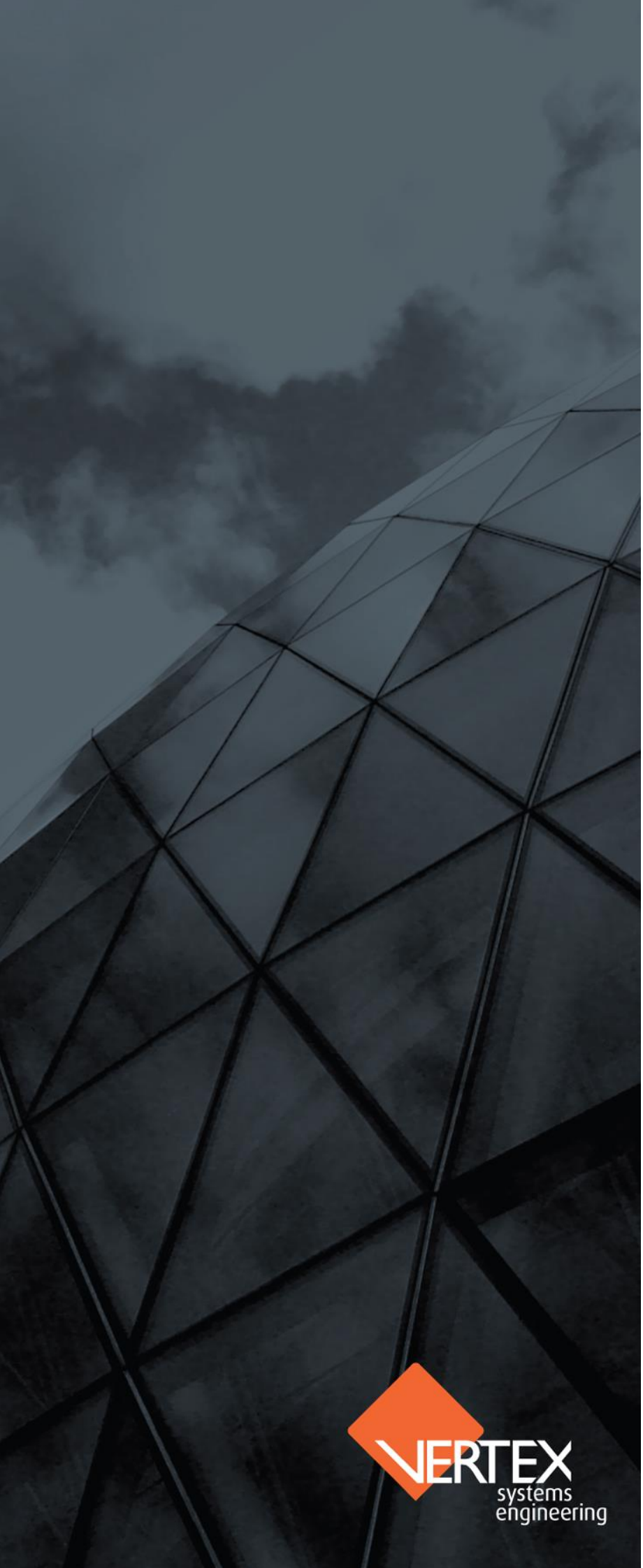

A Report for
Network Rail
from
Vertex Systems Engineering

Version 1.0
10th February 2015

Crossrail ETCS Enhanced TPWS - HAZID workshop with FGW Addendum

Controlled Copy No:	**UN**

APPROVAL				
Version	Date	Compiled by	Reviewed by	Authorised by
1.0	10th February 2015	Siraj Ali	S.Hebbes	M Elmes
Vertex Systems Engineering File Ref: 007.396				

DISTRIBUTION			
Name	Controlled Doc. No.	From (version)	To (version)
1 copy of document each to:-			
Eddy Schwartz, Network Rail	N/A	1.0	C
Sivapalan Sivendran, Network Rail	N/A	1.0	C
Ian Watson, Network Rail	N/A	1.0	C
Vertex SE File	N/A	0.1	C
Uncontrolled copies distributed as required			
C = Current version			

AMENDMENT HISTORY		
Version	Sections	Amendment Details
1.0	All	First Issue

Original held by Vertex Systems Engineering at
Soane Point, 6-8 Market Place, Reading, RG1 2EG
Tel: +44 (0)1189 255 462, Fax: +44 (0)1189 255 888

Table of Contents

1 Introduction and Purpose

This paper is an addendum to the previously issued Final Option Selection Report (Ref 1) and supporting Hazard Log which considers the impact of possible delays to ERTMS implementation on the Great Western mainline between 0m and 12m.

This paper provides a summary of a Workshop held with First Great Western (ToC) representation on the 8th of January 2015 and subsequent addition hazard analysis/review of the final selected option.

The Workshop was convened at the request of First Great Western, who wished to review the selected option and its associated Hazard Log in light of their operational experience on the route and to ensure that ATP functionality had been properly base-lined.

In addition to the Workshop, this report also contains extended information about the proposed method of integration of TPWS into the signalling system and how this would behave under TPWS failure.

2 Agenda

At the commencement of the workshop the group, see Appendix A, agreed a two part agenda consisting;

Section No	Section Title	Location
1	Review of SDG scheme design for Plan B TPWS works on 0-12 miles.	Network Rail Offices, Davidson House, Forbury Square, Reading, RG1 3EU
	Update on ORR Exemption Application Letter	
	Status and Feasibility of Current and Contingency Crossrail works	
2	HAZID and controls reviewed and updated	Vertex Offices, Soane Point, 6-8 Market Place, Reading, RG1 2EG

3 Workshop Findings

3.1 Option Lifespan and Future Risk Optimisation

The Option Selection Report (Ref 1) stated that TPWS equipment may have to be fitted for up to 25 years due to the cost/difficulties of removal once migration to ETCS has been achieved. The following was discussed:

1) Staff having to maintain or repair the additional equipment are therefore exposed to associated hazards when working on the track
2) Performance issues could occur if the equipment fails

The first item is partially covered in paragraph 24 of the exemption application letter in particular Railway Safety (Miscellaneous Provisions) Regulation 1997 (Ref 3).

It was concluded that as the signalling system migrates to ETCS Level 2, Network Rail will be required to review the risk profile of maintaining/not maintaining and removing/retaining the installed TPWS equipment. This would be based on the rolling stock population, number of train moves under each type of protection system (TPWS vs ATP vs ETCS) and the optimal balance between protection of passengers and protection of workers required to maintain the equipment. Should the risk profile justify it, the additional TPWS equipment should be removed prior to the 25 year service life.

3.2 Update of Hazard Log

The HAZID log, Appendix B, was updated including comments from FGW and additional hazards were identified relating to ATP functions that cannot be provided by TPWS. None of the additional hazards were considered to be of sufficient gravity to affect the Option selection and Option 3 remained the preferred solution.

Additional control measures were identified and added to the Hazard Log. These principally pertain to driver training.

3.3 TPWS Fault Reporting

The issue of the proposed method of integration of additional TPWS equipment into the control system and the consequences on the signaller's display under TPWS failure conditions was discussed by the group.

To avoid costly data changes, the additional TPWS equipment will be integrated such that failures will be indicated to the signaller as 'lamp out' failures ("Method 3" under Train Protection and Warning System (TPWS) Signalling Interface Design Requirements (Ref 4)).

The use of Method 3 will provide all the necessary controls utilising current industry practice to protect the driver and signaller. In failure conditions, the fault will appear as a signal failure and the train will be held at the signal in rear. Consequently the train will not be able to move up to the signal that has the failed TPWS at normal line speed (whilst under braking). The signaller will apply the regulation controls for a failed signal, and inform control. They in turn will arrange for the reported failure to be rectified by the fault team. The fault team will determine the root cause using existing methods for interrogating the interlocking and at site for the TPWS equipment.

As is the current situation, due to the high level of moves carried out in the area and the layout, it is likely that the signaller will be made aware by drivers that they can see the signal ahead is showing a red aspect (lit), and therefore know it is likely a failed TPWS. This is captured in Hazard ID 08.

Where the TPWS fitted signal is preceded by a second TPWS fitted signal, an associated 'ripple effect' has also been identified. In this case, when the signal is replaced to danger by the Signaller, all of the TPWS fitted signals on the approach to the signal replaced, will be replaced to danger in sequence. Again this effect is not considered to be dangerous but can lead to Category B SPADs, however recommendations for eliminating the possible adverse effects of this timing error and the ripple effect are specified in (Ref 4).

Therefore, the benefit of method 3 is that no special controls are required or changes to interlocking. The disbenefit is it will take a greater time to determine if the failure is or is not TPWS, however this situation is present at all other Method 3 locations.

Ian Brighthouse (FGW) agreed that existing driver and signaller operation arrangements for degraded mode procedures are adequate for the final selected Option (No. 3). The low level of recorded TPWS failures in the area also indicates (on the basis the same type of equipment is deployed) that the number of interventions by maintenance to address failure will also be low.

4 Conclusion

Following further analysis of the Hazards and discussion of the proposed Option, the group were unanimous that the proposed solution was suitable for presentation to the ORR with FGW's support.

It was noted that the benefits to non-ATP traffic of the enhanced TPWS solution should be brought to the fore. As the railway signalling system and rolling stock evolves towards ERTMS operation, the balance of benefit of additional TPWS installations versus operational risk (due to failure) and safety risk (due to on-track maintenance activities) will need to be reviewed to ensure that risks remain minimised.

FGW agreed that existing driver and signaller operation arrangements for degraded mode procedures are adequate for the final selected Option (No. 3) due to the low level of TPWS failures anticipated.

5 References

1) Crossrail ETCS Final Option Selection, v1.3 10th February 2015, Vertex Systems Engineering
2) ETCS "Plan B" Study 122271ISD-ASS-ESG-0000001. Version: 1.0; 27th June 2014
3) ORR Exemption Application Letter WAA1A-ESG-COT-NCA-000002 A01 22 December 2014
4) Train Protection and Warning System (TPWS) Signalling Interface Design Requirements (formerly RT/E/S/10133). Ref NR/SP/SIG/10133 Issue 3. April 2004

Appendix A – Workshop Attendees

Name	Company
Richard Evans	Network Rail
Dave Milburn	Network Rail
Peter Evans	Network Rail
Ian Watson	Network Rail
Sivendran Sivapalan	Network Rail
Daniel Smart	Network Rail
Matthew Elmes	Vertex SE
Stephen Hebbes	Vertex SE
Siraj Ali	Vertex SE
Ian Brightmore	First Great Western (FGW)
Geoff Brison	First Great Western (FGW)

Appendix B – Hazard Log

This hazard log file is intended to provide a snapshot of the status of the safety management of the project or system of the title (below).
The History section below should be updated to provide an audit trail of changes/version control.

References (e.g. hazid reports) should be accessible by the Assessment Body.
For a staged EiS a copy of relevent sections (Works Package Hazard Log) should be issued (evidencing closed hazards) and referenced below in the live log.

Journal

	Jun-16	(XC) Created initial template

People

Safety and Assurance Special	Xenophon Christodoulou xen.christodoulou@networkrail.co.uk
DPE	Simon Eastmond
PM	Richard Evans
CEM	

Contractors and Main Suppliers

SSL	Signalling Solutions Limited

Abbreviations

CEM	Contractors Engineering Manager
ETCS	European Train Control System
DPE	Designated Project Engineer
EiS	Entry into Service
GRIP	Guide to Rail Investment Projects (development phases)
IDC/IDR	Inter-Disciplinary Check/Review
PM	Project Manager

Please complete this table to explain hazards

Issues and Assumptions

Please complete or add reference

HAZARD LOG Form

HAZARD ASSESSMENT												DESIGNER CONTROL MEASURES						RESIDUAL RISK						HAZARD TRANSFER
								Risk																
Hazard ID	**Location**	**Source**	**Discipline**	**Sub-discipline** - Topic within the engineering discipline (eg. Cess).	**Hazard Description** - Description of the Hazard relating to building construction, use (as a workplace), operating in normal/abnormal/emergency/degraded modes, cleaning and maintaining, altering, dismantling and demolition of a structure.	**Hazard Consequences**	**Red List Hazard**	**Persons at Risk**	**F**	**C**	**Result**	**Measures Taken by Designer** - Detail the hazard elimination or risk reduction actions.	**F**	**C**	**Result**	**Location of details**	**Status**	**Designer comments** - Designer comments on the designer control measures section contents that records decisions taken and clarification of actions taken by the designer.	**Residual Hazard Description** - Description of the Residual Hazard relating to building construction, using (as a workplace), operating in normal/ abnormal/emergency/degraded modes, cleaning and maintaining, altering, dismantling and demolition of a structure.	**Persons at Risk**	**Possible Residual Control Measures**	**Residual Hazard Owner**	**Residual Hazard Information Transmission**	**Designer Comments to Explain Residual Hazard** (To be completed where necessary for clarity and convey intent)	**Project Transfer Status** - Details of status of hazard when residual risk is being transferred to identified owner. No entry required until hazard formally offered to residual risk owner.
01	Generic - across all of the line (0m - 12m30)	VSE Review	Signalling		TPWS not as effective at preventing SPAD as GW-ATP. TPWS OSS are 'spot' rather than continuous supervision and therefore driver could accelerate to a red signal.	Risk of SPAD leading to collision (rear-end). Multiple fatalities possible, especially given derailment could occur onto adjacent lines.		Passengers, Workers	2	5	Intolerable risk	only exists until ETCS is brought in - estimated 2 years max	1	5	Tolerable risk				Only exists until ETCS L2 starts, estimated 2 years maximum.	Passengers, Workers	Post-incident analysis would show if acceleration towards red light - briefings/amendments to training policy would be implemented. Professional Driving Policy (assumed Crossrail ToC would have similar)	ToCs			
02	Generic - across all of the line (0m - 12m30)	VSE Review	Track		Workers must be line-side to install TPWS equipment. Risk of being struck by train.	Fatality to worker struck.		Workers	1	4	Tolerable risk	Work in Possession, competent staff and SSOW	1	4	Tolerable risk				One off during installation .	Workers	Possession Management/ SSOW for possessions staff. PPE/PTS for line-side staff. Briefings to lineside staff. Competence of PICOP, COSS, ES and individual.	Possessions staff (including NR and contractors)			
03	Generic - across all of the line (0m - 12m30)	VSE Review	Track		Additional TPWS equipment installed on track, leads to increased risk of trips/falls to staff working track-side	Minor injury to worker		Workers	3	2	Tolerable risk	competent staff and SSOW	3	2	Tolerable risk			No. of fitments has already been reduced to enhance train protection benefit whilst minimising risk to staff i.e. only essential fitments selected.	Exists for life of TPWS >25 years, or until removed following risk assessment.	Workers	SSOW for lineside staff. PPE/PTS for line-side staff. Briefings to lineside staff. Competence of individual. Minimisation of failure by selection of most reliable equipment. Minimisation of visits required by RoSE. Should TPWS become redundant, the TPWS could be removed should train protection function no longer be required.	Any lineside staff (NR or contractors)			
04	Generic - across all of the line (0m - 12m30)	VSE Review	Lineside E&P		Additional TPWS equipment must be maintained- increased exposure to line-side working and associated risk of workers being struck by vehicles	Fatality to worker struck.		Workers	2	4	Tolerable risk	Work in Possession, competent staff and SSOW	2	4	Tolerable risk			No. of fitments has already been reduced to enhance train protection benefit whilst minimising risk to staff i.e. only essential fitments selected.	Exists for life of TPWS >25 years, or until removed (or not longer maintained) following risk assessment.	Workers	SSOW for lineside staff. PPE/PTS for line-side staff. Briefings to lineside staff. Competence of individual. Minimisation of failure by selection of most reliable equipment. Minimisation of visits required by RoSE. Should TPWS become redundant, the TPWS could be removed should train protection function no longer be required.	Any lineside staff (NR or contractors)			
05	Part of the line where ATP is present	VSE Review	Driver		Additional TPWS equipment trips ATP trains due to ATP drivers style of driving not compatible with new OSS positions	Minor injuries to passengers due to falling- especially given approach to Paddington when people are standing to exit/ moving through carriages to find seats.		Passengers	0	2	Negligible risk	Option 3 puts TPWS OSS at 'normal' distances from signals, albeit on signals that would not normally be fitted with TPWS.	0	2	Negligible risk			ATP more onerous than TPWS and therefore unlikely that this situation would exist. TPWS design criteria have taken this into account and eliminated it.	N/A						
06	Generic - across all of the line (0m - 12m30)	VSE Review	Signalling		TPWS installed with no definitive indication of failure to signaller (i.e. lamp-out provided, not 'blue square' indication) or maintainer, leading to confusion over state of railway should TPWS fail.	A worker would have to investigate putting them in danger. Worst case: worker struck by train leading to fatality.		Workers	2	4	Tolerable risk	LED signals are fitted in the area. 'Lamp Out' failures are therefore likely to be TPWS failures.	2	4	Tolerable risk			Failure rate of TPWS is very low. Driver would be asked to report signal aspect/ lamp status at signal affected under existing procedure., thus identifying fault as with TPWS.	Exists for life of TPWS >25 years, or until removed (or no longer maintained) following risk assessment.	Workers	Signaller briefing as to which signals have been fitted with TPWS. SSOW for lineside staff. PPE/PTS for line-side staff. Briefings to lineside staff. Competence of individual. Minimisation of failure by selection of most reliable equipment. Should TPWS become redundant, the TPWS could be removed should train protection function no longer be required.	signaller, workers			
07	Level NTC: L2 ETCS fringe (Heathrow Tunnel)	VSE Review	Driver		New fringe created from AWS/TPWS to ETCS L2 at entrance to Heathrow tunnel. Driver becomes confused/ improperly trained and does not carry out transition properly.	Risk of not having a correct protection system active on board. Increasing the SPAD risk and derailment. Worst case: collision, multiple fatalities.		Passengers	1	5	Tolerable risk	Driver Training, Signage at Transition	1	5	Tolerable risk			ETCS transitions are automatically controlled.	Exists for as long as trains are required to transition (i.e. ETCS not available).	Passengers, Workers	Driver training must take this into account and will not commence until requirements defined.	ToC			
08	Generic - across all of the line (0m - 12m30)	VSE Review	Signalling		Operational issues caused by TPWS failures leading to signal in rear held at red. Method 3 integration means signaller unaware of cause of failure. Would lead to degraded mode operations if signal approached at danger until cause could be established.	Risk of train collision due to trains being talked past red signals (caused by TPWS failure) and therefore full interlocking protection is lost. Any collision would lead to multiple fatalities.		Passengers	1	5	Tolerable risk	Existing degraded mode procedures.	1	5	Tolerable risk			Current processes (Reg. 20) would have the 1st train through stopped at the signal with the failure. The signaller and driver would confer on what the driver sees i.e. to determine if lamp failure or TPWS failure.	Exists for life of TPWS >25 years or until TPWS removed. Potentially increased likelihood of Reg . 20 incidents due to increased no. of TPWS fitments which could fail 'lamp out'.	Passengers, Workers	Additional TPWS equipment could be reviewed once no longer necessary for train protection (i.e. once rolling stock has migrated to ETCS or ATP)	ToC Signaller			
09	Junctions with approach release/ divergent routes with varying speed limits	VSE Review	Signalling		Approach speed controlled junctions fitted with GW-ATP not speed restricted when approached by non-ATP train. Leads to risk of over-speed.	Potential for derailment - multiple fatalities especially if adjacent line obstructed.		Passengers, Workers	2	5	Intolerable risk	Crossrail TOC driver training to give sufficient Route Knowledge as to junction speed limits. Also check speed limit boards are visible	1	5	Tolerable risk			Most of these routes (MAR) are into/out of depots/yards which are not electrified. MAY-FA provides additional advance warning of lower speed turnouts already. FGW state that overspeeds are rare.	Overspeed derailment should lower-speed turn-out be taken at too high speed.	Passengers, Workers, Members of the Public	Driver training and briefing. Detailed design to look at if Class 345 will be able to accelerate to above the limit of the lower speed route given that it is a stopping service.	ToC			
10	Generic - across all of the line (0m - 12m30)	VSE Review	Driver		Drivers unfamiliar with use of Level NTC and associated route knowledge due to expecting to use cab signalling via ETCS. Risk of over-speed and SPAD.	Potential for derailment or SPAD leading to collision.		Passengers, Workers	2	5	Intolerable risk	Crossrail TOC driver training to include NTC Operations and how to Transition from NTC to L2 and vice-versa	1	5	Tolerable risk			On-board processes are the responsibility of the ToC	Only exists until ETCS L2 implemented and transition is eliminated.	Passengers, Workers	Driver training must be sufficient	ToC			
11	ESR/TSR locations	VSE Review	Driver		Driver does not obey TSRs/ESRs which are no longer enforced by GW-ATP.	Potential for derailment or SPAD caused by over-speed.		Passengers, Workers	1	5	Tolerable risk	If boards are not out, then trains are cautioned. AWS/2-light indicator deployed TSRs published in WON	1	5	Tolerable risk				Regulated speed limits have OSS	Passengers, Workers	Driver competence	ToC			
12	Future signalling fringe	VSE Review	Driver	N/A	Should Level NTC running be required following introduction of Crossrail service through-running from Stratford, a new fringe will be created at CBTC: NTC boundary	SPAD/overspeed leading to collision should signalling transitions not be handled correctly		Passengers, Workers											Only applicable if ETCS further delayed.	Passengers, Workers					
13	Signal with complex approach	VSE Review	Signalling		TPWS failure may affect multiple routes at complex junctions, leading to increased operational impact of any TPWS failure at that signal. Performance impact to multiple routes	Delays whilst trains are talked past signals						Non-safety risk- operational delays. Safety risk covered by previous hazard.							Investigate using local relay system to mitigate TPWS failure impacts at complex junctions. i.e. cutting OSS in/out depending on route set.						
14	Generic - across all of the line (0m - 12m30)	VSE Review	Train		TPWS reset procedure in Level NTC not well understood: rate of 'reset and continue' type errors not known.	Erroneous reset and continue could lead to collision and multiple fatalities.		Passengers, Workers	1	5		Mk 4 TPWS unit to be fitted. This on-board fitment mitigates this type of incident. Driver is informed as to reason why they have been tripped and therefore will not mis-interpret trips as TPWS system faults.	1	5	Tolerable risk			Hazard cannot be further reduced.		Passengers, Workers	Driver training	Driver training is responsibility of ToC			
15	Generic - across all of the line (0m - 12m30)	VSE Review	Train		Level NTC degraded mode procedures not well understood. Operational Procedures between driver and signaller may need to be looked at in event of Level NTC on-board failure. If GW-ATP fails, train is still protected by TPWS (as typically they are dual-fitted e.g. Heathrow Connect). This is not the case for TPWS only train as no secondary train protection system is present.	Increased risk of SPAD in degraded mode leading to collision potential.			1	5	Tolerable risk	Responsibility for defining on board equipment is with the TOC (in compliance with Rule Book for failed on board equipment)- transfer to the TOC.	1	5	Tolerable risk			Hazard already addressed in existing degraded mode processes.	Only exists until ETCS L2 implemented	Passengers, Workers					
16	Trains - Transition Points L2 to NTC	VSE Review	Signalling	Balises	EMI issues which compromise ATP function at the transition point	Increased risk of SPAD leading to collision and or derailment		Passengers, Workers	1	5	Tolerable risk	Product acceptance of balises takes into account ATP compatibility.	1	5	Tolerable risk				Only exists until ETCS L2 implemented	Passengers, Workers					

HAZARD LOG Form

HAZARD ASSESSMENT										Risk		
Hazard ID	**Location**	**Source**	**Discipline**	**Sub-discipline** - Topic within the engineering discipline (eg. Cess).	**Hazard Description -** Description of the Hazard relating to building construction, use (as a workplace), operating in normal/abnormal/emergency/degraded modes, cleaning and maintaining, altering, dismantling and demolition of a structure.	**Hazard Consequences**	**Red List Hazard**	**Persons at Risk**	**F**	**C**	**Result**
17	PSR locations	VSE Review	Driver		Driver does not obey PSRs/line-speed which are no longer enforced by GW-ATP.	Potential for derailment or SPAD caused by over-speed (TPWS no longer fully effective as positioning assumes deceleration from line-speed).		Passengers, Workers	1	5	Tolerable risk
18	All ATP fitted areas	2nd HAZID review	Driver		ATP protects against roll-back. TPWS does not provide this functionality.	Collision due to train rolling back to point of conflict e.g. junction.		Passengers, Workers	1	5	Tolerable risk
19	Paddington Buffer Stops	2nd HAZID review			ATP protects approach to buffer stops at Paddington to lower speeds than TPWS can provide. TPWS OSS also not health monitored.	Collision with buffer stops at higher speed than with an ATP train leading to serious injuries/ fatalities if speed is high enough e.g. to hit persons on concourse.		Passengers, Workers, Members of the Public	1	5	Tolerable risk

	DESIGNER CONTROL MEASURES							RESIDUAL RISK							HAZARD TRANSFER
Hazard ID	**Measures Taken by Designer** - Detail the hazard elimination or risk reduction actions.	**F**	**C**	**Result**	**Location of details**	**Status**	**Designer comments** - Designer comments on the designer control measures section contents that records decisions taken and clarification of actions taken by the designer.	**Residual Hazard Description** - Description of the Residual Hazard relating to building construction, using (as a workplace), operating in normal/ abnormal/emergency/degraded modes, cleaning and maintaining, altering, dismantling and demolition of a structure.	**Persons at Risk**	**Possible Residual Control Measures**	**Residual Hazard Owner**	**Residual Hazard Information Transmission**	**Designer Comments to Explain Residual Hazard** (To be completed where necessary for clarity and convey intent)	**Project Transfer Status** - Details of status of hazard when residual risk is being transferred to identified owner. No entry required until hazard formally offered to residual risk owner.
17	PSRs are published and required as part of route knowledge. Regulated PSRs are fitted with TPWS OSS on approach EVC enforces 90 mph max. speed of Class 345. Exemption already exists to requirement for PSR enforcement on plain line except for regulated fitments.	1	5	Tolerable risk				Regulated speed limits have OSS	Passengers, Workers	Driver training/competence	ToC			
18	unknown if Class 345 contains protection against roll-back as part of the train design	1	5	Tolerable risk			control of train movements is responsibility of ToC		Passengers, Workers	Driver training/competence	ToC			
19	Linespeed is 25 mph or 40 mph on approach	1	5	Tolerable risk			Would require driver to completely ignore speed limits on approach to Paddington. Buffer stops on plats 11 and 12 are listed and cannot be easily replaced with safer modern equivalents.		Passengers, Workers, Members of the Public	Driver training/competence. Investigation of the condition of the buffer stops and potential improvements.	ToC			