Consultation comments and responses

Document number: **Client safety assurance of high integrity software-based systems for railway applications**

Consultation closing date: **19 April 2022**

1. Responders to consultation

No	Name	Company
1	David Warwick	Network Rail
2	Orry King	Network Rail
3	James Wilson	First Group
4	Mark Molyneux	RDG
5	Richard Stainton	Network Rail
6	Yuki Ohashi	Angel Trains
7	Stephen Trigg	GWR
8	Ian Cuthbertson	Lner
9	Peter Morris	Hitachi Rail
10	Lucia Capogna	AEGIS Certification Service
11	Olufemi Okeya	Network Rail

2. Summary of comments

Code	Description	Total
-	Consulted	
CE	Critical errors	
ED	Editorial errors	
TY	Typographical errors	
OB	Observations	
-	Total comments returned	

Classification codes for a way forward:

- DC – Document change
- NC – No change

3. Collated consultation comments and responses

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
1			General Comment: I think this is a well developed document which will provide useful guidance in the area intended.		1	NC			Noted with thanks.
2			General Comment: This document is not software specific and is more system related.	It would be great to have more guidance on the software side, that explains how the existing standards should be applied and what are the evidence a Client should request to suppliers based on that.	10	NC			Noted. The RIS is intended for high integrity software-based systems which include both software and hardware. The standard will be periodically reviewed as part of the standard lifecycle. The need for inclusion of more guidance on the software side could be considered when next reviewed.
3		General	Who is the client		11	DC		1.1 G 2.3	The term client refers to the group of people within the client's organisation who are collectively responsible for the procurement and the use of a safety-related software based system. Section 1.1 has been expanded relating the client role to that of Proposer (typically IM and RU) and to include more guidance on client organisations. Further explanation of client organisation in relation to the change of client organisation was provided in section G 2.3 Working examples of client organisations have been sought from the industry, which could be developed and included in a future version of the RIS-0745-CCS.
4		General	What is deemed high integrity system?		11	NC		1.2.1	For the purpose of this RIS, high integrity software-based systems, are those systems that deliver functions assessed to have a safety integrity level (SIL) greater that basic integrity, or Performance Level (PL) at b, c, d and e as set out in the BS EN ISO 13849 series, and where the functionality of the system is primarily delivered through the execution of software (as set out in clause 1.2.1)
5	7	1.1	The first paragraph explains what is in the standard but could be improved by explaining why the document should be followed.	Include reference to the legal requirements to manage risk and how following the standard assists in demonstrating compliance.	2	DC		1.1.3 and 1.1.4	A new paragraph added to section 1.1 with reference to the legal requirements. Existing 1.1.3 expanded to include how the standard assists in demonstrating compliance. (now 1.1.4) 1.1.3 The Health and Safety at Work, etc. Act (HASAW) places legal responsibilities on organisations regarding the management of safety. The Management of Health and Safety at Work regulations reinforce HASAW, placing duties on employers and employees to manage health and safety. 1.1.4 The Railways and Other Guided Transport Systems (Safety) Regulations (ROGS) require transport operators to maintain a safety management system. This standard can be adopted by a client organisation under their safety management system (SMS), to assist the management of risks relating to high integrity software-based systems.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
6	7	1.1	Whilst introduction of the role of client links to the RAIB report that gave rise to the new standard, it would be useful to put it into context of terms used elsewhere in the industry.	Relate the client role to that of Proposer in CSM RA legislation – this may assist later in the document when CSM RA risk management is referenced.	2	DC		1.1.5 - 1.1.7 Definitions	The following have been added to section 1.1: 1.1.5 Common Safety Method for Risk Evaluation and Assessment (CSM RA) provides a standard approach for proposers of a technical, operational or organisational change that affects safety to evaluate and assess risk. If a change is significant, the proposer is responsible and accountable for applying the CSM RA process. 1.1.6 In many circumstances, the proposer will be a railway undertaking (RU) or infrastructure manager (IM). Other types of proposers include an entity in charge of maintenance (ECM) who is responsible for the maintenance and modification of rail vehicles. 1.1.7 When a high integrity software-based system is procured, the client organisation could be the RU or IM who would be the proposer of the change for CSM RA purposes. Added the following in Definitions: **proposer** One of the following: a) a railway undertaking or an infrastructure manager b) an entity in charge of maintenance c) a contracting entity or a manufacturer which invites: i) an approved body or a designated body to apply the UK verification assessment procedure in accordance with regulation 17 of and Schedule 4 to the Railways (Interoperability) Regulations 2011; or ii) an EU notified body to apply the EC verification procedure in accordance with Directive 2008/57/EC or a designated body according to Article 17(3) of that directive. Source: CSM RA

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
7	7	1.1.2	It is not clear if the scope of this RIS is intended to cover Train Operating Companies and vehicle owners. This could lead to confusion in the industry.	Examples of client organisations could be provided.	9	DC		1.1	In general. a licence holder is only required to comply with RISs (or parts of RISs) that are applicable to its licenced activities. The licence holder does not have to comply with a RIS if, following consultation, it has adopted and is complying with an equally effective measure. Any rail industry company that is not a licence holder can choose to adopt all or part of a RIS through company procedures or contract conditions. Section 1.1 has been expanded relating the client role to that of Proposer and to include more guidance on client organisations. Further explanation of client organisation in relation to the change of client organisation was provided in section G 2.3 Working examples of client organisations have been sought from the industry, which could be developed and included a future version of the RIS-0745-CCS. The following have been added to section 1.1, (in response to Comment No 6) 1.1.5 Common Safety Method for Risk Evaluation and Assessment (CSM RA) provides a standard approach for proposers of a technical, operational or organisational change that affects safety to evaluate and assess risk. If a change is significant, the proposer is responsible and accountable for applying the CSM RA process. 1.1.6 In many circumstances, the proposer will be a railway undertaking (RU) or infrastructure manager (IM). Other types of proposers include an entity in charge of maintenance (ECM) who is responsible for the maintenance and modification of rail vehicles. 1.1.7 When a high integrity software-based system is procured, the client organisation could be the RU or IM who would be the proposer of the change for CSM RA purposes.
8	7	1.1.4	BS EN 50128:2001 is listed, however the latest version of this standard is EN 50128:2011 + A2:2020	To amend with the latest EN 50128 version.	10	DC		1.1.8	Revised. The was an editorial error. It was intended to be BS EN 50128:2011, as listed in the reference section.
9	7	1.1.4	It states, “The standard is structured to align with the 12-phase lifecycle set out in BS EN 50126-1:2017”.	I would expect this standard to be structured on the EN 50128 and EN 50657 lifecycle phases. This generates confusion.	10	NC			BS EN 50126 ‘is applicable to railway application fields, namely Command, Control and Signalling, Rolling Stock and Fixed Installations’ to the specification and demonstration of RAMS for systems, including software. BS EN50126 addresses system issues on the wider scale, while BS EN 50128 only covers software aspect of railway control and protection applications, and BS EN 50657 covers Software on Board Rolling Stock. The scope of RIS-0745-CCS covers both on-board and trackside systems.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
10	8	1.2.1	It states, ”RIS-0745-CCS issue one covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than 0 …”. Please note that the concept of SIL 0 has been replaced with Basic Integrity in all Standards listed in Clause 1.1.4. It is also noted that G2.1.11 states: “Systems that are determined to have a SIL of 0 are referred to in BS EN 50126-1:2017 as 'basic integrity'”.	Please amend to read ”RIS-0745-CCS issue one covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than **BI** …”	10	DC		1.2.1 And G 2.1.11	1.2.1 Revised. Replaced with ‘basic integrity (BI)’, now reads: RIS-0745-CCS issue one covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than basic integrity (BI), or performance level (PL) at b, c, d and e as set out in the BS EN ISO 13849 series, and where the functionality of the system is primarily delivered through the execution of software. Also, first part of G 2.1.11 rewrite to replace ‘SIL 0’: The suite of railway software standards places a reduced set of requirements on the design and development of systems that have a basic integrity. However, many of the activities set out in this standard could be beneficial even at basic integrity because….
11	8	1.2.1	Does control logic controller meet this definition or software application in a wheel lathe		11	NC			RIS-0745-CCS covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than basic integrity, or performance level (PL) at b, c, d, and e, and where the functionality of the system is primarily delivered through the execution of software. The performance level of the lathe software will fall within the performance levels set out in 1.2.1 of RIS-0745-CCS. However, the RIS should only be applied where the develop and use of these systems are as set out in 1.2.3.
12	8	1.2.2	Not sure why we mention on track separately. I would change the wording	RIS-0745-CCS issue one applies to systems used in railway applications, primarily infrastructure, trains, on-track machines and plant and their operation to deliver a service especially where software controls safety functions.	7	NC		1.2.2	The on-track machines (OTM) and on-track plant (OTP) are mentioned separately, because the control systems on these machines are generally derivatives of those used on civil engineering machines that need to comply with the Supply of Machinery (Safety) Regulations 2008 (as amended). Also, most of the base machines are from European manufacturers that will already be supplying control systems compliant with EN ISO 13849 series and EN 61508 series. Therefore, the control systems on these machines will use the BS EN ISO 13849 series and BS EN 61508 series.
13	8	1.2.2	Does the standard apply to portable transportable and mobile plant, fixed plant and depot plant?		11	NC			RIS-0745-CCS covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than basic integrity, or Performance Level (PL) at b, c, d, and e, and where the functionality of the system is primarily delivered through the execution of software. If the portable transportable and mobile plant, fixed plant and deport plan are to be used on Network Rail managed infrastructure, and that the performance level fall within the performance levels set out in RIS-0745-CCS draft 1f clause 1.2.1, then the RIS applies. However, the RIS should only be applied where the develop and use of these systems are as set out in 1.2.3.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
14	8	1.2.2	NTH Plant suggests referencing relevant existing RIS for On-track machines and on-track plant which adequately addresses the same risk or reference to these standards. They are RIS 1530 PLT for OTP and RIS 1702 PLT for OTM.		11	DC			On Track Machines and On Track Plant are fitted with complex control systems, therefore RIS-0745-CCS could be useful to support the safety assurance of the systems. RIS-1530-PLT Issue 6 'Technical Requirements for On-Track Plant and Their Associated Equipment and Trolleys', currently covers software in clause 5.11.7: 5.11.7 All software and software systems shall be validated and documented. All software incorporated into a system with a performance level of d shall meet the requirements of a SIL 2 system as defined in BS EN 61508:2010. RIS-1530-PLT is being revised and at the request of the plant community the section on software will be aligned with the wording in the recently published EN 15746-2:2020 'Road-rail machines and associated equipment Part 2: General safety requirements', where the reference to SIL 2 in the current issue of RIS-1530-PLT will be avoided: '5.14.2.2 Software All safety related software and software systems shall be validated and documented. The software validation shall include checks that all foreseeable sequence of operations have been included and validated as set out in EN ISO 13849-1:2015, 4.6 and EN 61508:2010.' 1.2.2 now reads RIS-0745-CCS issue one applies to all systems used in railway applications, primarily infrastructure, trains, and their operation to deliver a service. G2.2.5 updated to refer to RIS's for OTP and PLT The Supply of Machinery (Safety) Regulations 2008 as amended by the 'Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019' applies to the safety-related software within control systems used by on-track machines and on-track plant. Requirements for control systems on these machines are set out in RIS-1530-PLT and RIS-1702-PLT.
15	8	1.2.3	How about off the shelf systems proven in service which are already in use? Is this standard retrospective.		11	NC			1.2.3 a) of the RIS states the requirements in this standard apply to 'the development of a generic product or system where the development is commissioned by a client, excluding systems for which there is no client distinct from the supplier (for example, generic products being developed by a supplier for the market)', therefore off-the-shelf systems are not in scope of the standard. This standard is not retrospective, the compliance requirements and dates have not been specified because these are the subject of internal procedures or contract conditions. Clause 1.3.1 states 'Compliance requirements and dates have not been specified because these are the subject of internal procedures or contract conditions.' RIS's are normally not expected to be retrospective, however it is up to the client organisation to decide when and how to apply.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
16	9	1.3	If OTM and OTP are in scope, should applications for these assets not come to NTH Plant if he/she were to mandate this RIS via NR/L2/RMVP/0200, 'Infrastructure Plant Manual'?		11	NC			The licence condition require compliance with applicable RISs if a licence holders plan to do something that does not comply with a RIS, they may identify and use an equally effective alternative measure to achieve the purpose of the RIS, after consultation with those who are likely to be affected. It is for Network Rail to decide whether RIS-0745-CCS should be added to the list of mandated standards in NR/L2/RMVP/0200.
17	10	G 2.1.1	Introduce the issue of hazards being introduced by the work being undertaken.	"Increased complexity and hazards arising from …"	2	DC		G 2.1.1	Updated as suggested
18	10	G 2.1.2	'Safety risk' is used regularly in the document.	Add to definitions section.	2	DC		Definitions	The following definitions are added: **safety risk** Risk related to human health or to the environment.
19	10	G 2.1.2	Isn't this also the case with software upgrades. Should we add this	Controlling the safety risk associated with software defects and upgrades involves an extension to the approaches used to control the safety risk associated with older technologies because the way in which software fails is different.	7	NC		G 2.1.2	Yes, the software defects could arise from new development or upgrades. The fundamental point is that software fails in different ways to other systems.
20	10	G 2.1.2	The text is clear but concludes stating that "Controlling the safety risk associated with software defects involves an extension to the approaches used to control the safety risk associated with older technologies because **the way in which software fails is different**." Actually the software is subject to systematic failures. Also the HW can have systematic failures	I suggest to explicitly mention the Software is subject to systematic failures and given that exhaustive testing is impossible to demonstrate the qualitative aspects are fundamental. This should connect very well with the next paragraph (G2.1.3)	10	NC			Agree that software is subject to systematic failures, and hardware can have systematic failures. However, the intention of section 2.1 is to include introductory material that aims for director level readers or others who have limited knowledge in specific technological terminologies. G 2.1.3 explains in detail the way of how software failure is different to hardware.
21	10	G 2.1.3	Additional software systems in additional equipment fitted to a vehicle can also render the software unreliable or extenuate a failure mode or vulnerability		7	NC		G 2.1.3	Agreed. This could be one of the failure modes captured by usage scenarios as required by 4.4.1.
22	10	G 2.1.5	Reference to 'expensive' encourages comparison to cost of safety.	"tends to use more resources ~~be more expensive~~"	2	DC		G 2.1.5	Updated as suggested
23	10	G 2.1.5	It may not always introduce a defect though. It could still work as intended and still remain compatible with the existing system but give an adverse outcome to the added system		7	NC		G 2.1.5	G 2.1.5 refers to the use of proven and rigorous techniques for software to introduce fewer defects, as it is generally not possible to confirm the behaviour of software-based systems by testing all possible combinations of input. Defect in software, is an error, mistake or inaccuracy that could result in a deviation from the intended performance or behaviour of the software. Giving an adverse outcome to the system should be clarified as a defect.
24	10	G 2.1.5	line 3 typo - 'using'		11	NC			No typo found; possible later version has fixed this.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
25	10	G 2.1.6	Reference is first made to the 'suite of software railway standards' but there are only explained in G 2.2.4.	Move the wording 'For brevity the standards BS …..software standards in this document' to G 2.1.6.	4	DC		G 2.1.6	The 'suite of railway software standards' was first briefly introduced in 1.4. G 2.1.6 revised to include these standards, with the further explanation retain in the section (2.2) regarding 'Relationship with existing standards and legislation' G 2.1.6 …. For each SIL, the suite of railway software standards (BS EN 50657:2017, BS EN 50128:2011, BS EN 50126-1:2017, and BS EN 50126-2:2017) provides guidance on the techniques to be used for controlling the risk in the design of safety-related software-based systems……
26	10	G 2.1.6	It states, "The extent to which functions of a system relate to safety is often expressed in terms of the SIL as set out in BS EN 61508 and associated standards..". 61508 is not railway specific. Why does this paragraph not reference EN 50126?	To reference EN 50126 instead of 61508.	10	NC			EN 50126 forms part of the railway sector specific application of BS EN 61508. G 2.1.6 introduced the term SIL which was originated from BS EN 61508. Relationship with existing standards and legislation are set out in the next section (2.2) of the document.
27	11	G 2.1.7		As such, safeguards to control the risk of hardware systems failing are also applied.	2	DC		G 2.1.7	Updated as suggested
28	11	G 2.1.7	Software based systems simply cannot function without hardware.	Amend to read 'Software-based systems operate on hardware and….'	4	DC		G 2.1.7	Updated:
29	11	G 2.1.9	Typo - 2nd sentence (erroneous 'it')	Amend to read '….leading to circumstances where what is specified is…'	4	DC		G 2.1.9	'it' removed.
30	12	G 2.2.2	The two standards contain very similar requirements but are applicable to different sorts of systems. A new standard is under development, prEN50716:2021, which is intended to supersede both BS EN 50128:2001 and BS EN 50657:2017 Is there a projected timescale for the production of this combined standard?	Documenting the proposed publication date for this standard may be useful	8	NC			BS EN 50716 is expected to be published on 22/06/2023 (according to the BSI website). However, the date is unconfirmed and is subject to change, therefore was not added to the reference.
31	12	G 2.2.4	BS EN 50128:2001 is listed, however the latest version of this standard is EN 50128:2011 + A2:2020. See also comment No.1	To amend with the latest EN 50128 version.	10	DC		G 2.2.4	Revised. The was an editorial error. It was intended to be BS EN 50128:2011, as listed in the reference section.
32	12	G 2.2.5	Noted		11	NC			G 2.2.5 has been added recognising the alternative way of conformance to the Supply of Machinery (Safety) Regulations 2008 as amended by the 'Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019'.
33	12	G 2.2.6	Current performance level requirements for OTM and OTP achieves this		11	NC			Noted. Assume this is against G2.2.6 in Draft1e. [G 2.2.6 The focus of this standard is on ensuring that the software within high integrity software-based railway systems does not cause hazards. This software will run on programmable electronic hardware, and it is equally important to ensure the hardware does not cause hazards.]

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
34	13	G 2.2.12 & G 2.2.13	Legislation requires the risk of the change to be managed. CSM RA is required by legislation to be used for significant projects although Network Rail require CSM RA to be used for non-significant change too – refer HSMS V6 section 3.1.2: "NRIL has adopted the principle that for any change (technical, operational and organisational) proposed, it applies the risk management framework defined in the CSM RA, including as its methods of safety verification."	Strengthen advice to use CSM RA to manage hazards arising from the changes being implemented and those that are existing.	2	DC		G 2.2.12 & G 2.2.13	G 2.2.12 & G 2.2.13 revised to strengthen the advice to use CSM RA. G 2.2.12 The CSM RA regulation sets out a harmonised risk management process used to assess the impact on safety from technical, operational and organisational changes to the railway system. Guidance on CSM RA is set out in GEGN8646. If the technical changes related to introducing the software or system are significant, as defined in article 4 of the CSM RA, then an independent assessment of the risk assessment is undertaken for CSM RA as set out in 3.6 of this document. G 2.2.13 Some of the requirements of this standard overlap with the requirements of legislation and of other standards, particularly the CSM RA. If the CSM RA applies to a project then it is efficient to align the safety assurance activities set out in the safety assurance strategy with those for the CSM RA.
35	13	G 2.2.13	States 'if the CSM RS applies to the project' – however, hazard management should always apply. This should be the theme throughout this document. The only decision to be made is whether or not to use CSM RA, if not mandated within the client organisation e.g., NR HSMS.		2	DC		G 2.2.12&13	Section 1.1 has been revised to Include reference to the legal requirements to manage risk. (See response to Comment No 5) G 2.2.12 & G 2.2.13 has been revised to strengthen the advice to use CSM RA. (see response to comment No 34)
36	14	G 2.3.5	Some client organisations may wish to procure engineering services rather than directly employing staff. They may wish to use this procured resource to carry out the client defined actions. This may be necessary because the client organisation is very small, or alternatively it may be a choice taken within an organisation.	Amend the clause to confirm that it is possible to use procured resources, but that the responsibility remains with the client. In addition G 3.2.1.6 could be amended by adding it is possible to close a resource gap by procuring suitable external resource.	3	NC		G 2.3.5	Clause G 2.3.5 explains the two different phrases used in the RIS 'The Client shall' and "The Client shall require that" to accommodate the different management arrangement. Significant considerations were given so that only minimum set of requirements are using 'the client shall'. It is however up to the client organisation of how to make competence resources available for any projects.
37	15	G 2.4.3	2nd sentence - Wording could be improved.	Amend to read 'Requirements for client action during…'	4	DC		G 2.4.3	Updated
38	15	G 2.4.4	1st sentence - Wording could be improved.	Amend to read '….specific requirements for client action during…'	4	DC		G 2.4.4	Updated
39	15	G 2.4.5	1st sentence - Wording could be improved.	Amend to read '….specific requirements for client action during…'	4	DC		G 2.4.5	Updated
40	15	G 2.4.6	1st sentence - Wording could be improved.	Amend to read '….specific requirements for client action during…'	4	DC		G 2.4.6	Updated

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
41	16	G 2.5.1	Note: generally cyber-security of a system is concerned with preventing unauthorised people accessing confidential data on it or causing it to stop working or causing it to do something unwanted." It is understood why this note has been added for the "Unauthorised access" hazard within the table, however it is felt that the comment can be misleading. Whilst cyber-security does cover preventing unauthorised access, it also could cover events that occur due to personnel with authorised access making an error or acting with malicious intent. I feel having this statement within a RIS could lead to people regarding cyber-security as only being related to unauthorised access.	The removal of the "generally" is proposed. A suggestion on the wording of this note is: "One area of cyber-security is the prevention of unauthorised people accessing…"	6	DC		G 2.5.1	The note in the table has been revised accordingly. Note: one area of cyber-security is the prevention of unauthorised people accessing confidential data on it or causing it to stop working or causing it to do something unwanted.
42	17	G 2.6.3	Figure 2, General Blue box, 3.4 Convene stage gate reviews can not be delegated. I believe some clients will not be able to competently do this.		11	NC			Assume it is now against G 2.6.4 in Draft1f Significant considerations were given so that only minimum set of requirements are using 'the client shall'. It is essential for a client to convene stage gate reviews as part of the safety management. It is up to the client organisation of how to make competence resources available for any projects. If a client is a licences holder, the licence condition require compliance with applicable RISs. if a licence holders plan to do something that does not comply with a RIS, they may identify and use an equally effective alternative measure to achieve the purpose of the RIS, after consultation with those who are likely to be affected. Any rail industry company that is not a licence holder can choose to adopt all or part of a RIS through company procedures or contract conditions
43	17	G 2.6.4	Paragraph doesn't read correctly. Should there be a full stop between "controlled" and "That"?		7	NC		G 2.6.4	The full stop is need. 'That assurance' at the start of the second sentence refer to the assurance that safety risk has been effective controlled referenced in the first sentence.
44	19	3.1.1	System Assurance Strategy – could be linked to CSM RA to start baking in hazard management using a defined process.		2	NC		3.1.1	The intention of this standard is to identify the activities for client organisations to undertake as part of the safety management of high integrity software-based systems. The link to CSM RA has been strengthened in section 1.1 and Part 2 of the document.
45	19	3.1.1 .1	The safety assurance strategy is very generic and not software specific. A more detailed SW specific list would support better the organisations	To be more SW specific.	10	NC			The intention for the RIS is to identify the activities for the role of a client as part of the safety management of the high integrity software-based systems. The requirements in this standard support compliance with the suite of railway software standards but do not replace or overrule any part of them. The high integrity software-based systems includes both software and hardware.
46	20	G 3.1.1.11	Typo – 2nd sentence	Amend to read 'alteration'	4	DC		G 3.1.1.11	Amended

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
47	20	G3.1.1.1	Bullet a) states: “a maximum tolerable rate for hazard occurrence”. Software is subject of systematic failures. This is not applicable in the SW context.	Please make it SW specific. Please also consider aligning with the new EN 50126, the terminology adopted seems to be related to the old version of the standard. THR and SIL Allocation are outside the scope of the SW as per EN50128 and EN50657 (see also 3.1.3.1 bullet b)).	10	NC			Assume the comment is against G 3.1.1.4. The high integrity software-based systems includes both software and hardware. G 3.1.1.4 provides guidance for various ways of defining target for safety. The guidance does not specify which one to use. 3.1.3.1 b) refer ‘the SIL determination for each safety function’ for safety assurance records. This is necessary for both software and hardware elements. Clause 4.3 of BS EN50128 states ‘The required software safety integrity level shall be decided and assessed at system level, on the basis of the system safety integrity level and the level of risk associated with the use of the software in the system.’
48	20	G3.1.1.5	This clause makes an important point that would usefully be introduced in the opening paragraphs of the document.		2	NC		G3.1.1.5	Section 1.1 has been revised to Include reference to the legal requirements to manage risk. (see response to comment No 5)
49	21	3.1.2	This is already determined for OTM and OTP hence reason to refer to existing RIS that cover them G 3.1.2.4; G 3.1.2.5 & G 3.1.2.6		11	NC			Noted. It would be efficient to align the safety assurance activities set out in this standard with those for other safety and hazard management processes.
50	21	G 3.1.2.2		“in a way that will efficiently yield the greatest …..”	2	DC		G3.1.2.2	Updated.
51	22	G 3.1.2.12	States ‘if the CSM RS applies to the project’ – however, hazard management should always apply. This should be the theme throughout this document. The only decision to be made is whether or not to use CSM RA, if not mandated within the client organisation e.g., NR HSMS.		2	NC		G 3.1.2.12	See response to comments No 35.
52	22 & 43	3.1.3.1 & 4.5.1.1	It is unclear what level of requirements should be recorded / managed here. For example if procuring an ETCS system, a client would probably specify at the level of ERA standards. However those standards contain many requirements, such as those defining how to calculate the braking curves. An ETCS supplier would then probably take the ERA standard requirements and further develop them to produce software requirements.	Clarify the requirement level that should be managed by the client. Is it acceptable to manage to the top level in the example given if anything below that is covered by a Software Assessment Report from an Assessor?	3	NC		3.1.3.1 & 4.5.1.1	Clause 3.1.3.1 referred to safety function of the system, it is at the system and functional level. The important aspect of this requirement is to establish the safety assurance records and maintain traceability. This requirement is in case of 'The client shall require that [some defined action is taken]', as defined in G 2.3.5, which means ‘it is possible for the client organisation to delegate the defined action to another organisation provided that it retains accountability for the performance of this action.’
53	23	G 3.2.1.5	It states: “Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017 and Annex B of BS EN 50128:2001 which might be relevant if the client organisation is carrying out tasks associated with these roles.”	Please add EN 50657 Annex B	10	DC		G 3.2.1.5	Added BS EN 50657:2017 Annex B. G 3.2.1.5 now reads: Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017, Annex B of BS EN 50128:2011 and Annex B of BS EN 50657:2017 which might be relevant if the client organisation is carrying out tasks associated with these roles.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
54	23	3.2.2.1	To enable the supplier to accurately cost the scope of this work, the client should provide its own assurance strategy for the project.	Recommend that there is an additional point that the client should distribute its own assurance strategy to the supplier.	9	NC			Section 3.2.2 includes requirements on supply selection. The requirement on client to place contract terms on suppliers engaged in safety-related activities, for these activities assigned to them in the safety assurance strategy is set out in 3.3.1.1a). The safety assurance strategy is maintained throughout the life of the system, it is expected all organisations involved in the project would need to share information to support this strategy.
55	23	G 3.2.2.4	Specific requirements for the SW Independent assessor are detailed in EN 50128 and EN 50657	Please add a reference to SW Standards	10	DC		G 3.2.2.4	Replaced the reference to BS EN 50126-2:2017 with the suite of railway software standards. G 3.2.2.4 now reads: If the project includes an Independent Safety Assessors (ISA) then the suite of railway software standards places a specific responsibility on them for the evaluation of the competency of the project staff and organisation.
56	24	3.3	It should be made clear that it is the client's responsibility to ensure that they have sufficient contractual arrangements to enforce this RIS.	Recommend adding the following guidance: 'The client can effectively apply the safety assurance strategy only if it has contractual arrangements in place to do so. This would should include explicit reference to this RIS and the suite of standards'	9	DC		G 3.3.1.2	The safety assurance strategy (3.1.1) requires the definition and justification of how the requirements of this standard are being applied on the project. The requirement on contract terms (3.3.1) uses the phrase "the client shall…" so it is clear it is the client's responsibility to ensure contract terms are in place for relevant activities (3.3.1.1a) and process/standards (3.3.1.1b) identified in the safety assurance strategy. The suite of standards is induced in 3.3.1.1 d). Additional rationale added to start of G 3.3.1.2: The client can effectively apply the safety assurance strategy only if it has contractual arrangements in place to do so. …
57	24	3.3	This is not a technical requirement, I suggest wording be relaxed if it is to be left in this technical standard. Ultimately the organisation paying would determine how they manage their contracts		11	NC			The contract terms placed on suppliers supports the control of safety risk and the provision of evidence that supports the safety assurance strategy and other standards identified in the strategy. If a client is a licences holder, the licence condition require compliance with applicable RIS's. if a licence holders plan to do something that does not comply with a RIS, they may identify and use an equally effective alternative measure to achieve the purpose of the RIS, after consultation with those who are likely to be affected. Any rail industry company that is not a licence holder can choose to adopt all or part of a RIS through company procedures or contract conditions
58	24	3.3.1.1	It would be beneficial if the clients own assurance strategy for the project was contracted too.	Recommend adding the client's safety assurance strategy to the contract terms list.	9	NC			The relevant activities assigned to the supplier and process/standards identified in the safety assurance strategy has already been included in the contract term list (3.3.1.1a and 3.3.1.1b).

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
59	24	3.3.1.1	Similar to point 3 above, the list should include clear reference to the RIS and the suite of standards.	Recommend the list includes a reference to this RIS.	9	NC			The safety assurance strategy (3.1.1) defines and justifies how the requirements of this standard are being applied on the project. The relevant activities assigned to the supplier and process/standards identified in the safety assurance strategy has already been included in the contract term list ((3.3.1.1a and 3.3.1.1b). In general. a licence holder is only required to comply with RISs (or parts of RISs) that are applicable to its licenced activities. The licence holder does not have to comply with a RIS if, following consultation, it has adopted and is complying with an equally effective measure. Any rail industry company that is not a licence holder can choose to adopt all or part of a RIS through company procedures or contract conditions.
60	24	G 3.2.2.6	It states: “Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017 and Annex B of BS EN 50128:2001”	50128:2001 should be replaced with the latest version of this standard and EN 50657 should be added.	10	DC		G 3.2.2.6	Added BS EN 50657:2017 Annex B. G 3.2.2.6 now reads: Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017, Annex B of BS EN 50128:2011 and Annex B of BS EN 50657:2017.
61	26	3.5	This section should also refer to hazard management and hazards arising from the change being implemented. Often these changes require further hazard identification work focusing on the change to scope or programme that is being implemented.		2	DC		G 3.5.1.6 e)	This section is about change control that is applicable throughout the lifecycle. Without change control, safety activities might not be carried out on a consistent version of the design Requirement in 4.3.2 (now 4.3.3) ‘Ongoing risk analysis and evaluation’ refers to need for the client to require that ‘hazard record is produced to record the results of system hazard identification and risk assessment and is kept up-to-date as relevant new information becomes available and changes occur.’ G 3.5.1.6 e) has been updated as follows: G 3.5.1.6 e) Change control Once a configuration item has been included within a baseline, any proposed change to it is fully assessed and approved before the change is made and tracked to completion. The assessment of the change includes safety analysis of the impact of the change…
62	26	3.5	This would aid the PA process and reduce the need for relevant PA certs to be updated every time a change is made to software. Current wording for PA certs was developed when the railway was hardware intensive and is not suitable for software systems. This section or standard can help amendment of relevant PA requirement for significant changes to be reflected on PA for all assets(including software).		11	NC			Noted, this comment is about Network Rail's internal Product Acceptance process.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
63	26	3.5.1.1	Some safety systems (eg. ASDO, TSRs) rely on databases to function. While changing the database does not impact the actual software code it can affect the safe operation of the system. Some database changes are required at short notice, or even immediately in the case of an ESR/TSR. Changes to such databases need special consideration given the immediate / short term nature of the change.	Add a requirement for the client to ensure a robust process is in place for managing changes to databases, including the validation & verification element. For example in an ASDO system: if data for a single platform is modified, can a process be put in place to ensure that no other data was erroneously changed in the database? Propose a test at the platform in question before rollout of the new database.	3	NC		3.5.1.1	Noted and agreed the need for process in place for managing changes to data. The term 'configuration data' is used in the standard referring to data that defines the environment in which the system will run and its desired behaviour. Clause 1.2.4 states 'It is important that the safeguards to assure that the software is correct are extended to cover the configuration data as well.' The existing requirement in 3.5.1.1 covers the need for process are established for configuration management of the system, its applications, its components and associated documentation and data, including arrangement for controlling change The 'configuration data' is listed as one of the typical 'configuration items' in Clause G 3.5.1.4, which is subject to change control as set out in G 3.5.1.6 e).
64	26	G 3.5.1.4	Focus the project team on the proposed changes by altering the wording as suggested.	Only the ~~key~~ effected items	2	NC		G 3.5.1.3	Assume this is for G3.5.1.3. Change control and configuration management applies to more than just the items being modified or effected.
65	28	G3.5.1.10	Not sure this clause is relevant – would all users of this RIS have access to NR/SE/001 anyway?		7	DC		G 3.5.1.10	This was included to acknowledge contribution of material from that NR document. Clause revised to refer to further guidance instead, so that the reference is only for readers wishes to get more information. Further guidance is set out in Network Rail System Engineering handbook (NR/SE/001).
66	29	3.6	How about when the client is simply buying a compliant off the shelf product? In this case they will have a product and a certificate - what would the client be assessing or assuring? Most software modules with safety critical function are either bought or certificed by a specialist, what would be assessed or assured in this scenario without duplicating initial compliance and purchase scrutiny activitiy by the client (Converter or Vehicle Owner?)		11	NC			1.2.3 a) of the RIS states the requirements in this standard apply to 'the development of a generic product or system where the development is commissioned by a client, excluding systems for which there is no client distinct from the supplier (for example, generic products being developed by a supplier for the market), therefore off-the-shelf systems are not in scope of the standard. 4.5.2 of the RIS requires safety justifications are provided for pre-existing subsystems or software elements. The suite of railway software standards also contains guidance relating to re-use.
67	30	Part 4	Is it the aim of this part of the RIS to provide clarity to the clients activity? Do the authors believe BS EN 50126-1:2017 is not clear enough for clients to interpret it on their own? This Part will not apply to OTM and OTP if reference is made to existing standards that adequately fulfills the purpose of this RIS. Section comment made on clause 1.2.2.		11	NC			The RAIB report on Cambrian Coastline incident on 20 October 2017 highlights the need to for the rail industry to '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 RIS has been developed in response to the RAIB report. This part identifies specific requirements placed on client to act on during specific phases of the system lifecycle. If safety assurance activities have been carried adequately following existing standards, it would be efficient to align the safety assurance activities set out in this standard with those for other safety and hazard management processes, so that there are no duplicated efforts.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
68	30	G 4.1.1	Typo – 2nd sentence	Amend to read '…system lifecycle is described…'	4	DC		G 4.1.1	Done
69	32	Table 2	Typo – 4.5 'Relevant client's activities' box	Amend to read 'Engage with the decisions taken…'	4	DC		Table 2	Done
70	32	Table 2	Typo – 4.8 'Relevant client's activities' box	Amend to read 'Liaise with stakeholders inside and outside the client's organisation…'…'	4	DC		Table 2	Amended
71	33	G 4.2.1.3	1st sentence – Wording can be improved	Amend to read 'The deliverables identified in section 7.3.3 of BS EN 50126-1:2017 are a system…..'	4	DC		G 4.2.1.3	Amended.
72	33	G 4.2.1.3	It states: "The deliverables identified by BS EN 50126-1:2017 (7.3.3) are a system definition, a safety plan, and a RAM plan. Guidance on these deliverables and the activities needed to produce them is provided in the suite of railway software standards" Please note these documents are not deliverable of any specific SW Standard such us EN 50128 EN 50657. This creates an inconsistency with the Railway standards	Please consider amending this section to list planning documents requested by SW Standards, e.g. SQAP (SW Quality Assurance Plan, SW verification and Validation Plan, SW Configuration Management Plan, etc..	10	NC			The RIS is intended for high integrity software-based systems which include both software and hardware, and it aligns with the lifecycle and deliverables from BS EN 50126-2:2017. The planning documents as listed are software specific and already covered by specific software standards such as BS EN 50128. These documents would be needed for the verification and validation of the software design, where the client involvement is set out as a general requirement in 3.4 of the RIS to approve phased deliverables.
73	33	4.2.2.1 a)	This statement contradicts G 2.4.6 which states Phase 12 (Decommissioning) is out of scope of this standard.	Please clarify.	4	DC		G 2.4.6 4.2.2.1 a)	There is no contradiction: G.2.4.6 states that this standard puts no requirement for client action in Phase 12; Clause 4.2.2.1 requires the development of lifecycle concepts in Phase 2 which demands the consideration of the approach to lifecycle phases 8, 9, 11 and 12. G 2.4.6 has been revised to clarify: This standard contains no specific requirements for the client to act during Phase 12 because the activities during that phase are considered to be out of scope. However, it is necessary to consider how the decommissioning phase impacts the system design, and this is covered by the production of lifecycle concepts during Phase 2.
74	36	4.3.1	Include requirement to undertake risk analysis and evaluation for potential failure modes.		2	NC		4.3.2	The requirement in 4.3.1 (now 4.3.2) refers to the need to consider 'the full scope of system functions, interfaces, user roles, lifecycle concepts, and usage scenarios' Potential failure modes are included in 'usage scenarios', as set out in 4.4.1 of the standard.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
75	38	G 4.3.1.16	Place this clause at the beginning of 4.3 since the whole of 4.3 explains fundamentals of hazard management that should be implemented using CSM RA on the mainline railway network. CSM RA provides a framework for risk analysis and evaluation that provides for change to be integrated into the operational network or other projects/railway organisations. It also allows migration of a project that begins with a limited scope that develops into a more complex project. . By placing the contents of G 4.3.1.16 at the end of section 4.3, the reader may conclude that CSM RA is additional to the hazard management previously described in section 4.3. This may result in duplicate work, un-necessary expenditure, and confusion.	Reiterate legislation in UK mandates CSM RA to be used for managing hazards throughout the project lifecycle for all significant changes to mainline railway. This standard, RIS 0745-CCS, is aimed at managing risk in connection with technology which, by its' very nature, is novel, complex and safety critical. Any change to such infrastructure is nearly always significant under the CSM regulations. On mainline railway, CSM RA should also be applied to non-significant changes when required by the owner, e.g. Network Rail, although an independent assessment body is not necessarily required.	2	DC		G 4.3.1.1 G 4.3.1.2	Guidance G 4.3.1.16 moved to the beginning of 4.3 and reworded: Compliance with CSM RA is required in GB for duty holders through the safety management system under ROGS. Further guidance on CSM RA is provided in GEGN8646. There might be overlap between activities undertaken to meet the requirements of this standard and those needed by CSM RA. it is efficient to align the safety assurance activities set out in the safety assurance strategy with those for the CSM RA.
76	38	G 4.3.2.1	Include changes to scope and programme require the system definition to be updated and the hazard identification to be revisited to consider the changes. Such changes may result in unintended interfaces or operation situations, e.g. interim or temporary operating methods and practices.		2	NC		G 4.3.3.1	Agreed. The hazard identification to be revisited if change occurs is indicated in G 4.3.2.1 (now 4.3.3.1). The safety assurance strategy set out in 3.1.1 that is maintained through the lifecycle of the system, includes 'a) the description of the system in terms of its functions, users, and interfaced external systems;' The strategy would need to be updated if there are any changes to the scope of a project. These changes would also need to controlled according to the change control process in set out in 3.5.
77	39	4.3.3.1	Wording can be improved	Amend to read 'The client shall require that a register of safety -related conditions on the application of the system is prepared (known as the register of safety-related application conditions)	4	DC		4.3.4.1	Existing G 4.3.3.7 (now G 4.3.4.1) already provides guidance on safety-related application conditions. 4.3.3.1 (now 4.3.4.1) revised: The client shall require that a register of safety-related conditions on the application of the system is prepared.
78	39	4.3.3.2	Wording can be improved	The client shall require that the conditions in the register of safety-related application conditions are respected at all times.'	4	NC		4.3.4.2	It is not necessary to include 'at all time' for 4.3.3.2 (now 4.3.4.2).
79	40	G 4.4.1.3	Should include normal operating environment. For example, operating in temperature extremes or exposure to weather in the components usual location		7	NC		G 4.4.1.3	'Normal operation' was included in G 4.4.1.3 Also, the exposure to weather etc relates more to specific hardware failure, which are normally covered by standards relating to Reliability, Availability and Maintainability, as shown in Table 1 in RIS-0745-CCS.
80	40	Between G 4.4.1.5 and G 4.4.1.6	In order to ram home the need for specific guidance on incident investigation, a new clause should be added here.	Add 'Incident investigation covers the provision of facilities to retain system data to support the identification of root cause in the event of an occurrence that needs to be investigated'	4	DC		G 4.4.1.6	New guidance added as G 4.4.1.6: Incident investigation covers the provision of facilities to retain system data to support the identification of root cause of adverse events.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
81	41	G 4.4.1.12	1st sentence, wording could be improved.	Amend to read '….those key safety functions, whose correct behaviour….'	4	DC		G 4.4.1.10	Assume the comment is against G 4.4.1.10 The process of checking system requirements against the usage scenarios will allow the identification of those key safety functions, whose correct behaviour…
82	42	G 4.4.2.9	Further clarification to be added.	Add 3rd sentence 'However, it is important that the software-based system remains safe with data values that are outside 'normal bounds' and this should be confirmed'	4	DC		G 4.4.2.9	Software-based systems are often highly configurable and include a significant amount of configuration data which define the environment the system is intended to operate in as well as its desired behaviour. It is rarely possible to demonstrate that a system will work for every combination of configuration data values. However, it is important that the software-based system remains safe with data values that are outside 'normal bounds' and mitigations are in place for safety risks associated with data defects.
83	42	G 4.4.3.6	[Minor] "Integration finds problems at interfaces between systems." Is it "Integration" that finds problems at interfaces, or would it be the next step "System Validation"? I assume that the risks associated with interconnected systems are to be highlighted in stage 3 Risk Analysis and Evaluation? Therefore is the purpose of the sentence trying to guide the client to think about the tests that can be performed to check if there are any problems at the interfaces?	Is the sentence required? – proposed it is deleted. Or "Integration considers problems at interfaces between systems"	6	DC		G 4.4.3.7	A new paragraph should have started from 'Integration finds ...'. the sentence also revised as suggested. Integration considers problems at interfaces between systems. If a system has interfaces with many external systems and everything is put together at the same time, problems can be very difficult to find….
84	44	4.5.2	Pre-existing SW is already regulated by specific requirement of EN50128 and EN50657.	Please align with SW Standards.	10	NC			Agreed pre-existing software already covered by BS EN 50128:2011 and Annex B of BS EN 50657:2017. It is not the intention of the RIS to repeat what has been adequately covered by other standards, rather to concentrate on identifying activities for client to act on.
85	44	G. 4.5.2.2	A key aspect missing from this list are any hardware differences	Add f) evidence that the hardware being used to run the software element is identical to the pre-existing use case..	4	NC		G. 4.5.2.2	The requirement does not preclude hardware element. The wording in 4.5.2.2 referring 'the subsystem or software element under consideration' includes hardware. In case of a pre-existing software element is proposed, it is likely that the hardware to run the software is different, safety justification need to be provided for running the software element on other hardware, and/or within other software subsystems. In case of pre-existing subsystem (with both hardware and software), the hardware being used to run the software element could be identical, however safety justification is required for the use of the subsystem as a whole.
86	44	G 4.5.2.3	Wording can be improved	Amend to read 'If this analysis was not carried out it might…..	4	DC		G 4.5.2.3	Amended: If this analysis was not carried out it might be discovered later that the subsystem or software requirements could cause a hazard.

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
87	49	G 4.6.10	The use of operational mitigations in the case of a pre-commissioning defect would not be a course of action that I would support lightly.	This should be considered as a last resort and only consider when the source of the defect has been identified. A key issue in the past has been putting a system into use restricts the access to investigate and rectify the underlying problem thus further extending the defect period and potentially the cost impact.	1	DC		G 4.6.10	G 4.6.10 Guidance has been revised: Defects identified during system validation are often expensive to rectify. The client might choose to put in place restrictions on the use of the system to mitigate these defects and allow the system to continue into operation. These restrictions might be permanent, or temporary until the fault is fixed and the validation activity repeated. Operational mitigations are used as a last resort and are only considered when the source of the defect has been identified, as putting system into use might restrict the access to investigate and rectify the underlying problem thus further extending the defect period and potentially the cost impact.
88	50	4.8	The scenario described in appendix G.B.2.9 where a failure of the type that caused an incident of a similar nature had been identified with a related system in operation on another administration.	There should be some guidance that it is desirable to have in place a process where such defects are shared with interested parties. Realistically the onus needs to be on the supplier to identify this situation as only they have an overview where the equipment concerned has been deployed.	1	NC			Clause 3.3.1.1.f requires the client to place contract terms on suppliers for provision of incident information through-life.
89	50	4.8.1	Lifecycle requirements	Consider adding as guidance: Ensure that any activities put in place to satisfy an SRAC are still in place and being executed.	3	DC		4.8.1.6	G 4.8.1.6 revised to include activities in place for SRAC Activities planned and carried out under this requirement will include those identified in the maintenance lifecycle concept (4.2.2 of this document) and related usage scenarios (4.4.1 of this document). Activities to satisfy SRACs will remain in place. These activities will often be an integral part of the business-as-usual processes for the system's operator and maintainer.
90	50	G 4.8.1.2	Typo – 2nd sentence	Amend to read '…impact safe operation is identified quickly.'	4	DC		G 4.8.1.2	'are' replaced with 'is'
91	51	G 4.8.3.4	It is already accepted nomenclature on the railway for the D in DRACAS to represent 'Defect'	Amend to read '….scope of a Defect Recording Analysis….'	4	DC		G 4.8.3.4	Updated.
92	54	G A.4.2	Further clarification to be added.	Add 'Has the system been confirmed to react in a safe manner with data values that are outside 'normal bounds.'	4	DC		G A.4.2j)	The list in G A.4.2 relates to 4.4.1 'User scenarios' that need to be consider when looking for missing system requirements. The following has been added: j) Have requirements been defined to deal with defect data or data values that are outside boundaries?
93	55	G A.5.2	A key aspect missing from this list are any hardware differences	Add 'Is the pre-existing software element running on the same hardware as previously deployed?'	4	NC		G A.5.2	The list relates to pre-existing subsystems or software elements. See response to No 85.
94	56	G A.7.2 – h)	Missing word	Amend to read ' …which could create the potential for an incident'	4	DC		G A.7.2 – h)	Added 'the' before 'potential'
95	59	G B.2.9	Typo	Amend to read '… but had the chance been implemented then…'	4			G B.2.9	Replaced 'be' with 'been'

No	Page	Clause	Comment	Suggestion	By	Way forward	Page	Clause	Response
96	59	B.3 Railway power disruption	Please remove this example. It incorrectly gives the impression that this is a greater than SIL 0 system. It isn't. Please also review BS EN 50562. This states *"A SIL-allocation for functions of electric traction systems is not required within the framework of EN 50562."*	Delete	5	DC		B.3 Railway power disruption	Deleted.
97	61	Table 5	Typo (Why are the [] here?)	Amend to read '….Change Control Processes'	4	DC			Section B.3 deleted (see response to No 96)
98	62	Table 6	Typo (Why are the [] here?)	Amend to read '….Change Control Processes'	4	DC		Table 5	Removed bracket in the table, changed the subtitle in 3.5.1 to 'Change control processes'
99	66	G C.1.3	Typo	Amend to read '…scenarios that cover all modes….'	4	DC		G C.1.3	Done.
100	67	G C3.1.1. c)	Suspected wording error. Not clear why 'Inconsistent or incomplete specifications of any of the interfaces could lead to failures' is presented here.	Please clarify where this statement should appear in the document.	4	DC		G C3.1.1.2	This statement should appear as a separate paragraph after G C.3.1.1 Updated.
101	69	DRACAS Definition	It is already accepted nomenclature on the railway for the D in DRACAS to represent 'Defect'	Amend to read 'Defect Recording Analysis….'	4	DC		DRACAS Definition	Definition updated.
102	73		Please remove reference to GLRT1210 and BS EN 50163:2004. Neither of these standards have any SIL or software requirement	Delete	5	DC			The two documents were only referenced from B.3. Removed.
103	73		BS EN 61508 missing from refences	Add missing reference	5	DC		References	Added: BS EN 61508-1:2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems.
104	73	RSSB 2022	This is cited as an RSSB document. There seems to be something missing from the definition.	Please clarify.	4	DC		RSSB, 2021	This information on A400M incident summary, and is a report dated 2021, and is downloadable from a RSSB web page. Reference revised: RSSB, 2021 A400M disaster 2015, RSSB, 2021 [Online]. Available from www.rssb.co.uk [Accessed 7 Jan 2022]