20-034 Client safety assurance of high integrity software-based systems for railway applications

[This page should be deleted at the publication stage of the project]

Version:	0.2		
Purpose:	Approval to proceed to consultation		
Authors:	Jane Dobson, Portfolio Head Ged Neacy, Professional Head of CCS Jianhong Jin, Principal CCC Engineer, CCS		
Sponsor:	Ged Neacy, Professional Head of CCS		
Lead industry committee:	Control, Command and Signalling Standards Committee (CCS SC)	**Date:**	17 March 2022
Supporting industry committee:	Rolling Stock Standards Committee (RST SC)	**Date:**	11 March 2022
Supporting industry committee:	Plant Standards Committee (PLT SC)	**Date:**	03 March 2022

Decisions

Control Command and Communications Committee is asked to

DECIDE if the proposed new issue of RIS-0745-CCS issue one delivers the intentions of the proposal for change.

DECIDE if the proposed new issue of RIS-0745-CCS issue one is in a suitable state for consultation.

APPROVE that the proposed new issue of RIS-0745-CCS issue one and the withdrawal of GEGN8650 issue one are consulted on.

IDENTIFY any specific organisations or individuals to be included in the consultation.

Rolling Stock and Plant Standard Committees are asked to:

DECIDE if the proposed new issue of RIS-0745-CCS issue one delivers the intentions of the proposal for change.

DECIDE if the proposed new issue of RIS-0745-CCS issue one is in a suitable state for consultation.

SUPPORT that the proposed new issue of RIS-0745-CCS issue one and the withdrawal of GEGN8650 issue one are consulted on.

IDENTIFY any specific organisations or individuals to be included in the consultation.

20-034 Client safety assurance of high integrity software-based systems for railway applications

This business case for change has been developed to support standards committees in taking decisions related to changes to standards, it includes an assessment of the predicted impacts arising from the change.

Proposed documents

Number	*Title*	Issue
RIS-0745-CCS	Client safety assurance of high integrity software-based systems for railway applications	1

Documents for withdrawal

Number	*Title*	Issue
GEGN8650	*Guidance on high integrity software-based systems for railway applications*	1

Summary

Background and change

RAIB report "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017," recommendation 1 states that "Network Rail, in consultation with RSSB and the wider rail industry and drawing on existing processes where appropriate, should develop and implement a mandatory safety assurance procedure (and associated guidance) for its client role on projects involving installation and modification of high integrity software-based systems. The process should incorporate relevant best practice from other safety critical industries"

In response to the RAIB recommendation, Network Rail (NR) recognised that an industry response needed to be taken as high integrity software-based systems can be infrastructure and/or train-based systems.

An initial scoping paper by NR was presented and approved by industry-wide Asset Integrity Group (AIG) on 29 July 2020. The paper proposed the production of a Rail Industry Standard (RIS) outlining the key requirements and guidance for clients involved in designing and installing new or modified high integrity software-based systems. An action plan was submitted to ORR forecasting the publication of the RIS in September 2022.

This project has been set up to support Network Rail to address recommendation 1 from the RAIB report, through the production of a Rail Industry Standard (RIS) that includes requirements, rationale and guidance on the specification, use and management of software-related systems across the overall lifecycle. It is expected that such a publication would be applied within the framework of an organisation's safety assurance procedure.

The RIS will help industry to better manage and reduce the number of incidents where the performance of software is one of the causal factors, with the subsequent improvements in safety and reliability that will bring.

Industry impact due to changes

Impact areas	Scale of impact	Estimated value £ 's
A. Legal compliance and assurance	Medium	Not proportionate to quantify
B. Health, safety and security	Medium	£5M over five years
C. Reliability and operational performance	Medium	£2.2M over five years
D. Design and maintenance	Medium	£1M over five years
E. People, process and systems	Medium	Not proportionate to quantify
F. Environment and sustainability	N/A	Not proportionate to quantify
G. Customer experience and industry reputation	Medium	Not proportionate to quantify
Total value of industry opportunity =		**£8.2M over five years**

The standards change contribution to the total value of industry opportunity				
☐ None or low	☐ Minor but useful	☐ Moderate	☑ Important / essential	☐ Urgent / critical

Detail

1. What are the objectives associated with this change?

Objective 1 – Support Network Rail to address recommendation 1 from the RAIB report "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017"

1.1 The objective of this project is to support Network Rail to address recommendation 1 from the RAIB report "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017," through the production of a Rail Industry Standard (RIS) that includes a set of principal requirements, rationale and guidance that can be applied within the framework of an organisation's safety assurance procedure.

Objective 2 – Undertake a review of GEGN8650 issue one (Guidance on high integrity software-based systems for railway applications)

1.2 RIS-0745-CCS issue one takes into account GEGN8650 issue one (Guidance on high integrity software-based systems for railway applications') in terms of its relevance and how it may complement and support the principal requirements of the Duty Holder.

2. How does the content in the standard need to change to achieve the objectives?

Objective 1 – Support Network Rail to address recommendation 1 from the RAIB report "Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017"

2.1 The requirements in RIS-0745-CCS issue one provide requirements, rationale and guidance for staff discharging the client role responsibilities essential for the safe introduction, use and maintenance of new and modified high integrity software-based systems.

2.2 The requirements in RIS-0745-CCS issue one are supported by rationales and guidance, including relevant good practice from other safety critical industries. It has followed the generic system lifecycle and safety management principles defined in ISO, IEC, CEN/CENELEC and other standards.

2.3 The RIS defines the role and project management process of the client as specified by RAIB in recommendation 1 by:

a) clearly documenting its expectation of each supplier as part of the project's overall safety assurance process, including the required safety justifications, documentation and the traceability of safety evidence throughout the project's lifecycle;
b) supporting the selection of suppliers that are competent and capable of delivering a safe system;
c) specifying the role of independent safety assessment bodies, such as ASBOs (assessment bodies);
d) capturing the need for good engineering safety management, configuration management and change control in the contractual requirements;

e) defining the required safety integrity of the key safety functions, the operational context and external interfaces;
f) defining the process to be applied when placing reliance on the re-use or adaptation of a system with previous acceptance, or commercial off-the-shelf products;
g) working with the supplier to properly understand the safety risks and define the system safety requirements and architecture;
h) monitoring the supplier's verification of its design (hardware and software);
i) ensuring that the design is suitably validated prior to commissioning;
j) undertaking audit and inspection by the client;
k) setting out the extent of the client's review of independent assessments, and its own consideration of the safety justifications as part of the approval process;
l) testing and commissioning of the installed system, and subsequent maintenance; and
m) recording and retaining data needed for investigation of safety related failures.

Objective 2 – Undertake a review of GEGN8650 issue one (Guidance on high integrity software-based systems for railway applications)

2.4 Relevant guidance from GEGN8650 issue one has been included in RIS-0745-CCS issue one which makes GEGN 8650 issue one redundant and it will be withdrawn.

3. How urgently does the change need to happen to achieve the objectives?

3.1 RIS-0745-CCS issue addresses a RAIB recommendation following the Cambrian Coast Line incident of 20 October 2017. The action plan submitted by Network Rail (NR) to the ORR forecasted the publication of the RIS by September 2022.

3.2 The rail industry is becoming increasingly reliant on software for the management of the infrastructure and efficient operation of their trains, and there has been a number of incidents in the rail and other sectors recently and over the last few years where software issues have been one of the causal factors.

3.3 It is therefore important to progress this project to contribute to the minimisation of the number of incidents caused by software failures.

4. What are the positive and negative impacts of implementing the change?

Justification of impact, scale and quantification for the seven impact areas

A. Legal compliance and assurance

4.1 Assurance can be undertaken more effectively, and suppliers that are competent and capable of delivering a safe system selected, so that industry can better manage and improve processes that could reduce the number of incidents where software is one of the causal factors, with the subsequent improvements in safety and reliability that will bring.

4.2 It is not proportionate to quantify any potential benefit associated with the assurance process.

B. Health, safety and security

4.3 Network Rail and the wider rail industry will benefit from this new standard. It will contribute to improving safety by reducing the number of accidents and incidents where software deficiency is one of the causal factors, due to greater clarity and consistency in implementation.

4.4 The Cambrian Coast line incident in 2017, caused by the loss of safety critical signalling data, could have resulted in a major accident. This was one of twelve (approximately 8%) potentially high risk accidents involving passenger trains in 2017-2018. The health and safety benefits associated with the introduction of RIS-0745-CCS issue one are estimated to be £5M over five years (comprising £0.7M/year and £0.3M/year), based on the following:

- Proportion of passenger train accidents caused by software=8% (as set out above)
- Frequency of passenger train accidents=4.07/year (Safety Risk Model v8.5)

Frequency of passenger train accidents caused by software of 0.34/year x notional cost of an accident of £2M (including material damaged and business interruption but excluding safety) = £0.7M/year.

- Proportion of passenger train accidents caused by software=8% (as set out above)
- Risk of passenger train accident=1.75 fatalities and weighted injuries (FWI) (Safety Risk Model v8.5)

Risk of passenger train accidents caused by software of 0.15 FWI/year x Value of preventing a fatality of £2.017M (RSSB Taking Safety Decisions-Cost Benefit Analysis 10/11/21) which is approximately £0.3M/year.

C. Reliability and operational performance

4.5 Reducing the number of incidents and accidents where software issues are a causal factor improves reliability and operational performance of the railway. An incident involving Thameslink class 700 and 717 trains on 9 August 2019 resulted in a power failure following a lightning strike and inability to return to service quickly. A number of trains required manual and complex intervention to restart causing significant disruption including 371 cancelled services, 200 part cancelled services and 873 delayed services, and 14,428 delay minutes. Based on three such incidents every five years and a delay cost of £50 per minute the cost to industry would be equivalent to 14,427x £50x3 which represents £2.2M over a five year period.

D. Design and maintenance

4.6 Requirements and guidance provide benefits from greater coordination and mutual understanding of the potential hazards involved with complex software-related systems between procurement, technical specialists, and supplier, supporting the deployment of ERTMS.

4.7 Better understanding supports companies in using software to improve maintenance of infrastructure and vehicles.

4.8 For Traffic Management Systems it typically takes an 8-hour shift to upload new software, plus a day or more of testing time especially with new traction and tilt software. These

updates might take place twice a year. At a cost of £60/hour, this could amount to approximately £2,000 per year per train (16 hours x £60/hr x 2/year). Feedback from operators is that there is always some kind of software load going on at the depots. Requirements and guidance on the specification, use and management of software related systems across the overall lifecycle, embedded within an organisation's safety assurance procedure, will support improved software requirements and integration before the software leaves the factory, thereby reducing the need for continual software updates of approx. £2,000 per year per unit. With an estimated 2,000 new units (source: Department for Transport Vehicle Ageing Report 15 August 2021) across the network introduced since the late 1990's, a reduction in cost from improved software requirements and understanding of software related systems of 5%, which is equivalent to £100 per unit, could bring benefits of £1m over five years (2,000 units x £100/unit x 5 years).

E. People, process and systems

4.9 A better understanding facilitates right first-time software, thereby reducing technician support, writing and updating further iterations, transporting and modifying equipment of the trains.

F. Environment and sustainability

4.10 The proposed changes are not directly relevant to the environment and sustainability and no benefit is claimed.

G. Customer experience and industry reputation

4.11 RIS-0745-CCS issue one will support the reduction in the number of incidents and accidents where software issues are a causal factor, thereby enabling improved operational performance to be achieved. Improved operational performance has a positive impact on customer experience, while reducing the number of incidents reduces potential reputational damage to the industry. Incidents of extensive delays can attract a lot of media interest, lasting over several months, particularly fuelled by social media. The associated benefit of software assurance on customer experience and sustainability is considered not proportionate to attempt to quantify.

5. What is the contribution of this standards change in realising the value to industry opportunity?

5.1 RIS-0745-CCS issue one will fill an existing gap in achieving common guidance for all industry members, including Network Rail, Train Operating Companies (FOCs) and Freight Operating Companies (FOCs), in collaboration with the software suppliers, and across all relevant railway interfaces for projects involving installation and modification of high integrity software-based systems. The standards change contribution to the total value of industry opportunity is categorised as important, with an estimated value of £8.2m over a five year period. Whilst this is a rail-specific document, the standard will benefit from lessons learned from other systems and modes, such as aviation and automotive who have broader experience of managing software.

6. What was the effort required by RSSB to make the change?

6.1 RSSB has supported Network Rail in determining the principal requirements and guidance through the membership of a drafting review group administered and facilitated by Network Rail, led by Network Rail's external supplier; RSSB has also codified drafting review content into RSSB requirements and guidance, and is managing consultation and approval through Industry Standards committees and supporting its embedment in industry.

7. Can RSSB deliver against industry's expected timescales?

7.1 The project is currently on program to meet the publication date of 3 September 2022 and commencing industry consultation on 4 April 2022.

8. How will the industry implement the change?

8.1 Network Rail will encourage the use of the new safety assurance requirements and guidance through their safety management systems, processes and procedures.

8.2 The safety assurance requirements and guidance are adopted by Network Rail and the wider industry, within the framework of their safety assurance procedure for high-integrity software-based systems.

9. How will RSSB assess whether the change is achieving the objectives?

9.1 RSSB will seek feedback from stakeholders on the application of the RIS.

9.2 A review of RIS- 0745-CCS will be undertaken one year after its publication to assess whether the objectives are being achieved.

Appendix A Disposition Table

Table A1: GEGN8650 issue one - Guidance on High-Integrity Software-Based Systems for Railway Applications to RIS-0745-CCS issue one - Client safety assurance of high integrity software-based systems for railway applications

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
Part 1 Introduction	N/A	Withdrawn	This part provides general introductory text including purpose, background and related European standards.	2
1.1 Purpose	N/A	Withdrawn	This section provides the purpose of the guidance being assisting the procurement, specification and contractual arrangements for high-integrity software and software-based systems. The document is for those in procurement and project teams which is included in the client role specified within RIS-0745-CCS.	2
1.2 Background	N/A	Withdrawn	This section refers to the reliance on high-integrity software to perform safety function and that software- based systems are being used more frequently on the railway. These are described in 2.1 of RIS-0745-CCS. This section also refers to safety incidents and RSSB research report T1047, both are also covered by RIS-0745-CCS.	2
1.3 European standards relevant to this guidance note	N/A	Withdrawn	This section refers to a set of European standards relating to generic requirements for software, including quality management and safety management requirements. Guidance on 'relationship with standards and legislation' (2.2 of RIS-0745-CCS) includes references to all standards in this section.	2
1.4 Approval and Authorisation	N/A	Withdrawn	No comment.	2
Part 2 What are High-Integrity Software and Software-Based Systems?	N/A	Withdrawn	Title	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
2.1 High-integrity software	N/A	Withdrawn	This section provides definition of high-integrity software, the term "Rigour" and methods to support rigour, including software V&V process. This section refers to the previous version of BS EN 50126-1:1999 (now BS EN 50126-1:2017) for the V&V process This section also includes some guidance on potential of software faults resulting in failures and that dynamic testing alone is not enough to testing all behaviours generated by any complex software. Related guidance is provided in part 2 of RIS-0745-CCS. The guidance in this section also includes introduction to Safety Integrity Levels (SIL) which are covered in BS EN 50128:2011 and other standards. The guidance refers to two acronyms: software SL and system SIL, however the guidance does not use 'system SIL' apart from the definition. RIS-0745-CCS used SIL as a general term which aligns with European standards. It recognises the importance of ensuring safety as an integrated software-based system that including hardware that the software will run on.	2
2.2 High-integrity software-based systems	N/A	Withdrawn	This section provides definition of high-integrity software-based system. It is expected the same documentation for the system as it would be if the software were procured separately. A definition for high-integrity software-based system is provided in 1.2 of RIS-0745-CCS.	2
2.3 Measuring integrity	N/A	Withdrawn	Title for the section.	2
2.3.1 Random failures versus systematic failures	N/A	Withdrawn	This section introduces the categories of failures in the context of safety critical systems. The classes of failures can be found in 5.6.2 of EN50126-1:2017. 2.3.1.4 refers to mitigating systematic failures following a rigorous V&V process with appropriate methodology and techniques according to SIL. RIS-0745-CCS aligns with the V&V process in EN50126:1:2017. G 2.1.5 of RIS-0745-CCS provides guidance on controlling risk from software failure using proven and rigour techniques. 3.1.2 of RIS-0745-CCS provides guidance on the approach to proportionate assurance.	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
2.4 Software development life cycle	N/A	Withdrawn	This section includes: • Introduction to software development life cycle, referring to EN50128. • Guidance on common design software faults and how it is difficult to discover faults through testing. • Details on verification of software design at early stage to reduce later design changes, and how simulation can be used for validation of design early in the process. • Reference to Annex A of 50128 on development techniques and V&V activities for different SIL. • How verification at each stage help reduce number of faults in the product. • Guidance on formal methods • Guidance on change management process for traceability of the requirements throughout the life cycle of the software. Most part of guidance in this section relate to verification of software during development process, which are included in BS EN50128:2011. RIS-0745-CCS covers requirements and guidance relevant to the client role in managing the safety assurance of high integrity software-based system. In relating to the guidance in this section, RIS-0745-CCS provides: • requirements structured around a system lifecycle (2.4) • guidance on software faults in the overview section (2.1) • requirements and guidance on state gate reviews for phases (3.4) • requirements and guidance on change control (3.5).	2
Part 3 Guidance on the Procurement of High-Integrity Software and Software-Based Systems	N/A	Withdrawn	Title	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
3.1 Introduction	N/A	Withdrawn	This section provides guidance on the importance of adequate requirements capturing and documentation before placing a contract and to include change management in the contract. RIS-0745-CCS provides requirements and guidance on: • produce and maintain a safety assurance strategy that requires the documentation of requirements and process. (3.1) • specification of system requirements (4.4) by considering full range of lifecycle concepts (4.1). • change control (3.5). • contract for assurance (3.3)	2
3.2 Requirement development	N/A	Withdrawn	This section states the reliance on technical experts and these who understand how the system behave in the domain of application. RIS-0745-CCS provides requirements and guidance on: • ensure competency (3.2) • specification of system requirements (4.4) by considering full range of lifecycle concepts (4.1) • system definitions to be reviewed by appropriate set of stakeholders who have the competency and knowledge of how the system will be used (4.2).	2
3.3 Documenting the design choices	N/A	Withdrawn	This section provides guidance on documenting the traceability of the requirements with the code during software development phase and refers to BS EN 50128:2011 This section also refers to consider impact of any change to the requirements on SIL and related processes. RIS-0745-CCS provides requirements and guidance on: • change control (3.5). • safety assurance records (3.1.3) that requires establishing/maintaining records and traceability. This includes records for SIL determination for each safety function and assurance evidence, that would support the assessment of impact of changing requirements.	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
3.4 Documenting the selection of V&V activities	N/A	Withdrawn	This section includes guidance on: • documenting the V&V activities. • the choice of V&V activities for SIL (referred to BS EN 50128:2011). • good practice for supplier to justify the choice of V&V activities. • documenting methods for V&V activities (referred to BS EN 50128:2011) • obtain V&V documentation when procuring software. • more rigorous V&V and maintenance plan for higher SIL (referred to BS EN 50128:2011) RIS-0745-CCS provides requirements and guidance on: • safety assurance strategy (3.1.1) that requires documenting all assurance activities. • safety assurance records (3.1.3) that requires establishing/maintaining records and traceability. This includes the assurance responsibility and evidence. • proportionate assurance (3.1.2)	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
3.5 Maintenance plan	N/A	Withdrawn	This section includes guidance on: • the use of maintenance plan to record changes, provide traceability. • more rigorous V&V process and maintenance plan for higher SIL (referred to BS EN 50128:2011) • information may be included in the plan. • Consider obsolescence strategies at development stage and the cost implications of COTS hardware obsolescence. RIS-0745-CCS provides requirements and guidance on: • change control (3.5) • safety assurance records (3.1.3) that requires establishing/maintaining records and traceability • proportionate assurance (3.1.2) • retain system data for incident investigation (4.8.2) • safety assurance strategy (3.1.1) that requires documenting all assurance activities. • Retain system capability through life (4.8.1) • Report, analyse, and correct system performance issues and defects (4.8.3) • Pre-existing subsystems or software elements (4.5.2); obsolescence issues identified when consider the intended use of COTS systems.	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
3.6 Procurement of high-integrity software or software-based systems	N/A	Withdrawn	This section includes guidance on: • preparing draft specifications of safety function and failure criteria before procuring high-integrity software. • principles on writing requirements (referred to Part 4) and supplier management (referred to Part 5) • what requirements to include in the contract (referred to 5.2.1) • including range of stakeholders for decisions on COTS software considerations • following the same process for software on its own or as part of a system • possible transferring of roles from supplier to customer if software being customised for a particular use. Referred to comments for relevant part for those referenced to other part of the document. RIS-0745-CCS provides requirements and guidance on: • specification of system requirements (4.4) by considering full range of lifecycle concepts (4.1) • risk analysis and evaluation (4.3) • pre-existing subsystems or software elements (4.5.2) • safe assurance strategy (3.1.1) requires the definition and recording of roles and responsibilities throughout the lifecycles.	2
Part 4 Guidance on the Preparation of High-Integrity Software Specifications	N/A	Withdrawn	Title	2
4.1 Determining the software SIL	N/A	Withdrawn	This section refers to 3.6.1 of the guidance and BS EN 50128:2011 for allocation of the software SIL.	2
4.2 Adequate requirement specification	Appendix C C.1	No change	This section provides guidance on benefit of adequate requirements specification and how complete requirements are typically supported. Carried forward as C.1 of RIS-0745-CCS.	1 and 2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
4.3 Principles for complete requirements	Appendix C C.2 Principles for complete requirements	No change	Title	2
4.3.1 Safety analysis during requirement development	N/A	Withdrawn	The section includes guidance on undertaking safety analysis at early stage and in accordance with CSM RA (referred to the prevision set of RSSB guidance notes on CSM-RA). RIS-0745-CCS includes references to the current combined RSSB guidance note GEGN8646 Guidance on the Common Safety Method for Risk Evaluation and Assessment.	2
4.3.2 Requirement categorisation	Appendix C C.2.1	Redrafted – No material change, content reworded to improve clarity (editorial change)	This section includes guidance on considering categories of requirements when checking completeness. Carried forward as C.2.1 of RIS-0745-CCS.	1 and 2
4.4 Principle for correct requirements	Appendix C.3 Principles for correct requirements	No change	Title	2
4.4.1 Documenting the system's operating environment	Appendix C C.3.1	Redrafted – No material change, content reworded to improve clarity (editorial change)	4.4.1.1 has been covered by requirements and guidance for 4.2 of RIS-0745-CCS. The rest of the section is carried over as C.3.1 of RIS-0745-CCS.	1 and 2
4.4.2 Documenting what the software must and must not do	Appendix C C.3.2	Redrafted – No material change, content reworded to improve clarity (editorial change)	This section includes guidance on documenting and identifying limit of operations of software. Carried forward as C.3.2 of RIS-0745-CCS.	1 and 2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
4.5 Principles for consistent requirements	Appendix C.4 Principles for consistent requirements	No change	Title	1 and 2
4.5.1 Managing changes in software requirements	Appendix C C.4.1	Redrafted – No material change, content reworded to improve clarity (editorial change)	Carried forward as C.4.1. of RIS-0745-CCS.	1 and 2
4.5.2 Verification of requirements	Appendix C C.4.2	No change	Carried forward as C.4.2. of RIS-0745-CCS.	1 and 2
Part 5 Management of Software Suppliers for Software-Based Systems	N/A	Withdrawn	Title	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
5.1 Introduction	N/A	Withdrawn	This section includes guidance on: • explicit requirements for contract on customer's intention • project risk assessment • adequate documentations and plans (referred to 5.3.2.4 of BS EN50128:2011 • documentation that provides traceability of activities, requirements and architecture in each phase. • formal method for V&V process • supply selection and competency RIS-0745-CCS provides requirements and guidance on: • specification of system requirements (4.4) by considering full range of lifecycle concepts (4.1) • risk analysis and evaluation (4.3) • safety assurance strategy (3.1.1) that requires assurance activities are planned and documented. • safety assurance records (3.1.3) that requires establishing/maintaining records and traceability • supplier selection (3.2.2) and contract terms (3.3.1)	2
5.2 Principles for managing suppliers	N/A	Withdrawn	Title	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
5.2.1 Technical requirements for contracts	N/A	Withdrawn	This section provides guidance on contractual clauses. The list of clauses includes support during requirement definition, testing, change management, documentation, training, upgrades and etc. The related requirement in RIS-0745-CCS (3.3.1) on contract terms refer to safety assurance strategy for activities assigned to suppliers and that the need for suppliers to comply with standards, engage in stage gate review and inform the client of any changes. The guidance also refers to including the definition of the ownership of the software in the contract, the guidance refers to GEGN8607 for the use of escrow arrangement as a way to manage IPR. The contractual clauses also include the management of cyber security. Cyber security is one of "other disciplines" listed in the section 2.5 of RIS-0745-CCS, stating that each of these disciplines has its own standards setting out methods and approaches.	2
5.2.2 Need for independent certification of software	N/A	Withdrawn	This section includes guidance on: • the assessment of software by qualified independent assessor (referred to BS EN50128:2011) • the assessment of whole change, the need for an independent assessment if changes are significant (referred to CSM RA) • consideration of whether an independent assessment is required and the provision for it included in the contract • review the applicability of any existing independent certifications RIS-0745-CCS provides requirements and guidance on: • audit and assessment (3.6) • safety assurance strategy (3.1.1) that requires the definition of roles for all organisations involved. • aligning the safety assurance activities with CSM RA and referring to GEGN8646 for further guidance. (2.2.11 and 2.2.12). • pre-existing subsystems or software elements (4.5.2).	2

From GEGN8650 issue one	To RIS-0745-CCS issue one	Way forward	Comments	Objective
5.2.3 Generating evidence of V&V activities	N/A	Withdrawn	This section includes guidance on: • verification &validation (V&V) for software correctness. • evidence from both processes documented • factory acceptance test (FAT) and user acceptance testing (UAT) reports as part of the evidence. RIS-0745-CCS provides requirements and guidance on: • stage gate reviews (3.4) • configuration items include outputs of V&V (change control in 3.5) • system validation (4.6) supported by a check list including factory and site tests (A.6).	2
5.2.4 Specifying notations to be used	N/A	Withdrawn	This section includes guidance on notations and the benefit of rigorous notation. Different notations that could be used for each software SIL are covered by BS EN 50128:2011.	2
5.2.5 Role of the customer	N/A	Withdrawn	This section provides guidance on the customer being involved throughout the software development RIS-0745-CCS sets out requirements and guidance for the role of the client in managing safety assurance of high integrity software-based system used in railway applications. The safety assurance strategy (3.1.1) of the RIS requires the definition of roles for all organisations including roles of the client.	2
5.3 Principle for managing suppliers for the maintenance of the software	N/A	Withdrawn	The section provides guidance on managing suppliers for software maintenance: • including contractual obligations that enables future maintenance with items to consider • management plan (referred to BS EN 50128:2011) RIS-0745-CCS provides requirements and guidance on: • contract terms (3.3.1) to carrying out actives assigned to them and produce the artefacts assigned to them in the safety assurance strategy (3.1.1). • Operation, maintenance, and performance monitoring (4.8) that requires retain system capability through life.	2