the infrastructure and the approval of vehicles with accompanying guides, and concerns both SW that implements safety requirements and SW that only implements requirements in TSIs or NNTRs, which are not necessarily safety-related. Other processes than those specified in EN50128 and ISO/IEC 90003 can be relevant for SW that was developed many years ago. The guide can also be used in connection with changes to such systems. See more about this in chapter 15 and the example in annex 2.

Hardware (HW) and SW changes can be equally critical, and it can complicate risk management if changes are made in both at the same time. This guide focuses purely on SW changes. The guide cannot therefore stand alone, but must be used in conjunction with the other guides of the Danish Transport and Construction Agency.

Software that is only concerned with ‘security’ is not dealt with in this guide. If ‘security’ software is included in other safety-related software, the guide can be used.

2. Purpose

The purpose is to provide guidance on how railway undertakings, infrastructure managers and their suppliers are expected to involve themselves in SW development and changes thereto, as

---

1 Corresponding standards could also be used, including the previous version of EN50128. However, as far as possible it is recommended that the latest standards are followed, as these are regarded as ‘best practice’. See chapter 15 regarding the management of systems with SW that were not developed in accordance with a recognised practice.

2 NNTR stands for ‘Notified National Technical Rule’.

3 Security SW means SW that protects against unauthorised persons with malicious intent gaining access to make changes to software that concerns railway safety.
well as to provide guidance on how it is being investigated whether the Danish Transport and Construction Agency should be involved in the approval process.

3. **Change history**

<table>
<thead>
<tr>
<th>Version</th>
<th>Section</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary draft, of 23 October 2015</td>
<td>All</td>
<td>Distributed to the Industry Panel for Railways</td>
</tr>
<tr>
<td>Version 1 of 28/02/2016</td>
<td>All</td>
<td>Updated based on reviews and comments received from the Industry Panel</td>
</tr>
<tr>
<td>Version 2 of 22/03/2016</td>
<td>Annex 3</td>
<td>System drawing resolution improved.</td>
</tr>
</tbody>
</table>

Note: The Danish Transport and Construction Agency wishes to gain experience with the guide. Comments may be submitted to: info@tbst.dk

4. **How to read the guide**

The chapters are best read in numerical order, as several concepts are introduced on a continuous basis.

Abbreviations are explained in chapter 5.

References can be found in chapter 6. The following syntax is used for pointers to references; /x/, where x is the reference in question.

Chapter 7 introduces the concept of 'the CSM system', and in the figures in the guide the CSM system's interface is always shown with a bold blue line.
Introduction

Software (SW) is physically intangible, since within the physical, operational system, SW is a file containing the generated program code and data, which only a computer can read and interpret.

SW is defined in standard EN50128 as: 'Intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system'.

In other words, software is always something that is part of a physical system and participates in the system’s functions. This is illustrated in Figure 1:

Figure 1 SW is part of the system

When a subsystem in the overall railway system is changed, this may entail the subsystem having to be re-certified by NoBo/DeBo or a vehicle expert, and at the same time the CSM RA regulation must be applied, whereby it must first be examined whether the change is significant.

The criteria for determining significance in the CSM RA regulation are typically directed towards the physical system and its integration into the railway system. By applying the CSM RA process it is possible to identify the CSM safety requirements (including SIL requirements) to be implemented by the safety functions. However, the CSM RA does not lend itself to controlling which unintentional consequences an SW change can have. Therefore it is necessary to use a recognised practice (e.g. EN50128) to ensure that the software is developed such that the safety requirements are met.

This guide therefore aims to describe the above framework conditions, and how it can be assessed whether a change in a system with SW:

- is significant, cf. CSM RA and/or
- must be certified by NoBo/DeBo/vehicle expert,

as well as when the Danish Transport and Construction Agency should be involved.

*Procedures, rules and documentation means procedures, rules and documentation relating to software development and implementation. Data used by the computer are considered 'SW.'
## 5. Definitions and abbreviations in the guide

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
</table>
| AsBo         | Assessment body, cf. CSM RA /3/.
| ASR          | Assessor, cf. EN50128 /5/.
| ASSR         | Assessor, cf. EN50129 /6/.
| BEKxxx       | Order No xxx.
| BUS          | A BUS (the word is related to the Latin 'omnibus', meaning 'for all') is the communication system that transmits data in a computer, or between several computers. |
| Computer     | The hardware (HW), which consists, for example, of the components CPU, IO, Rack, BUS and the Memory, which contains the program code, data, etc. |
| Configuration Manager | The person at the SW supplier with responsibility for Software Configuration Management pursuant to EN50128. '3.1.5, configuration manager: entity that is responsible for implementing and carrying out the processes for the configuration management of documents, software and related tools including change management'. Configuration Management is an administrative activity. |
| CPU          | Central Processing Unit. This may also be known as a central unit or simply a processor. |
| CSM safety requirements | Requirements placed on the CSM system, established through CSM RA. |
| CSM system   | A functional unit in the subsystem consisting of HW and SW with one or more specific SW functions located either in a vehicle or in the infrastructure. |
| DeBo         | Designated body. |
| Subsystem    | The result of the railway system's division into structural and functional subsystems, as specified in IOD annex II. |
| ECM          | Entity in Charge of Maintenance. |
| Proposer     | Cf. CSM RA Article 3, 11) the proposer can be one of the following: |
|              | a) a railway undertaking or an infrastructure manager which implements risk control measures in accordance with Article 4 of Directive 2004/49/EC |
|              | b) an entity in charge of maintenance which implements measures in accordance with Article 14a(3) of Directive |

CSM RA, Article 3: 'safety requirements' means the safety characteristics (qualitative or quantitative or, where necessary, both qualitative and quantitative) for the construction, operation (including operational rules) and maintenance of a system necessary in order to meet legal or company safety targets.
2004/49/EC

c) a contracting entity or a manufacturer which invites a notified body to apply the 'EC' verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or a designated body according to Article 17(3) of that Directive

d) an applicant for an authorisation for the placing in service of structural subsystems.

HW  Hardware is a general term for the mechanical and electronic components that go to make up a system.

IO  Input/Output.

IOD  The Interoperability Directive. /8/.

IM  Infrastructure manager.

Configuration Authority  The function in the railway undertaking or infrastructure manager who is responsible for implementing and enforcing configuration management processes for the HW/SW used operationally, in compliance with the undertaking's safety management system. Configuration management is an administrative activity.

Module  In software, a module is a defined part of the software corresponding to 'Software components' in EN50128. The term 'module' is also used as a verification procedure, cf. /12/.

NNTR  Notified National Technical Rule.

NoBo  Notified body.

PIS  Passenger information system.

Program / Program code  That part of the SW found in the computer.

QMS  Quality management system of the manufacturer.

Safety function  Defined in EN50128: 'A function that implements a part or whole of a safety requirement.' A safety function can depend on SW, HW, procedures and human intervention. Safety functions can be internal to the CSM system, or act across the CSM system's interfaces.

RU  Railway undertaking.

SIL  Safety Integrity Level. EN50126: 'One of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems'. The SIL (0-4) is an expression of the confidence one can have in a safety function working as intended at system level. For a function with SIL = 0 one cannot have any great confidence that it will work as intended, while one may be very confident that a function with SIL = 4 will work correctly. Safety functions are typically implemented with contributions from both HW and SW.

Software safety integrity level (SSIL)  'Classification number which determines the techniques and measures that have to be applied to software'. See also SIL.

That part of the system's Safety Integrity Level assigned to SW. The SSIL is often the same as the SIL, but the two are kept separate in the guide.
SMS  Safety management system of the railway undertaking/infrastructure manager.

SAR  Safety assessment report.

SW  Software: ‘An intellectual creation comprising the programs, procedures, rules and any associated documentation pertaining to the operation of a system’.

SW safety function  This refers to the software’s contribution to the overall safety function, which may include mechanical/electrotechnical components, etc..

SW requirement specification  Defined in EN50128, 7.2.4.2: The Software Requirements Specification shall express the required properties of the software being developed. These properties, which are all (except safety) defined in ISO/IEC 9126 series, shall include:

- a) Functionality (including capacity and response time performance),
- b) Robustness and maintainability,
- c) Safety (including safety functions and their associated software safety integrity levels),
- d) Efficiency,
- e) Usability,
- f) Portability.

System  General term for anything that can be defined as being part of ‘the system’. It can cover many things depending on the context.

TSI  Technical Specification for Interoperability.

Validator  Unit responsible for validation.

Verifier  Unit responsible for one or more verification activities.
6. References

/1/ BEK653 Order No 653 of 8 May 2015 on the approval of vehicles in the rail sector, amended by Order No 859 of 07/072015 amending the order on the approval of vehicles in the rail sector.

/2/ BEK661 Order No 661 of 8 May 2015 on the placing into service of subsystems in the railway infrastructure, amended by Order No 864 of 07/072015 amending the order on the placing into service of subsystems in the railway infrastructure.


/11/ IOD implementing order Order No 1281 of 19 November 2015 on the interoperability of the rail system.

Managing software

7. Introduction

As described in the introduction, SW is executed in a computer, which forms part of the functional unit, which is referred to in this guide as ‘the CSM system’. This is part of a larger system coherence in the overall subsystem in the railway.

The system containing SW is known as the CSM system because it is a unit that processes functions through SW and should therefore be managed in accordance with the guide. This can be illustrated by the following example for a railway vehicle, where the CSM system is a door control system. Here the CSM system is the entire functional unit comprising doors, locking mechanisms, trap protection, monitoring, manoeuvring, the computer, etc.:

**Figure 2 System breakdown**

The computer is the part of the CSM system containing the software's program code. The program code can be found in the computer's memory. In this context, HW and SW must be seen as equally critical, whether changes are made to SW or HW, but this guide is primarily aimed at changes to SW.

The contents of the system definition for the CSM system including the computer are detailed in chapter 10.

Once the CSM system is defined, this guide suggests that the following should be assessed in connection with a change:

1) Whether the SW change is a significant change to the CSM system (Chapter 13)
2) Whether the SW change in the computer is ‘critical’. The result of this assessment will be that the change is either ‘major’ or ‘minor’ (Annex 1)
3) Whether the change affects already issued verification certificates and/or can be considered as a renewal/upgrading (Chapter 11)

---

5 Verification certificates issued by a NoBo, DeBo, or a vehicle expert.
The relationship between standards, CSM RA and concepts

If the change is considered significant or is covered by a TSI/NNTR specifying that CSM RA should be used, this means the proposer should follow CSM RA. For a position on significance, refer to chapter 13 of this guide. When CSM RA is followed, and SW also has to be developed/changed, the processes for this can be illustrated as shown in Figure 3 below:

Figure 3 CSM RA and EN50128 processes

Figure 3 illustrates that the program is run in the computer (red box), which is part of the system function for the CSM system (blue box), which in turn is part of the overall subsystem (black dashes).

The computer (incl. program) is part of the CSM system, which in turn is part of the subsystem.

According to DV 29bis, CSM RA can be used for the safe integration of subsystems and between elements in subsystems, including safe integration with the infrastructure (yellow arrows). Chapter 10 describes how the system definition for this can be created.

CSM RA can thus be used to risk-manage all hazards related to the interfaces and safe integration.

The EN50128 standard is a recognised method that can be used to control the hazards associated with SW development, and thereby help make SW safe to use. EN50128 is based on the assumption that safety requirements have been drawn up at system level, hereafter referred to as 'CSM safety requirements'.

The CSM safety requirements are established by applying CSM RA. The system architecture and apportionment of safety requirements are determined simultaneously in the iterative CSM process.

6 EN50126 is also frequently followed.
The following Figure 4 illustrates the relationship between CSM safety requirements, safety functions and SW functions.

**Figure 4 Software's contribution to the overall safety function.**

When the CSM safety requirements (incl. SIL) and the system architecture have been determined, it can then be decided what requirements to place on the software.

The safety requirements for the software can be roughly divided into two parts:

1. A requirement for SW safety integrity (SSIL).
2. A requirement for SW safety functions, where the manufacturer has specified which safety functions the SW must process.

Re 1: The determination of the SSIL is based on the SIL of the safety function. Depending on the system architecture used, and on whether several standalone computers / programs are used to process safety functions in the SW, the SSIL can in some cases be lower than the SIL. Recognised methods for this can be found in, among others, EN50129 /6/.
The Life Cycle Model

The more detailed method for establishing the requirements for software can be found in EN50128, which is essentially built on the so-called 'Life Cycle Model'. The model shown in Figure 5 is an example of such a Life Cycle Model, where the step between determining the CSM safety requirements and the 'Software Requirements Phase' is of particular interest. It is here that the SW supplier's work begins.

**Figure 5 'Section of Life Cycle Model' for SW (ref. figure 3 in EN50128)**

<table>
<thead>
<tr>
<th>DESIGN AND TEST DOCUMENTS</th>
<th>VERIFICATION ACTIVITIES</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Requirements Specification</td>
<td>Overall Software Test Specification</td>
<td>External Input, starting point for SW supplier's work</td>
</tr>
<tr>
<td>System Safety Requirements Specification</td>
<td>Software Requirements Verification</td>
<td>Software Requirements</td>
</tr>
<tr>
<td>System Architecture Description</td>
<td>Software Architecture Verification</td>
<td>Software Architecture</td>
</tr>
<tr>
<td>System Safety Plan and V&amp;B Plan</td>
<td>Software Design Verification</td>
<td>Software Design</td>
</tr>
<tr>
<td>Software Requirements Specification</td>
<td>Software Component Design Verification</td>
<td>Software Component Design</td>
</tr>
<tr>
<td>Software Interfaces Specification</td>
<td>Software Test Specification</td>
<td></td>
</tr>
<tr>
<td>______________</td>
<td>______________</td>
<td>______________</td>
</tr>
<tr>
<td>Software Component Design Specification</td>
<td>Software Component Test Specification</td>
<td></td>
</tr>
</tbody>
</table>

Based on the proposer's:
- System requirement specification (user requirements, and statutory requirements, e.g. TSI CCS)
- System safety requirement specification (=CSM safety requirements),
- A description of the system architecture (=CSM system definition)
- A safety plan,

the SW supplier draws up, among other things:
- The software quality plan (Software Quality Assurance Plan in compliance with EN50128)
- The software requirement specification (see definition),
- The software test specification,
- The software requirement verification report.

In conjunction with drawing up the software test specification, it is established to what extent the SW supplier and the system supplier must perform system testing.

In some cases it is sufficient to test the software in a test set-up in a laboratory. In other cases it is the SW supplier who tests the software in the final subsystem.
Use of specialist assessors

The following Figure 6 shows the relationship between CSM RA and the EN standards, where EN50128 and EN50129 are part of the process for showing the CSM safety requirements have been met and as code of practice for risk-managing hazards related to systematic errors.

Figure 6 Relationships between CSM RA and EN5012x

Specialist assessors are understood to be assessors who are specialists within their respective field, e.g. ASR (software assessor, cf. EN50128) and ASSR (hardware assessor, cf. EN50129). The result of the specialist assessor’s assessment can be included as documentation for the AsBo (CSM assessor) for fulfilment of the CSM safety requirements.

In many cases there will also be a role as 'system assessor', cf. EN50126, and, if the change is significant, the system assessor and AsBo can be one and the same organisation.

In relation to Figure 6 it should be noted that:

- In the case of significant changes, the AsBo is responsible for assessing the overall system (HW and SW), but at the same time is dependent on the work of the specialist assessors.
- Since in some cases SW validation includes testing of the final system, the ASR assessment may also include this. Conversely, it may be necessary for the HW
manufacturer to test the system with specific SW. The ASSR assessment may therefore also include this.

- If the competences are in place, the roles of specialist assessor and AsBo can be performed by the same organisation.

As indicated above, it may be necessary to re-validate the HW functionality. In other words, it may be necessary to involve the HW supplier and his assessor in order to re-validate and assess the HW – even if only SW code is changed. This is because the SW is part of the CSM system, and if the SW is changed, the entire system changes at the same time.

It follows from EN50128 that it is the manufacturer who documents to the ASR that the requirements of EN50128 have been met.
It follows from CSM RA that it is the proposer who documents to the CSM assessor (AsBo) that the requirements of CSM RA have been met (if the change is significant).

The following division of tasks applies between AsBo and ASR:

Either:
1) The AsBo has the staff to assess compliance with EN50128, and can therefore also act as ASR itself. The AsBo drafts the SAR, which has a separate section for compliance with EN50128, or an independent assessment report, which is attached to the SAR.
Or:
2) The AsBo is not itself responsible for assessing whether the requirements of EN50128 have been met. The AsBo must still see the ASR's report, which documents the fact that EN50128 was applied satisfactorily, such that the safety requirements, including the SIL, may be deemed to have been met. In this case the AsBo should ensure that the ASR has the right resources and competences and is independent.

The requirements placed on the ASR’s competences and independence can be found in EN50128. The ASR should not be part of the manufacturer's or the contracting entity's organisation, unless this has been agreed in advance with the Danish Transport and Construction Agency.

7 When a change concerns series of identical systems - e.g. series of vehicles, the scope of the tests, including the scope of verification for the series, should be further defined.
Roles and responsibilities
The following Figure 7 shows the division of responsibilities between the manufacturer, who develops/changes the SW, and the customer\(^8\), which can, for example, be a railway undertaking.

**Figure 7 Division of responsibilities between manufacturer and railway company/infrastructure manager**

Scope of manufacturer’s responsibilities, cf. A) in Figure 7
EN50128 (chapter 5) places requirements on the manufacturer’s quality management system. This should as a minimum implement those parts of ISO 9001 that are concerned with organisation and the division of responsibilities.

\(^8\) If the railway undertaking or infrastructure manager is responsible for the development/change itself, it is to be regarded as the manufacturer.
Furthermore, annex B to the standard defines a series of staff functions and competence requirements that concern SW development/change. The manufacturer’s QMS must ensure that the project team that is assigned an SW development or change task performs the roles specified in the EN standard, and is organised in compliance with the standard.

**Figure 8 Organisation of SW projects (ref. figure 2 in EN50128)**

The following Figure 8, from EN50128, shows how an SW project can be organised, depending on the SSIL. However, the figure does not show all roles, cf. EN50128. For example, the position ‘configuration manager’ is not shown. It is obviously important that the manufacturer’s configuration management is well documented, among other things out of consideration for the transfer of the software to the customer (railway undertaking/infrastructure manager).
Scope of the railway undertaking/infrastructure manager’s responsibilities, cf. B) in Figure 7.

The railway undertaking/infrastructure manager’s primary responsibility is to ensure that the approved system is used in accordance with its conditions of use. In other words, it is operated and maintained in accordance with the manufacturer’s instructions.

Railway undertakings and infrastructure managers are not expected to possess the competences to develop/change SW in compliance with EN50128 (that is the manufacturer’s responsibility). On the other hand, the railway undertaking/infrastructure manager must, through its safety management system, designate those members of staff who possess the competences - and responsibility - to manage changes.
C) Managing changes

When SW is changed / renewed, it is important that there is a clear overview of the following:

- where in the system the change is, and how extensive it is,
- what configurations there are and how they are configuration-managed, and
- what is affected by the change at system level.

Changes to SW call for dialogue between the parties involved. There may therefore be a need for dialogue between RU/IM, NoBo, ASR, AsBo, DeBo, the Danish Transport and Construction Agency, a vehicle expert, etc.

If an EC declaration of verification has been drawn up, it may be necessary for this to be supplemented (by the manufacturer/contracting entity) in accordance with Annex V to the Interoperability Directive. This may mean the technical file accompanying the EC declaration of verification has to be updated.

Before placing into service, the railway undertaking/infrastructure manager must ensure, through its safety management system, that the change has been assessed by the competent parties so:

i. the criticality of the SW change should be assessed by the manufacturer.
ii. Whether a change must be regarded as a renewal/upgrading, cf. the Interoperability Directive, must be assessed by the contracting entity or the manufacturer.
iii. Whether already issued verification certificates are affected by the change must be assessed by the NoBo/DeBo/vehicle expert.
iv. Whether the change is significant, cf. CSM RA, must be assessed by the proposer.

Re i.: Where there is a need to change SW, standard EN50128, section 9.2.4.2, states that the manufacturer should initially assess whether a change should be regarded as 'major' (in this case the standard is applied in full) or 'minor' (in this case section 9.2 on maintaining SW is applied).

However, it is not apparent from the standard what should be understood by 'minor' and 'major'. Annex 1 therefore describes a procedure that can be used to determine whether a change is minor or major. According to EN50128, section 1.9, the assessment of a change's criticality (major/minor) must be submitted to an ASR.

Re ii.: The contracting entity will typically be a railway undertaking or an infrastructure manager.

Re iii.: If changes are made that could affect already issued verification certificates, the change must be submitted to the NoBo/DeBo/vehicle expert that drew up the verification certificate with a request to assess whether the certificate is still valid.

Re iv.: Where applicable, see chapter 5 on who can be a proposer. It is important to agree from the outset who is to be the proposer for the project. Since the CSM process must ultimately ensure that the railway system's subsystems are integrated safely, it will often be natural for the infrastructure manager or railway undertaking to act as proposer. In particular, in the case of changes at 'railway level', i.e. changes in the way the subsystems are integrated.

The process for assessing changes is described in detail in the following section.
8. The process model (I) – Starting conditions

The following chapter shows a process model that can be used to determine whether a given system with SW must be submitted to the Danish Transport and Construction Agency. Before the process model is used, it is important to investigate the following starting conditions:

**Figure 9 Starting conditions**

1. New SW or SW change?
   - Yes
   - No: The process model must not be used

2. Can affect safety or interoperability?
   - Yes
   - No

3. The organisation, SMS, QMS and competences are capable of managing SW?
   - Yes
   - No: The process model cannot be used yet
   - Yes: Starting condition satisfied. Go to step II

Re 1: The proposer has investigated and found that the change involves a software change\(^9\) in the railway system. This could, for example, be a change to the program or data.

Re 2: The proposer has also established whether the software has an impact on safety\(^10\), implying that in the worst-case scenario, SW and errors in SW could lead to some form of accident. If interoperability can be affected, the answer ‘yes’ must also be given.

Re 3: The new system or the change to the existing one is introduced by means of an SMS/QMS, and procedures have been introduced for managing SW, including configuration management. At the same time it has been found that the right competences to take charge of the process are in place.

\(^9\) Debugging of SW must also be regarded as a change. More on this in chapter 13.

\(^10\) The proposer must keep documentary evidence of its assessment, regardless of whether it is assessed that the change affects safety or not. The Danish Transport and Construction Agency may provide supervision in this regard.
9. The process model (II) – Flow diagram

A Starting conditions

B Draw up system definition

C Establish significance

D Is the SW in a vehicle?

E Is the system covered by TSI or NNTR?

F Must the system be certified?

F2 Must the system be certified?

G New subsystem or removal or upgrading?

H Criticality

I System must be certified by NOLLY/Della/vehicle expert

J System must be certified by NOLLY/Della

K Is the change significant or is it a new subsystem?

L Apply CSAR if the change is significant and/or TSI/NNTR if required

M Criticality

N Criticality

O Apply EN50128

P Apply EN50128 chapter 9.2

Q Apply EN50128 chapter 9.2

R Apply EN50128

S The system is commissioned in accordance with the railway undertaking’s and/or infrastructure manager’s safety management system

T Application for authorisation for placing into service/Presentation of the change, c.f. EN661/653

Blue: Proposer

Red: Manufacturer or contracting entity

Green: Manufacturer

Orange: Control organ

Yellow: Applicant

Dark: RU or IM
### Explanations of the process model

<table>
<thead>
<tr>
<th>Box</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| A   | **Starting conditions**  
See chapter 8 regarding prerequisites for the process. The meanings of the boxes used are:  

- □ = a process or activity,  
- = a decision,  
- = information that there is a subprocess. The colours of the boxes show who must oversee the process/activity/decision. The colours are explained in the figure. |
| B   | **System definition for systems with SW**  
The preliminary system definition must be designed so that it supports the assessment of significance. See chapter 10. |
| C   | **Establish whether the change is significant**  
Whether the change is significant must be decided by the proposer, and reference is made here to chapter 13. The proposer can be the RU, IM or ECM within the framework of the maintenance of the system or a party applying for authorisation to place into service. |
| D   | **Is the software in a vehicle?**  
Choose 'yes' if the software forms part of a system in a vehicle. |
| E   | **Systems covered by the Interoperability Directive may be covered by TSI or NNTR requirements:**  
The Interoperability Directive (2008/57/EC) covers the whole of the Danish railway network and vehicles used on it, except for the following railway systems, which are exempt pursuant to Order No 1281 of 19 November 2015 on the interoperability of the rail system:  

- a) Metros, trams and other light rail systems.  
- b) The local S-rail network and vehicles used exclusively on this.  
- c) Privately owned railway infrastructure and vehicles used exclusively on this infrastructure for the owner's own freight transport.  
- d) Infrastructure used exclusively for local, historical or touristic purposes, and vehicles that run exclusively on this infrastructure.  

Choose 'no' if the system in question is exempt. See chapter 11 on TSI requirements. |
| F   | **Must the system with SW be certified?**  
Choose 'yes' in the following cases:  

1) New vehicles not covered by the IOD.  
2) Changed subsystem covered by a verification or type-examination certificate that loses its validity due to the change.  

See also chapter 12 for further guidance on the certification of systems with SW. |
| F2  | **Must the system be certified?**  
Choose 'yes' in the following cases:  

1) New subsystem.  
2) Changed subsystem covered by a verification or type-examination certificate that loses its validity due to the change.  

See also chapter 12 for further guidance on the certification of systems with SW. |
| G   | **New subsystem or renewal or upgrading**  
In the case of a new subsystem, the answer is always 'yes'. |
Renewal and upgrading are defined in Article 2 of the Interoperability Directive: 
m) 'upgrading' means any major modification work on a subsystem or part subsystem 
which improves the overall performance of the subsystem, 
n) 'renewal' means any major substitution work on a subsystem or part subsystem which 
does not change the overall performance of the subsystem. 
Further guidance is provided in chapter 11, and in Commission Recommendation 
(2014/897/EU), Recommendation No 110.

**H, M, N** Criticality

Criticality (i.e. whether the change is major or minor, cf. EN50128) must be determined by 
the manufacturer and is a decisive factor in the extent to which EN50128 must be applied. 
Annex 1 provides guidance on how to determine criticality. The minor/major decision must 
be accepted by the ASR, cf. EN50128.

**I, J** The system with SW must be certified by the NoBo/DeBo/vehicle expert

If a system with SW has to be certified, the software’s baseline should be apparent from 
the certificates. 
It is also recommended that so-called 'pre-defined variants' are established, which make it 
possible to change the system subsequently, within certain limits, without new certificates 
having to be issued. See chapter 12.

**K** Is the change significant or is it a new subsystem?

See C and chapter 13 regarding the significance assessment. In the case of a new 
subsystem, 'yes' must always be chosen.

**L** Application of CSM RA

If the change is significant, CSM RA is applied to managing the safe integration, and the 
AsBo must prepare a safety assessment report. 
If CSM RA has to be applied for a particular purpose specified in a TSI/NNTR, the method is 
used for this purpose.

**O, R** EN50128 is applied in full, and the ASR must prepare an assessment report.

**P, Q** For changes categorised as 'minor', only chapter 9.2 of standard EN50128 is applicable. 
This means the change should be managed in accordance with DS/ISO/IEC 90003:2015, 
Software development – Guidelines for the application of ISO 9001:2008 to computer 
software.

**S** The railway undertaking/infrastructure manager’s SMS should include procedures for how 
systems with SW are to be managed. The Danish Transport and Construction Agency may 
provide supervision in this regard. 
The following documentation should be available to be presented: 
- Significance assessment and preliminary system definition, 
- The ASR’s assessment of the determination of criticality in case of a 'minor' 
  change, 
- The ASR’s assessment report in case of ‘major’ changes.

**T** See chapter 14 on the contents of the safety assessment report, change presentation, etc.
10. System definition for systems with SW

The Danish Transport and Construction Agency's general guide on the design of system definitions also applies to systems involving SW. However, in connection with the system definition for systems involving SW, information aimed precisely at SW needs to be weighted, which is the purpose of this chapter. If special properties can only be illustrated by the SW architecture or the design, Annex 1 contains further guidance in this regard.

Structure of the system definition
Systems with SW are defined on the basis of the CSM System and its interfaces. See Figure 3.

The following underlined headings are from the guide on system definitions, and for each heading additional topics are listed that are relevant to systems with SW.

For changes it is important to describe both the current situation and the desired new situation.

a. system objective, e.g. the intended purpose

The reason for the change, e.g. a desire for new functions, debugging, new SW platform, new HW, etc.

b. system functions and elements, where relevant (including e.g. human, technical and operational elements)

A block diagram should be used to outline where the computer/computers is/are in the overall system/subsystem (Where applicable, see Figure 12).

Changes in the implementation of system functions are described and it is shown which safety functions are processed by SW and which are e.g. processed mechanically; electrically; pneumatically; physically; by Instructions.

Any new functions are described.

Any new SIL classifications based on changes in implementation and system architecture are indicated.

c. system boundary, including interactions with other systems

Drawing, possibly involving different colours or figures, showing the boundary. Description of how the computer(s) fit(s) into the CSM and subsystem's functions.

d. physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces

One of the most important chapters in the system definitions, which is best described by a drawing. The drawing should show the internal and external interfaces.

The following should be shown

- The interface from the computer's Input/Output to other elements in the CSM system
- Common interfaces, e.g. with a common BUS
- If there are several computers, the interface with these is shown
- The interface between the CSM system and the subsystem is shown
- The interface between the subsystem and adjoining systems is shown

e. the system environment (e.g. energy and thermal flows, shocks, vibrations, electromagnetic interference, operational use)

The system environment in which the CSM system and the computer must work is described here.

f. existing safety measures and, after an iterative process, definition of the safety requirements identified by the risk assessment process

The starting point for the software development/change is described, i.e.:

- the CSM safety requirements, incl. SIL.
Note that the software requirement specification, including SSIL, does not necessarily need to be included in the CSM system definition, as this does not need to be part of the CSM risk assessment. See Figure 4, Figure 5 and Figure 6.

The SW development/implementation of a change may lead to the CSM safety requirements and the system definition having to be changed. This is done in an iterative development process. If new CSM safety requirements are identified in this connection, these new requirements must appear in the system definition. In this connection it may also become necessary to change the description in other sections of the system definition.

9. Assumptions in order to define the limits for the risk assessment

Here, for example, several assumptions and prerequisites can be listed regarding development, verification and validation processes, which are used during changes to SW, such as e.g.:

- Programming environment (including process flow from code to compiler, linker, executable file and installation)
- Use of recognised machine-based validation methods
- Use of test facilities – test laboratories and whether these are certified
- Change log and version management systems
- Organisation and competences of those involved
- Whether the manufacturer’s quality management system has been certified to develop SW

11. Renewal or upgrading

When a subsystem that is covered by the Interoperability Directive is changed, it must be decided whether the change involves a renewal or an upgrading. The purpose of this is to ensure that the subsystem remains interoperable or moves in a direction such that it ends up being interoperable.

Subsystems constructed in accordance with NNTR and TSI requirements are by definition interoperable. In other words, the NNTRs and TSIs define the satisfactory and necessary level of interoperability. It is therefore also the requirements of the NNTRs and TSIs that must form the basis of the assessment of whether a given change must be regarded as an upgrading or a renewal. The table below gives examples of provisions in the TSIs relating to SW:

<table>
<thead>
<tr>
<th>TSI</th>
<th>REQUIREMENT</th>
<th>REMARK</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOC&amp;PAS:2014, section 4.2.1.3</td>
<td>4) Electronic equipment and software used to perform safety-critical functions shall be developed and assessed using a method that is appropriate to safety-related electronic equipment and software.</td>
<td>It is not compulsory to apply EN50128/EN50129 to demonstrate compliance with 4.2.1.3, but it may be regarded as accepted practice if this is done.</td>
</tr>
<tr>
<td>TSI CCS 2012/88/EU, as amended, table 6.1, aspect: Reliability, availability, maintainability and safety (RAMS)</td>
<td>Check that the safety requirements specified in the basic parameters referred to in the relevant table in chapter 5 have been met, i.e.:</td>
<td>It is compulsory to apply EN50126/EN50128/EN50129 to demonstrate compliance with RAMS requirements, at component level. It is optional whether version 2001 or version 2011 of EN50128 is used.</td>
</tr>
<tr>
<td></td>
<td>1. Respect for quantitative Tolerable Hazard Rates (THRs) caused by random failures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The development process is able to detect and eliminate systematic failures.</td>
<td></td>
</tr>
</tbody>
</table>

...
### Table 1: Examples of SW-related requirements in TSIs

Where SW is required to be developed by appropriate methods, e.g. the requirement in TSI LOC&PAS:2014, section 4.2.1.3, changes classified as 'major', cf. annex 1 to this guide, should also be regarded as 'renewal or upgrading'.

### 12. Certification of systems with SW

The following section takes as its starting point that the CSM system is part of the subsystem, which is covered by requirements in NNTRs or TSIs, but the principles also apply to vehicles certified by a vehicle expert.

A NoBo/DeBo must be involved where:

1. A new subsystem is involved that is covered by an NNTR/TSI, e.g. CCS on-board or CCS trackside,
2. A change is involved to a subsystem that is covered by already issued verification certificates, including changes to interoperability components used,
3. In case of renewal or upgrading, the Danish Transport and Construction Agency decides that TSI/NNTR requirements apply.

In case 1) above, the NoBo/DeBo prepares a verification certificate confirming compliance with relevant TSI/NNTR requirements. Depending on which verification module\(^{11}\) is chosen, a type-examination certificate (module SB) or a design-examination certificate (module SH) is also drawn up.

If changes are made to an already certified subsystem (case 2) above), the rules in the module descriptions must be followed. Module SB states, among other things:

'8. The applicant shall inform the notified body that holds the technical documentation relating to the EC type-examination certificate of all modifications to the approved type that may affect the conformity of the subsystem with the requirements of the relevant TSI(s) or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EC type-examination certificate.

9. Each notified body shall inform its notifying authorities concerning the EC type-examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies concerning the EC type-examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued.

When a type-examination or design-examination certificate is drawn up, this should specify which SW baseline is included in the computers. If changes are made that could affect the certificate’s validity, the NoBo/DeBo/vehicle expert must be notified, to give them the opportunity to assess the certificate’s continued validity and if necessary prepare an addition or a new certificate.

To minimise the need for new certificates to be issued, the certificates can include ‘pre-defined variants’. A pre-defined variant can, for example, make it possible to change certain tables in the SW without the certificates losing their validity as a result.

\(^{11}\) The verification modules are described in /12/.
13. Determining significance

The Danish Transport and Construction Agency’s general guide on the assessment of significance also applies to systems involving SW. As SW has diverse properties, it will be necessary to supplement certain criteria, and in some cases there will be no need to perform a significance assessment.

Changes that may be regarded as non-significant
SW changes that have no impact on CSM safety requirements may be regarded as non-significant. This can be said to be the case if the following conditions are all satisfied:

1. The system definition is unchanged.
2. The SW that is changed is in operation.
3. CSM RA or EN50126 has been used to establish safety requirements for the system, and the SW was developed in accordance with EN50128 and has been assessed by the ASR.
4. The change will follow EN50128 and be re-assessed by the ASR.
5. 1-4 must be justified and accepted by the assessor organisation that prepared the safety assessment report for the system.

Re 1.
If no changes are made to the system definition (chapter 10, points a-g), the system safety requirements, and thus the starting point for applying EN50128, will be unchanged. In this case the risk assessment at system level is not affected by the intended change (no changes are therefore made to the external input, which is the basis for the SW supplier’s work, cf. Figure 5).

All changes since the most recent authorisation to place into service must be taken into consideration, e.g. changes to HW.

Even if only SW changes are made, it must be assessed whether the existing HW validation is affected. In such cases, a new HW validation and assessment must be performed (by the HW specialist assessor).

The development of the SW change (e.g. a debug process) may mean that the system definition has to be changed, and that the risk assessment at system level has to be reconsidered. In such cases, the change shall be significance-assessed in order to decide whether CSM RA also has to be followed. This applies regardless of whether or not the safety requirements are ultimately changed at system level.

Re 2.
The condition is born out of a desire to limit the ability to make SW changes in systems that have been certified and/or approved, but not commissioned, among other things to avoid ‘slicing’.

Re 3 and 4.
The fact that CSM RA/EN50126 has been used to establish safety requirements for the system means that there is already an assessed system definition with safety requirements, which can be used as a basis when the change has to be developed. Moreover, when EN50128 is used, there is likewise an SW requirement specification, test plan, etc. This allows the presumption that the existing SW was described at a level that makes it possible to make an SW change that does not result in unintended spill-over effects on the SW and thus inadvertent changes to the safety functions.

Condition 4 also provides an assurance that a method (EN50128) will again be used that is based precisely on the CSM safety requirements, and that the changed SW will not result in unintended spill-over effects on the SW and thus inadvertent changes to the safety functions.

Re 5.
Because 1. - 4. provide for the possibility of unintended interpretations, there is a further condition that an independent party - in relation to the proposer - must agree that the conditions have been satisfied. The assessor’s assessment must be available to be presented to the Danish Transport and Construction Agency.

12 The step between “System Development Phase” and “Software Requirements Phase” is explained in chapter 7, and shown in Figure 5 'Section of Life Cycle Model' for SW (ref. figure 3 in EN50128)
Example of a change that may be regarded non-significant:

The door system shown in Figure 10 below was analysed using CSM RA. Among other things, the analysis resulted in the following CSM safety requirements being established:

a) The train must not be able to move unless the doors are closed.

b) The doors must not be able to close if there are objects in the doorway.

Figure 10 Door control system

The safety requirements are implemented using a combination of HW and SW. The SW safety function is made up of the SW in the door control unit and the traction control in the train computer. The programs were produced pursuant to EN50128 by 2 different suppliers. An AsBo safety assessment report is available, which refers to 2 ASR reports for the software and one ASSR report for the HW.

After some time in operation a desire arises to change the door control software, since it has emerged that communication between the door control and the traction control is very slow. It is only possible to depart 45 seconds after the doors have closed.

Because the sole purpose of the desired SW change is to resolve a timing problem internal to the SW, and no safety requirements for timing have been recorded, the change is not expected to affect the CSM safety requirements. It should therefore be investigated whether the change may be regarded as non-significant:

Re 1. System definition

In this example, the original system definition does not include any safety requirements relating to time and timing, so the traction can, in principle, be properly activated just after the doors have closed.

The following documentation is drawn up:

- Documentation/argument for the system definition and CSM safety requirements being unchanged. Note that the documentation can only be finalised once the software has been changed. This is because during the development phase the need may arise to change the SW architecture, which necessitates a change to the CSM safety requirements, including drafting new CSM requirements, as a result of which the system definition is not unchanged.
No HW changes are made in the example. However, it may be necessary to involve an HW specialist assessor if the system validation so requires. Because the doors' mechanical function and the wheels' slip/slide are not affected in this example, this will not be necessary from a safety perspective.

Re 2 and 3.

In the example, conditions 2 and 3 are satisfied.

Re 4 and 5. The change will follow EN50128 and be re-assessed by the ASR.

The following are documented:

- The criticality analysis (the manufacturer's assessment of whether the change is major or minor)
- The ASR's assessment of the criticality analysis.
- The ASR’s assessment report in case of ‘major’ changes.
- The system assessor's/AsBo's assessment that conditions 1-4 have been satisfied.

Debugging

If an error is identified in a system with SW after it has been commissioned, it may be necessary to change the software to remove the error. A debug must be handled like all other types of change. However, more often than other types of change, debugs will be able to be classified as non-significant, cf. conditions 1-5 above. This is because, during debugging, it is not normally the intention to change the CSM system or the CSM safety requirements.

Supplement to significance criteria for systems with SW

The following text is a supplement to the Danish Transport and Construction Agency’s guide on significance assessment, and therefore does not address HW changes.

a) Consequence of failure (a credible worst-case scenario in the event of failure of the system under assessment, taking into account the safety barriers outside the system)

If the SW change's criticality is major\textsuperscript{14}, this is as a rule a change with a far-reaching consequence in case of failure and thus often also a significant change. See annex 1.

The criticality of the change should (in compliance with EN50128) be decided by the manufacturer and assessed by the ASR.

b) Innovation (used to implement the change; this applies both to what is innovative for the railway sector and what is merely new for the organisation implementing the change)

If the proposer can document

- that the same organisation made changes previously in the SW concerned
- that the SW concerned was developed in compliance with EN50128 and is in operation,
- that the SW change will be made in compliance with EN50128,
- that no ‘innovative’ changes/functions have been introduced into the CSM system,

there is normally no innovation.

c) Complexity of the change

\textsuperscript{11} EN50128 includes the following definitions:

3.1.9 Error, fault: defect, mistake or inaccuracy which could result in failure or in a deviation from the intended performance or behavior.

3.1.10 Failure: unacceptable difference between required and observed performance.

\textsuperscript{14}In some cases there is no need to change the system definition, even in the case of a major change. But the AsBo should still see evidence that the CSM safety requirements have been met, unless the change is not significant.
If the SW change’s criticality is ‘minor’, then as a rule a complex change is not involved. See annex 1.

The criticality of the change should (in compliance with EN50128) be decided by the manufacturer and assessed by the ASR.

d) Monitoring (inability to monitor the change made over the entire life cycle of the system and undertake appropriate interventions)

If autonomous technical barriers are already in place that ensure that errors in the CSM system are detected immediately, and action can be taken before accidents happen, the monitoring criterion will be able to be counted as a solid external barrier.

e) Reversibility (inability to return to the system as it was before the change)

The change can be said to be reversible if the previous SW version can be reinstated without changing the safety level and without having to make other changes at the same time.

f) Accumulation (assessment of the significance of the change taking into account all recent safety-related changes to the system under assessment that were not considered significant)

Previous non-significant changes to the CSM system must be included, regardless of whether they involved SW or HW changes.
Approval and supervision

14. Handling by the Danish Transport and Construction Agency

The Danish Transport and Construction Agency's guidelines on authorisation for placing into service for subsystems in the railway infrastructure and approval of vehicles also apply to subsystems and vehicles incorporating SW. The following guide should be seen as a supplement to these.

Change presentation

If the SW change is significant or should be regarded as a renewal or upgrading, the change must be presented to the Danish Transport and Construction Agency, cf. BEK 653, § 12 or BEK 661, § 9. This is done by submitting a project description, as described in the Orders. The table below shows the requirements placed on the project description, for vehicles and for subsystems in the infrastructure:

<table>
<thead>
<tr>
<th>CHANGE PRESENTATION, CF. BEK 653 AND 661.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEK 661, on authorisation for placing into service for subsystems in the railway infrastructure. /2/.</td>
</tr>
</tbody>
</table>

§ 9. In the case of a change to an existing subsystem that is deemed to be significant or is regarded as a renewal or upgrading, cf. § 7, para. 2 or 3, a project description must be submitted to the Danish Transport and Construction Agency before the change is implemented. The Danish Transport and Construction Agency decides whether the change requires a new authorisation for placing into service under § 6.

Para. 2. The project description must contain the following:
1) Documentation for the undertaking's assessment of the significance of the change, cf. § 7.
2) A preliminary system definition of the change to the subsystem, including details of:
   a) whether the undertaking wishes to use documentation from a corresponding change that was previously approved in Denmark, an EU or EEA country according to identical requirements under equivalent operating conditions, and
   b) whether the change according to the undertaking's assessment is covered by TSI requirements.

§ 12. In the case of a change to a vehicle, or a change to an approved vehicle type, cf. § 11, a project description must be submitted to the Danish Transport and Construction Agency before the change is implemented. The Danish Transport and Construction Agency then decides whether a new authorisation for placing into service is required, or a new type-approval and to what extent § 8 must be applied.

Para. 2. The project description must contain the following:
1) Documentation for the proposer's assessment of the significance of the change, cf. § 11, para.1.
2) A preliminary system definition of the change, including details of:
   a) whether the undertaking wishes to use documentation from a corresponding change that was previously approved in Denmark, an EU or EEA country according to identical requirements under equivalent operating conditions, and
   b) which TSI requirements are affected by the change, and which TSI requirements are expected to be applied if the change according to the undertaking's assessment is covered by a TSI,
   c) which notified national technical rules are affected by the change and which notified national technical rules are expected to be applied, and
   d) which verification procedures the undertaking wishes to use.
3) Preliminary risk analysis.

Where software changes are concerned, the preliminary system definition should be drawn up in accordance with chapter 10 of this guide. It is also recommended that the project description be accompanied by:

1) The assessment of the criticality of the change.
2) The ASR's assessment of 1).
3) Details of whether any existing certificates need to be updated.
The contents of the assessment reports

The AsBo’s report

If the AsBo also has the competences and resources to act as ASR, the safety assessment report can either have a separate section on compliance with EN50128 or a reference to an independent software assessment report, which is attached.

If the AsBo does not carry out the EN50128 assessment itself, the following guidelines apply: The AsBo should check that the ASR’s report can be used as evidence that the CSM safety requirements and SIL can be considered to have been met. The AsBo should also ensure that the ASR has used competent specialist assessors. The result of this check should appear in the safety assessment report. The ASR’s assessment report is attached to the safety assessment report.

The ASR’s report

The ASR’s SW assessment report should be prepared in accordance with EN50128, chapter 6.4. Among other things, the report should include:

- Identification of the SW and version(s)
- Assessment of how EN50128 was applied
- Assessment of the application conditions for the SW, e.g.:
  - Installation and test requirements
  - Configuration and change management requirements
  - Other safety-related application conditions (SRAC)
- Assessor’s additional application conditions
- What may be changed without a new assessment

Non-significant SW changes

As shown in the process model, a situation may arise in which an SW change is ‘major’ or ‘minor’ but not significant. In this case, the railway undertaking/infrastructure manager should, in addition to the significance assessment, retain the manufacturer’s criticality assessment, and the associated ASR assessment. The Danish Transport and Construction Agency can ask to see these documents in the course of its supervisory activities.

In the case of a ‘major’ SW change, there should also be a positive ASR assessment report. The Danish Transport and Construction Agency can ask to see the report in the course of its supervisory activities.
Managing `obsolete´ SW

15. Systems with SW `proven in use´

Existing older SW can be developed without the use of EN50128 and/or without the use of a defined SSIL level for the SW safety functions. Safety in systems that use SW without the use of EN50128 is often based on procedures that have not been documented supplemented by substantial testing of the SW in question instead of systematic processes. This situation can make it more challenging to change the software, when the principles of this guide should simultaneously be followed:

System definition

The recommendations in chapter 10 of the guide on how the system definition should be designed are not based on EN50128, and can also be applied to obsolete SW. However, it may be a challenge to obtain documentation for the CSM system, including the safety requirements. This is nevertheless necessary to be able to make the change in a responsible manner.

Assessment of criticality

The procedure for determining the criticality of the software change described in annex 1 is not dependent on EN50128 being applied. The criticality assessment will therefore also be able to be performed for older SW. However, it may be a challenge to describe the SW architecture etc. if documentation on this is not already available. This is nevertheless necessary to be able to change the software in a responsible manner.

Assessment of significance

Changes to obsolete safety-related SW must always be assessed for significance. The section of the guide on significance assessment and annex 1 are not based on EN50128 being applied, and can therefore also apply to assessments of obsolete SW.

Development process

SW development should always follow an appropriate procedure, and the so-called V-model is an example of this. See Figure 11 V-model for development below.
If the existing SW was developed according to a dedicated and documented procedure, this should normally also be followed when changes are made.

Otherwise EN50128 can be used as a basis, but it may be a challenge to specify the SW requirements if the existing SW is a 'black box'. This can be compensated for to a certain degree by producing an extensive test plan.

Assessment

Irrespective of whether EN50128 is followed or not, an SW assessor should always be involved when changes are made to SW that forms part of safety-critical systems. The assessor's tasks are in principle the same as when EN50128 is applied. However, if EN50128 is not followed, the assessor should also assess whether the development model is suitable.
Annex 1: Determining criticality

This annex describes a procedure that can be used to determine whether a SW change is minor or major. The procedure does not depend on whether or not EN50128 is applied, or another suitable process, but if EN50128 is applied, the procedure can be used to establish minor or major, since EN50128, as mentioned above, does not define principles for determining this.

Criticality is linked to what is referred to in the standards as the Safety Integrity Level (SSIL), which can best be described as a measure of how confident one should be that a particular function actually works when needed. This implicitly means that a high Safety Integrity Level normally also means that the SW is highly critical and a change to the SW will therefore quickly be a major change. The procedure defines certain exceptions to this basic rule.

The procedure includes determination of the safety integrity, pre-defined variant and simplicity, which are described in greater detail below.

SW design

Before criticality can be determined, the system definition (see chapter 10) must be supplemented with a more precise description of the software for certain of the headings that follow:

b) system functions and elements, where relevant (including e.g. human, technical and operational elements)

The following list specifies what is particularly relevant when criticality has to be assessed:

- Block diagram showing the interaction between multiple computers
- The computer's SW architecture (system architecture description, cf. EN50128)
- The affected SW modules (components, cf. EN50128)
- The affected SW safety functions
- Any state diagrams
- Any human interaction and control
- Where applicable, the computer's HW architecture
- The development environment and SW tools.

See also the figure below.

Figure 12 Block diagram in system definition

c) system boundary, including interactions with other systems
It is important to describe what parts can be said with logical arguments to be untouched. For example, adjoining computers without a bus connection to the computer in question, tools used, HW, etc.

The following are described:

- The interface from the installed SW to SW development tools
- The interface to the upload of new/changed programs
- Sketches showing how SW in the same computer may not be affected by the change if this is the case.

9) assumptions in order to limit the risk assessment

Here, for example additional assumptions could be specified regarding the programming language chosen, compiler, assembler, computer, etc.

**Determining criticality**

Criticality can be determined in accordance with Figure 13, below.

**Figure 13 Determining criticality**
Determining safety integrity (K1 and K3)

If the SSIL value is not known, determination can be performed by applying EN50129 Annex A or IEC 61508. The following table can in principle be used to support this.

<table>
<thead>
<tr>
<th>The computer’s safety functions concern</th>
<th>Typically defined SSIL</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interlocking (object control, central interlocking, etc.)</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Train control: ETCS, CBTC, ATC, HKT onboard</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Train detection axle counters, etc.</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Balises</td>
<td>4</td>
<td>Determination depends on the system concept. SSIL might well be e.g. 1-2 if several balises are involved.</td>
</tr>
<tr>
<td>Train computer with direct control of the train’s safety functions, where an error in the SW e.g. could cause a collision</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Train computer that monitors or indirectly controls the train’s safety functions.</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Object and person detectors (track and platform etc.), pattern recognition camera etc.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Hot axle box detection</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Fire alarms, engine control and communication in the train</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Brake computers, WSP systems</td>
<td>1</td>
<td>SSIL 1 requires the emergency braking system to be completely independent of these systems. If this is not the case, SSIL will typically be 3-4.</td>
</tr>
<tr>
<td>TMS, TCM, CTC, TCC (remote management)</td>
<td>1-4</td>
<td>The systems often have very few safety functions, and it can often be shown that SSIL 0 is sufficient. Here SSIL is set from 1 to 4, as certain safety functions are often processed. For local S-trains (CBTC system) there are safety functions with SSIL level 4.</td>
</tr>
<tr>
<td>Traction current control and switching equipment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCADA systems (monitoring and control)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switchboard for marshalling yards</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Information systems, air conditioning, visual displays, etc.</td>
<td>0-2</td>
<td>EN50128 is, cf. section 1.3 of the standard, not relevant to SW that has been identified as not important to safety, i.e. SW that, in the event of an SW error, cannot affect any safety functions. Information systems, and air conditioning that may be important for safety are covered by the standard. ETCS DMI is e.g. SIL 2.</td>
</tr>
</tbody>
</table>

Table 2 Determining SSIL
Pre-defined variant (K2 and K4)

A predefined variant is a change that has been foreseen in advance and is covered by the certified and approved system. The predefined variant can be part of the SW maintenance plan, cf. EN50128.

SW that is changed can e.g. involve data fields, data blocks, code fields, etc., such that a known capacity/performance is achieved by a known program code in the program being activated or run in a different way. The following guidelines apply to determination:

1. The change must be 'legal', which means that the action is covered by an existing assessment / approval / certification (by a NoBo/DeBo/vehicle expert).
2. The change follows certain predetermined rules and implementation procedures.

If this is the case, the change can be seen to be a pre-defined variant.

Example 1
An odometer can be set for different wheel diameters, where the change consists of replacing a code field e.g. a chip with the new data for the wheel diameter. The underlying program is approved to handle new input from the code field.

Example 2
An interlocking is designed so that SW can control one, two or three points mechanisms. If the number of mechanisms is changed, it is a value in a parameter in the SW that is changed.

Example 3
A level crossing facility is designed so that the SW can control one or two barriers, and/or one or two tracks. If the number of tracks and barriers is changed, new parameters in the SW are changed.

Example 4
A door control system is designed so that the SW can control doors both with and without sliding steps. In the computer, this is determined by a manual switch.

Determining simplicity (K6)

Certain changes can be assigned the value ‘simple’. However, a seemingly simple SW change can easily have several inappropriate and unforeseeable consequences if the change is not made in a highly controlled SW environment. For example, a small bug fix in one program can affect other parts of the same program both as a result of the program itself affecting the other program or as a result of the program using the same HW, e.g. data storage etc.

Appendix D.32 'Impact analysis' of EN50128 described certain requirements for considerations to be made when SW is changed. The considerations lead to, among other things, an analysis and decision as to how much of the SW is to be changed, and how much is to be re-validated and tested. These documented analyses can be used as a basis for determining simplicity.

Alternatively, the following can always be used for the determination:

1. The change must relate to a bug fix or modification in just one program module.
2. The change must be ‘encapsulated’ in an SW architecture where it can be proved that the change cannot have side effects or spill over into other program code.
3. It must be able to be established (see EN50128 chapter 7.5) that the change is sufficiently testable.

Re 1: A bug fix means that the module is not performing as specified and the change is designed to make the module perform correctly. In case of a modification, there will also be a new specification of how the module should function. The module has unique interfaces, and there are neither more nor fewer interfaces after the modification.

Re 2: However, it may be difficult to apply actual boundaries to the SW, and in the case of a ‘single processor system' you usually have to consider all the SW in the computer. If there are

15 Generally, multiple simultaneous corrections cannot be used for the determination, as this quickly becomes a complex correction.
established systematics for how 'the encapsulation' works, and the ASR agrees to this, the point is satisfied.

Re 3: By establishing the criterion from 1. and 2. it can be shown, combined with EN50128 chapter 7.5 on 'test coverage', that the module is sufficiently testable, which means all input combinations and all outputs are known and testable.

If this is the case, the change can be seen to be simple.

**Software in the same computer (KS)**

If the computer contains several types of program, where some process safety-critical functions (SSIL 1-4) and others do not, it is often difficult to distinguish and claim that changes are only being made to what is not critical (SSIL 0). Arguments should therefore be limited to systems that only involve SSIL 0.
Annex 2: Example of change to 'obsolete' SW

Contents

1) Introduction
2) System definition
   a. A system objective, e.g. the intended purpose
   b. System functions and elements, where relevant (including e.g. human, technical and operational elements)
   c. System boundary, including interactions with other systems
   d. Physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces
   e. System environment
   f. Existing safety measures and, after an iterative process, definition of the safety requirements identified by the risk assessment process.
   g. Assumptions relating to limiting the risk assessment.
3) The process model (I) – Prerequisites for the process
4) The process model (II) – Flow diagram

Introduction

This annex contains an example of a change to an existing ‘obsolete’ software in a passenger information system (PIS) in a train.

The information system ensures communication between the driver, conductor and passengers.

System definition

The proposer (in this case a railway undertaking) draws up the system definition, cf. chapter 10 of the guide:

a. A system objective, e.g. the intended purpose

In this case it is assumed that after a year’s operating experience a need has arisen to change the PIS software. There are a few changes: a) a special operating situation with coupled trains, where communication between driver and conductor is illogical and b) connection of a new type of handset.

b. System functions and elements, where relevant (including e.g. human, technical and operational elements)

Functions

The PIS system includes a number of functions:

- Driver messages to passengers (selective and global PA*)
- Intercom system between driver and conductor (selective and global IC*)
- DVA (automatic speaker information: ‘The next station is..’)
- Display control (internal and external)
- Seat reservation
- Emergency voice units (not emergency stop switches)

* selective/global means whether the message is given to a specific carriage/all carriages of the train. PA = ‘Public Announcement’ and IC = InterCommunication between e.g. conductor and driver.

During normal operation the functions are not safety-related, e.g. a global PA with ‘Notification of delay’.

In emergency situations, however, communication is safety-related, e.g. the train driver must be able to announce an evacuation via global PA in the event of a fire in a tunnel.
Elements

Figure 14 below shows a basic PIS system. The black boxes and lines in the figure are the PIS system, which is SW-based, i.e. all functions are performed by the entire SW in the connected controllers.

The PIS system can be expanded by a purely hardware-based 'UIC system', where the UIC system is the blue boxes and lines. This expanded system is known as PIS+UIC and therefore consists of the entire black and blue system.

In the PIS+UIC system it is possible to perform the functions global PA and global IC via both the black software-based PIS system and the blue UIC hardware line. It depends on the train type whether a train uses PIS or PIS+UIC.

Figure 14 System definition for PIS.

PIS is the black system. The blue UIC system is an expansion of the PIS system. (The abbreviations in the figure stand for SW/HW = soft-/hardware, UIC = a standard HW communication line.)

c. System boundary, including interactions with other systems

The PIS system is an autonomous technical system with a technical interface to the train radio. There are several direct human interfaces between train driver and conductor and passengers.

d. Physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces

See figure 14.

e. System environment

The PIS system belongs to the category in EN50155, 'Electronic equipment used on rolling stock'. This standard specifies shake testing, fire requirements, EMC, etc. It should be noted that EN50155 also includes simple ISO quality requirements for software.
f. Existing safety measures and, after an iterative process, definition of the safety requirements identified by the risk assessment process.

The PIS system is older, and the original SW was developed before EN50128 was released. The system is 'proven in use'.

As described above, the safety-related interest focuses on the global PA and IC functions. These are referred to below as 'G-PA/IC'.

The safety integrity at functional level of the G-PA/IC functions is determined at SIL1, cf. IEC 61508. The indicative table 2 in annex 1 'Determining SSIL' is used to check this.

Note that the SIL determination applies at functional level and is independent of whether it is implemented with the PIS or PIS+UIC system.

This can be broken down into the following HW/SW requirements:

<table>
<thead>
<tr>
<th>System</th>
<th>Safety integrity of the G-PA/IC functions, at system level</th>
<th>HW requirement</th>
<th>SW requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIS</td>
<td>SIL1</td>
<td>SIL1</td>
<td>SSIL1</td>
</tr>
</tbody>
</table>

g. Assumptions in order to define the risk assessment

In this case, the PIS software is provided by a known supplier. Corrections in the SW are made by a programmer who is familiar with the older development environment. The test environment is well tested.

The risk assessment below is performed for the PIS system alone, and therefore does not include the PIS+UIC system.

The process model (I) – Prerequisites for the process

The guide's process model requires the following:
1. That the change relates to software.
2. That the SW affects safety or interoperability.
3. The change is made in SMS/QMS by competent persons.

As is apparent from the above review of the PIS system, starting conditions 1. – 3. are satisfied, and the process model (II) can therefore be used.

The process model (II) – Flow diagram

The chapter 'The process model (II) – Flow diagram' from the guide is reviewed below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Topic</th>
<th>Description/analysis</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Starting condition</td>
<td>The project manager for 'Change of PIS system' is located at the operator's maintenance supplier.</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Draw up system definition</td>
<td>This has (largely) been drawn up above.</td>
<td></td>
</tr>
</tbody>
</table>

Note that the table is a support table. The SIL can be established by applying EN50129 Annex A or IEC 61508.

The example does not report in detail on SMS/QMS and competences. These factors are assumed to be under control.
<table>
<thead>
<tr>
<th>Step</th>
<th>Topic</th>
<th>Description/analysis</th>
<th>Result</th>
</tr>
</thead>
</table>
| C    | Establish significance | The criticality of the change is assessed by the SW supplier, and his SW assessor based on the principles in annex 1 to the guide. Here it is assumed that the change is a minor one. Significance can then be determined:  
**Consequence:** Serious; if G-PA/IC fails in scenario 'Fire in tunnel'.  
**Innovation:** Low; because known development environment and no innovative functions.  
**Complexity:** Low; because change is minor.  
**Monitoring:** High; because operator's existing procedures specify daily testing of G-PA/IC.  
**Reversibility:** High; because relatively easy to switch back to previous SW version.  
**Accumulation:** No. No previous changes were made in the example.  
**Assessment.** Not significant; serious consequence suggests significant, but, especially because of the high degree of monitoring and since the other parameter suggest non-significant, the change is assessed as non-significant. |  |
| E    | Is the system covered by TSI or NNTR requirements? | TSI Loc&Pas places requirements on both safety-related SW (see chapter 11 in the guide) and communication systems. | =>H |
| H    | Criticality (Minor / Major) | According to the flowchart in annex 1 to the guide, there are three requirements for simplicity (K6):  
1) Bug fix  
2) Encapsulated  
3) High testability in the software of G-PA/IC  
The PIS system itself is autonomous and thus encapsulated. The change concerns a bug fix and an internal interface component. The safety function G-PA/IC and the new component are highly testable, so overall the change is assessed as simple.  
It is now possible to decide that the change is minor, since K1=no; K3=yes; K4=no and K6=yes.  
The assessment is submitted to the ASR, in accordance with EN50128. | =>G |
| G    | New subsystem or renewal or upgrading? | There is no new subsystem.  
The contracting entity (in this case the railway undertaking) assesses that no renewal or upgrading is involved, cf. criteria referred to in point G in the process model. | =>F |
| F    | Must the system be certified? | No, since the system is not already certified. If the system had been certified by the NoBo, NoBo should have assessed the continued validity of the certificate, cf. chapter 12 of the guide. | =>K |
| K    | Is the change significant or is it a new subsystem? | The example involves a non-significant change to the existing 'rolling stock' subsystem. | =>M |
| M    | Criticality? | See H. | =>P |
| P    | Apply EN50128 chapter 9.2 | EN50128, chapter 9.2, refers to standard ISO/IEC 90003, which is a quality management standard for SW.  
See also chapter 'Managing obsolete SW'. |  |
| S    | The system is placed into service in accordance with the SMS of the railway undertaking and/or infrastructure manager. | Among other things, the railway undertaking retains:  
- The significance assessment and the system definition.  
- The supplier's criticality assessment.  
- The SW assessor's assessment of the criticality assessment. |  |

Table 3 Review of flow diagram in the guide's chapter 'The process model (II) – Flow diagram'
Annex 3: Example of change to CBTC on-board

Contents

1) Introduction
2) System definition
3) The process model (I) – Prerequisites for the process
4) The process model (II) – Flow diagram

Introduction

The example takes as its starting point a known change to the on-board equipment on Copenhagen's local S-railways. The change is described in a system definition 'SW Change to On-board S-train M1.99 Variant', Siemens doc: A6Z00037537227. Here referred to as SYSDEF. The equipment is known as 'CBTC on-board equipment' and is shown in a very global fashion in the black frame in the figure below.

The figure also shows that the equipment consists of several computers and a change to the mobile train control subsystem could affect the SW in one or more computers. The structure is highly complex, and a change to one computer can affect both other parts of the 'CBTC on-board equipment' and the local S-railways fixed CBTC system.

The change used in the example can be characterised as a minor functional correction and bug fix. The change is made in various SW modules, which run on different computers in the mobile CBTC system.
System definition in the example

a. **a system objective, e.g. the intended purpose**

S-train on-board database must be brought into line with the infrastructure and correction of error.

b. **system functions and elements, where relevant (including e.g. human, technical and operational elements)**

The block diagram below shows the overall subsystem where the computers/SW in the computers are located.
The red markings show where the changes are made. SYSDEF shows which specific corrections are made in the SW. There are no actual functional changes and the safety functions are to be maintained.

The SW architecture of the computer and the SW modules in question can be taken from the Siemens documentation via a reference.

All SW changes are listed in the form of a 'fix request'. There is no new human interaction and control.

c. system boundary, including interactions with other systems

The system boundary (high level) is shown in the figure.

In the example, the CSM system and subsystem are the same, since everything is fully integrated and changes are made in all parts.

d. physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces

In principle there are no changes. SYSDEF refers to the applicable system drawing for the S-train’s equipment.

e. the system environment (e.g. energy and thermal flows, shocks, vibrations, electromagnetic interference, operational use)
Unchanged

f. existing safety measures and, after an iterative process, definition of the safety requirements identified by the risk assessment process

Most existing safety functions are fixed at SIL 4 and are assumed to be unchanged following the change.

SYSDEF refers to the requirement specification for the entire 'on-board'.

g. assumptions in order to define the risk assessment

Since no new safety functions were identified, it is assumed that all requirements are unchanged.

The process model (I) – Prerequisites for the process

The guide’s process model requires the following:
1. That the change relates to software.
2. That the SW affects safety or interoperability.
3. That the change is made in SMS/QMS by competent persons.

Re 1.: cf. SYSDEF: “system definition for SW change” is there an SW change.

Re 2.: Since a change is being made in SSIL 4-classified SW, safety may be affected.

Re 3.: Organisation is unchanged in relation to the other introduction of CBTC on local S-railways.

Conclusion: Starting conditions 1. – 3. are satisfied, and the process model (II) can therefore be used.

The process model (II) – Flow diagram

The chapter 'The process model (II) – Flow diagram' from the guide is reviewed below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Topic</th>
<th>Description/analysis</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Starting conditions</td>
<td>These are satisfied, as described under The process model (I).</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>System definition</td>
<td>Has been drawn up. See previous section.</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Is the system covered by TSI/NNTR?</td>
<td>Local S-rail network and vehicles only used here are exempt from the IOD.</td>
<td>=&gt;D</td>
</tr>
<tr>
<td>D</td>
<td>Is the SW in a vehicle?</td>
<td>In this example; yes.</td>
<td>=&gt;F</td>
</tr>
<tr>
<td>F</td>
<td>Must the system be certified?</td>
<td>The on-board equipment that is changed was certified by a vehicle expert. The change is submitted to the vehicle expert, who in this example decides that new certificates must be drawn up, since the existing ones are no longer valid as a result of the change.</td>
<td>=&gt;I</td>
</tr>
<tr>
<td>I</td>
<td>The system is certified</td>
<td>The expert updates the certificates. This activity does not need to be completed in order to continue to step K.</td>
<td></td>
</tr>
</tbody>
</table>
| K    | Is the change significant or is it a new subsystem? | a) Consequence of failure Existing SW is classified as SIL 4. The SW supplier classifies the change as 'major' because it is being made in SIL 4 functions without any pre-defined variant. The ASR agrees.
b) Innovation | => L |
<table>
<thead>
<tr>
<th>Step</th>
<th>Topic</th>
<th>Description/analysis</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Long experience with changes in the SW in question&lt;br&gt;SW was developed in compliance with EN50128 and assessed by the ASR. The change will be made in compliance with EN50128 and assessed by the ASR.&lt;br&gt;No innovative functions are introduced.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c)</td>
<td>Complexity of the change&lt;br&gt;Changes are made in several places and may be seen to be complex.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d)</td>
<td>Monitoring&lt;br&gt;Not possible to prevent accidents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e)</td>
<td>Reversibility&lt;br&gt;Not possible in operation, and errors must be corrected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f)</td>
<td>Accumulation&lt;br&gt;The change is before APIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Conclusion</strong>&lt;br&gt;Even though b), innovation, suggests that the change does not need to be significant, a), c), d) and e) suggest that it should be assessed as significant.</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Apply CSM RA...</td>
<td>The AsBo must as a minimum have:&lt;br&gt;- The new system definition&lt;br&gt;- ASR’s report.</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>Criticality</td>
<td>The SW supplier classifies the change as ‘major’.&lt;br&gt;The ASR agrees.</td>
<td>=&gt;R</td>
</tr>
<tr>
<td>R</td>
<td>Apply EN50128</td>
<td>The standard is applied by the SW supplier. The ASR assesses the result. The assessment report is sent to the AsBo who, in this case, prepares an addendum to the safety assessment report.</td>
<td></td>
</tr>
<tr>
<td>K</td>
<td>Change presentation</td>
<td>The change is submitted to the Danish Transport and Construction Agency which, in this case, decides that a new authorisation for placing into service must be issued in accordance with the provisions of BEK653, § 8.</td>
<td></td>
</tr>
</tbody>
</table>

Table 4 Review of flow diagram in the guide’s chapter ‘The process model (II) – Flow diagram’
The guide addresses how the railway’s technical systems with software should be managed with regard to the regulatory approval of new systems or systems that are changed.