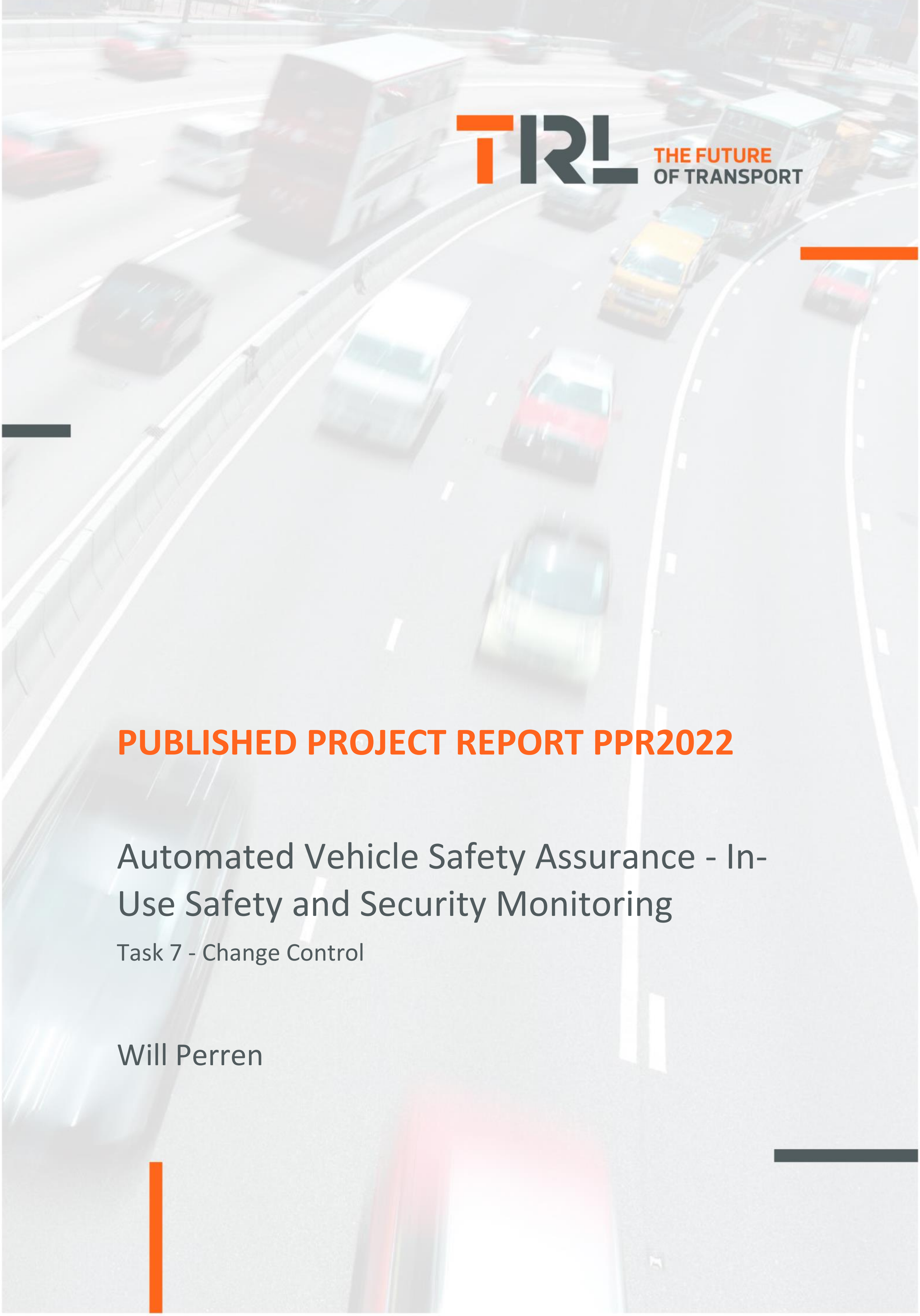

PUBLISHED PROJECT REPORT PPR2022

Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring

Task 7 - Change Control

Will Perren

Report details

Report prepared for:	Department for Transport		
Project/customer reference:	TETI0042		
Copyright:	© TRL Limited		
Report date:	30/06/2022		
Report status/version:	2.0		
Quality approval:			
Gareth Slocombe (Project Manager)	G. Slocombe	Ianto Guy (Technical Reviewer)	I. Guy

Disclaimer

This report has been produced by TRL Limited (TRL) under a contract with Department for Transport. Any views expressed in this report are not necessarily those of Department for Transport.

The information contained herein is the property of TRL Limited and does not necessarily reflect the views or policies of the customer for whom this report was prepared. Whilst every effort has been made to ensure that the matter presented in this report is relevant, accurate and up-to-date, TRL Limited cannot accept any liability for any error or omission, or reliance on part or all of the content in another context.

When purchased in hard copy, this publication is printed on paper that is FSC (Forest Stewardship Council) and TCF (Totally Chlorine Free) registered.

1 Executive Summary

The proposed in-use safety and security monitoring scheme can serve as an essential feedback mechanism for continual improvement of how the AV safety assurance scheme manages safety. In-use monitoring data can support in identifying changes and assessing their impact. However, making a change without due consideration of the impacts to all stakeholders may lead to increased regulatory inefficiency, undue burden on manufacturers and operators and may ultimately lead to worse safety outcomes.

This document outlines a change control process to manage and implement change throughout the entire AV safety assurance scheme to formally capture all learnings and provide feedback to identify, assess and implement positive change.

This report identified 6 key elements of good practice change control processes from other industries, they are:

1. Identify/ Plan
2. Assess
3. Review
4. Test
5. Implement
6. Monitor and Close

These 6 elements were applied to the AV safety assurance context to develop a change control process for the scheme. Specific examples of changes were used to identify potential impacts and how they should be managed within the scheme.

This report has introduced three key process roles: the change owner, change manager and change control board. These roles have a responsibility to make a change, once identified, through the change control process, review and approve changes to ensure changes are made with consideration to their impacts and in line with wider priorities.

The process is intended to be applied flexibly. This allows change processes to be less resource intensive for more minor changes as less information is documented and change approval is less involved. Because of this however, this provides less traceability of the change due to a lack of an audit trial. Changes to the AV safety assurance scheme could drastically affect the performance of safety critical systems on public roads. As a result, careful consideration is required before deciding whether any change control processes can be relaxed.

A summary of the proposed change control process is outline in Figure 1.

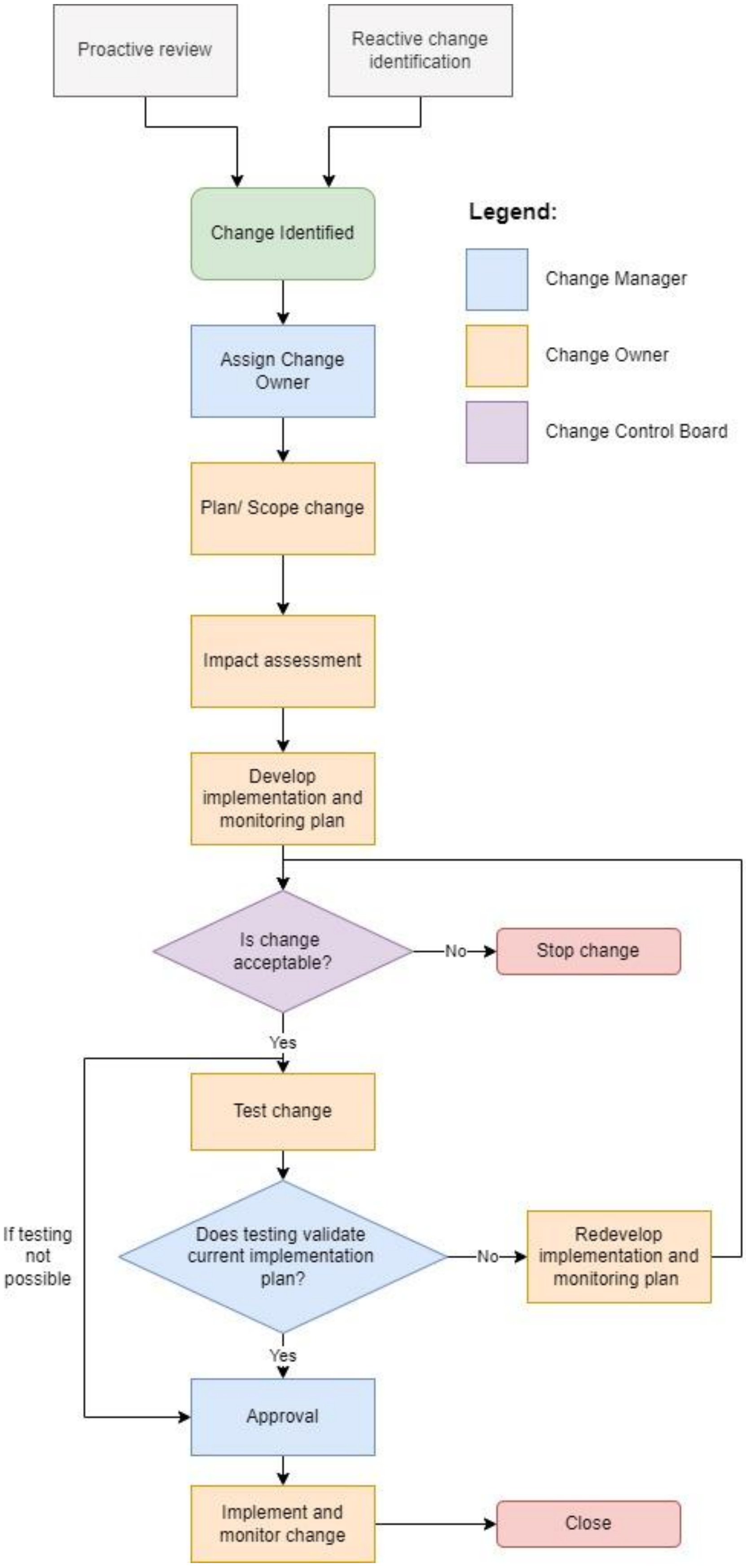

Figure 1: Change control process flow chart

Table of Contents

List of tables and figures

Tables

Figures

List of abbreviations

AV:	Automated Vehicle
CAST:	Causal Analysis Using Systems Theory
CRN:	Change Reference Number
ODD:	Operational Design Domain
QMS:	Quality Management System
SMS:	Safety Management System
STAMP:	System-Theoretic Accident Model and Processes

2 Introduction

The proposed in-use safety and security monitoring scheme primarily focuses on continually validating the safety of deployed Automated Vehicles (AVs) throughout their lifetime. However, it can also serve as an essential feedback mechanism for continual improvement of how the AV safety assurance scheme manages safety. Learnings identified from in-use monitoring may show gaps in approval and authorisation requirements which would need to be resolved to continually improve safety under the scheme. It is expected then that data collected from in-use monitoring will be used to support changes and updates to the scheme over time. In order to enable this, the regulator must ensure relevant data is collected in order to identify, evaluate and implement changes for the purpose of continuous improvement.

However, making a change without due consideration of the impacts to all stakeholders may lead to increased regulatory inefficiency, undue burden on manufacturers and operators and may ultimately lead to worse safety outcomes. A change control process is required to manage and implement change throughout the entire AV safety assurance scheme to formally capture all learnings and provide feedback to identify, assess and implement positive change. This will ensure that the scheme remains flexible, adaptable and will develop up to date good practice for assuring AV safety. This document discusses what potential changes could be identified through in-use monitoring, what data needs to be collected and process considerations for how the impact of change can be assessed.

3 Scope

This document discusses change management related to potential learnings identified through in-use monitoring in order to effect change to the AV scheme. This includes both pre-deployment (approval and authorisation) and post-deployment (in-use safety assurance) elements. This change process is to support feedback of new learnings gained through deployment. As such, many specific changes cannot be foreseen at this time. This report outlines a change process that is flexible to the nature of the exact change and examples are used to discuss how changes to certain scheme elements will need to be handled differently.

This report does not consider changes from external stimulus such as development of new standards or new international regulatory processes as it will require separate decision-making processes to decide how to incorporate these into the GB scheme. However, this report may provide helpful considerations for how to implement these changes in a controlled manner.

4 Change control

Change control processes typically exist as part of organisational Quality or Safety Management Systems (QMS or SMS) and used to ensure that changes to a product, system or process are introduced in a controlled and coordinated manner[1]. There are 6 key steps in traditional change control processes (Monahan, 2019):

1. **Identify/ Plan** – Changes can be identified by anyone and identifying and escalating areas for positive change should be encouraged. Once a change is identified, it is necessary to scope out the change in detail. This includes detailing the exact nature of the change, the potential benefit from conducting the change and any initial impacts identified. A plan for conducting the change should then be specified including how it is communicated/ implemented, who the owner of the change is and the target completion date.

2. **Assess** – The impact of the proposed changes should be assessed. This includes conducting risk and impact assessments which should aim to identify impacts on existing systems and processes, stakeholders and the organisation. Types of impact that are considered include cost, performance, delays, operational downtime and safety risks. The findings of the impact assessment(s) determine the priority of the change, how much effort is required to test and implement the change and the level of approval required.

3. **Review** – Review of the change is required to ensure stakeholder involvement and approval. This is usually actioned through a change board or steering committee but may be approved by a single person if the change is sufficiently low impact or low priority. In the review step, the plan/scope and impact/risk assessments are considered in the context of organisational goals, requirements, and resources required to enact the change. A decision is then made as to what changes are made and their priority.

4. **Test** - If the change control request is approved to move forward, the change owner and delivery team will execute the solution through a small-scale development process. This may include piloting the change with a small group/test space, simulation, or conducting and testing an incremental change in advance of the full change. The purpose of the test phase is to validate whether the proposed benefits are likely to be realised and whether the impacts are likely to be mitigated as intended. The results are then shared for a second review step prior to implementation

5. **Implement** - Upon approval, the implementation plan must be implemented, with all identified impacts and risks mitigated for. At this stage, any relevant documentation should be updated, and changes communicated to all relevant stakeholders.

6. **Monitor and Close** – It is necessary to monitor the success of the implementation to confirm all impacts and risks continue to be mitigated and there are no unforeseen issues. Change should be monitored until embedded as business as usual. Any issues

[1] There is considerable overlap between change control process and configuration management. Configuration management considers establishing and maintaining the consistency of complex systems. Change management is the collective term for change processes but most commonly applies to organisational change.

arising from this should be reviewed further mitigations added or change aborted if the issues are intolerable. Closure of the change process should be reviewed and approved.

Change control process typically consider two different types of change; reactive and proactive.

Reactive changes are ones identified in response to a certain event or piece of evidence. The change intends to rectify the causes of the situation that led to the undesirable event (or sequence of events). An example of a reactive change would be the addition of a scenario to the scenario simulation test set following a number of similar incidents during operation.

Proactive changes are based on the need to improve current performance though periodic review and assessment. These changes aim to pre-emptively tackle issues or improve performance before an undesirable event occurs. An example of proactive monitoring would be periodic increase of the safety standard that AVs are assessed against in line with Government policy.

5 Change control for in-use safety monitoring

The following section discusses options for how the key steps in a change control process can be applied for the AV safety assurance scheme.

5.1 Identify/ Plan

In-use monitoring will be expected to supply data necessary to help regulators identify and evaluate potential changes. Two broad categories of data are expected to be available:

Aggregated data - to enable statistical evaluation in order to evaluate trends in safety performance over time.

Individual event data – case study analysis of individual events to identify the causal factors associated with an event.

Both categories of data could potentially be used to identify opportunities for change. Aggregated data is proposed to be compiled by the manufacturer for individual deployments and then compiled further across the whole scheme by the in-use regulator. Aggregated data may identify trends in safety performance such as a sudden incidence of collisions associated with certain road user groups. This may then prompt further investigation to identify changes to resolve this. Aggregated data analysis of lagging metrics (i.e., collisions or other risk outcomes) is reactive in nature as it identifies changes from realised harm. Aggregated data analysis of leading metrics lends itself to proactively identify changes and as such the in-use regulator should set up periodic reviews of this data to track safety performance and identify any changes that need to be taken to improve.

Individual event data is generated from the investigation of events by the manufacturer. Broadly the individual event reports shared to the regulator should display sufficient information required for the regulator to determine whether the event violates the safety performance on which the approval was based. For this the manufacturer must establish the causal factors attributed to the event. Furthermore, any event (or set of events) escalated to the independent investigator will also be investigated and will seek to identify causal factors.

There is a growing trend in incident investigation approaches to explore causal factors at all levels. Within the System-Theoretic Accident Model and Processes (STAMP) approach, analysis is based on the presence of inadequate or unsafe control actions by controllers. Controllers can be human (individual or entity) or automated (software and hardware) (Leveson, Daouk, Dulac, & Marais, 2003). Causal Analysis using Systems Theory (CAST) considers regulatory policy and processes to be a controller that imposes system constraints on a system. Therefore, changes required to address regulatory policy and processes can be identified using this method.

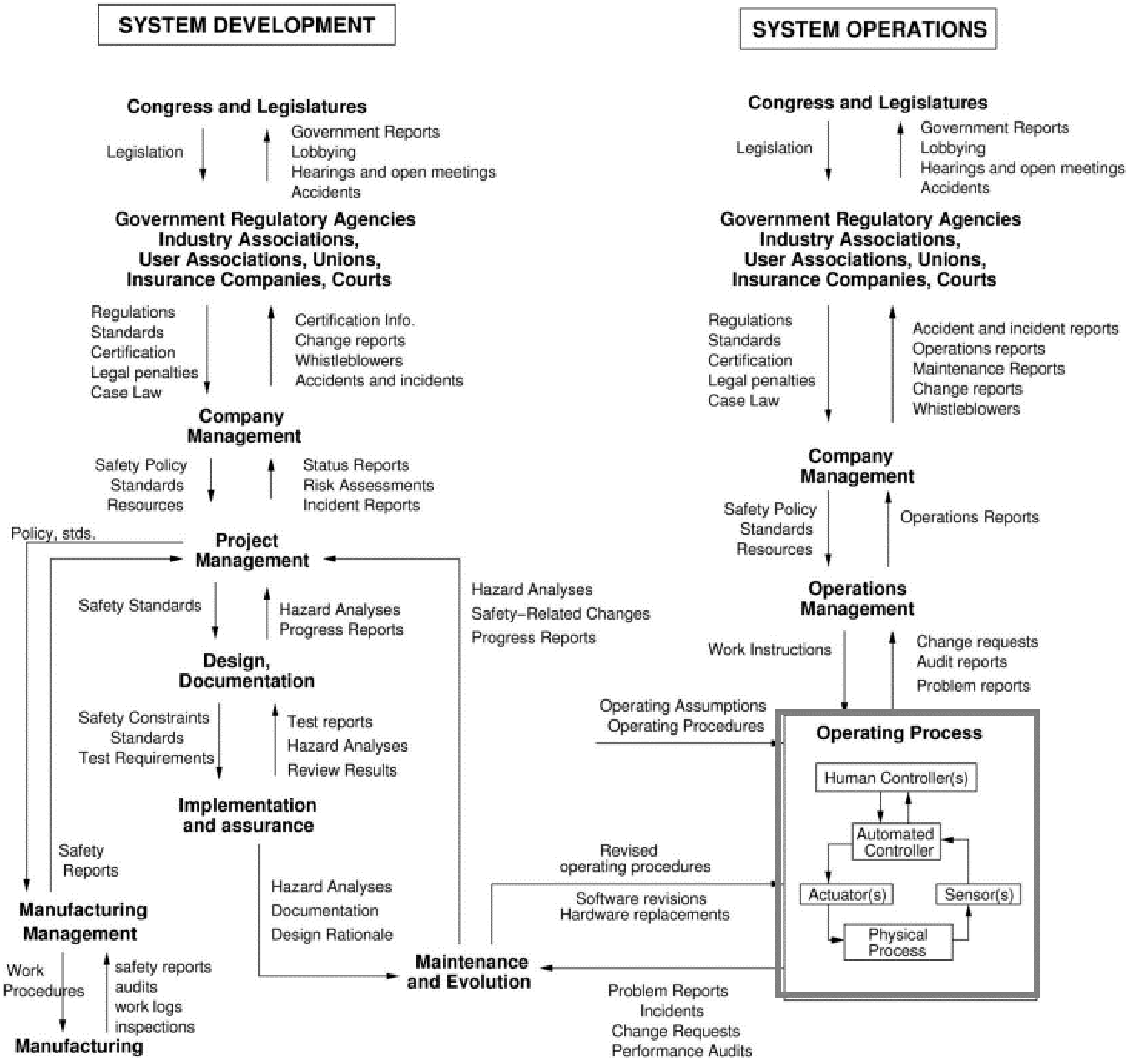

Figure 2: Example of a safety control structure (Leveson, N., 2019)

Accimap is another relatively new method for collision investigation. The AcciMap approach involves the construction of a multi-layered causal diagram in which the various causes of an event are arranged according to their causal remoteness from the outcome (Faruqe Hamim, et al., 2022).

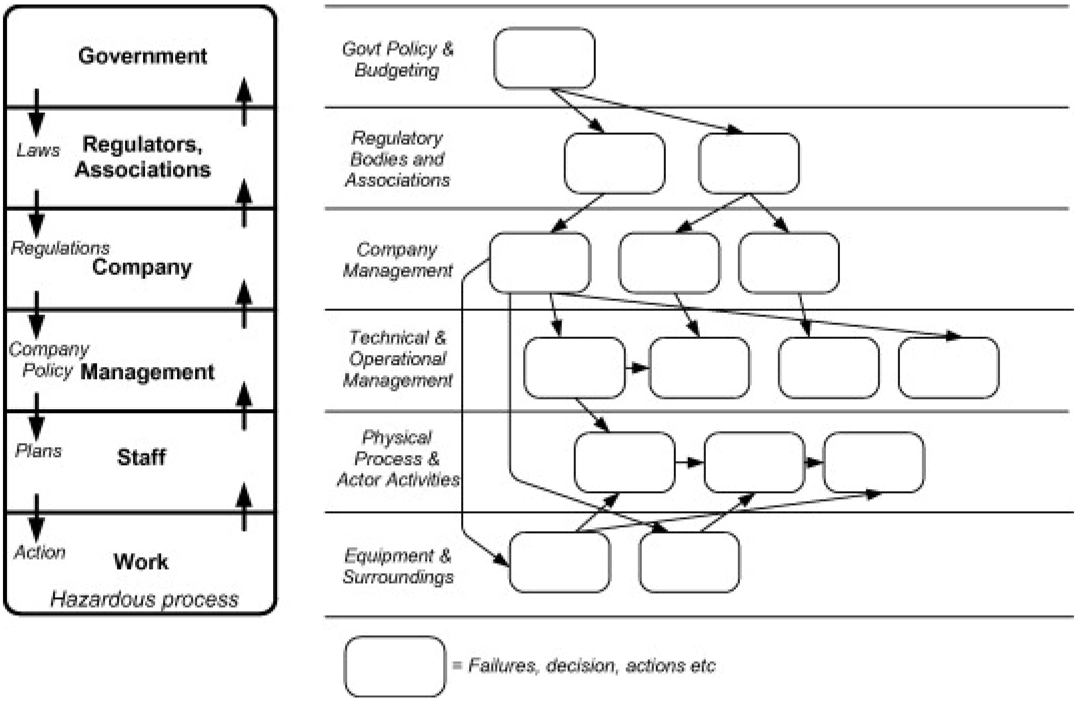

Figure 3: Accimap template (Faruqe Hamim, et al., 2022)

Similarly to STAMP/CAST, laws and regulations are seen as causal factors of an outcome in Accimap. Accimap can identify how failures in these can influence lower-level decisions, actions or failures such as company management, staff or system elements.

In order for changes to be identified for this scheme by event data, it is recommended that investigation methods are employed (such as Accimap and STAMP/CAST) that consider government and regulatory elements to provide recommendations for how they can be improved. This would be easily achieved by the independent investigator who could be tasked for this very purpose. Manufacturers could also be required to investigate such elements and feedback to the in-use regulator as part of their event reporting requirements. Care should be taken however with this as manufacturers may have a bias toward placing (what may be perceived to be) ‘blame’ towards the regulator instead of themselves, especially as this may expose them to sanctions.

Outside of these two broad groups, the in-use regulator should also engage proactively with manufacturers and operators under the scheme to identify any particular pain points and gaps they can see.

5.1.1 Potential changes

It is not possible to foresee the exact nature of the changes that may be necessary. However, a number of possible changes that may occur under the scheme have been identified in Table 1.

Table 1: Potential changes of the Approval and Authorisation scheme

Change Area	Example
Legislation	Changes to authorisation requirements (e.g. data collected for detected collisions)

	Change or reallocation of roles and responsibilities for entities involved (approval authority, in-use regulator, manufacturer, operator, etc)
Safety Case	Changes to guidelines/requirements for vehicle or deployment safety cases
	Change to safety case audit process
	Change to Safety Management System (SMS) assessment criteria
Risk Framework	Addition/removal of defined safety goals and/or technical requirements
	Changes to the safety standard set
ADS functional and behavioural requirements	New behavioural competencies defined
	Existing behavioural competencies redefined/ removed
	Changes to Operational Design Domain (ODD) specification guidance
Test requirements	New scenarios added to simulation scenario set
	Changes to sampling strategy for physical testing
In-use monitoring	Changes to data elements for recall
	Changes to reportable data type, format and frequency
	Addition or removal of leading or lagging measures
	Change to trigger threshold value for measures
	Restriction of scheme wide AV operations under certain conditions

Table 1 highlights the variety of safety assurance scheme process areas that may require change. As such the change control process must be flexible in order to apply to all aspects of the scheme. The impact of changes within these categories is discussed further in Section 5.2.

5.1.2 Planning for change

When a change has been identified, it is necessary to scope out and plan the change. In this context however, consideration should be given to the primary purpose of the in-use monitoring scheme. Primarily, in-use monitoring seeks to validate safety performance and identify areas of non-compliance by the manufacturer and the operator. As such, it is necessary to determine what is actual non-compliance by an AV manufacturer or operator and what constitutes an issue with the safety assurance scheme.

It is necessary to consider the following when reviewing the needs to implement a change:

- Does the evidence provided specifically indicate a gap in the approval or authorisation scheme? Detailed analysis through event investigation (Accimap, STAMP/CAST) may provide strong justification that this is a causal factor of undesired events.
- Is the evidence that indicates an issue exclusively from a single AV deployment? Corroboration of similar issues across different manufacturers and operators gives more weight to the argument that the issue is a gap in requirements.
- If an issue is identified in a single deployment, could the issue foreseeably affect other deployments? Even if the evidence indicates issues affecting one deployment, implementing a change now could prevent issues in others before they arise.

The planning stage should also seek to scope out the justification for the change. As this concerns a safety assurance scheme, the primary justification is likely to be a reduction in safety risk. As such an initial appraisal of safety benefit should be conducted. This may incorporate in-use monitoring data to evidence the potential safety benefit.

A justification could be stated as follows "In-use monitoring identifies that the highest proportion of rule violations occur in proximity to zebra crossings. Greater testing and validation requirements of scenarios involving pedestrians at zebra crossings prior to approval could lead to positive safety outcomes and a reduction in the current 'X' number of safety relevant rule violations at zebra crossings".

It is good practice to appoint a change owner who is responsible for, once a change has been identified, managing it through the change control process. The change owner should be responsible for scoping and planning the change, completing all documentation relating to the change and seeking approvals from the relevant decision authorities (see Section 5.3). The change owner does not have to be the person who identified the change or the need to initiate the change control procedure.

5.2 Assessing impact

The next step is to fully define and understand the impacts of the change and how to achieve the desired outcome. This should involve discussions with all potentially affected parties. For the AV safety assurance scheme, changes may impact regulatory bodies as well as the manufacturers and operators being regulated. Impacts may be to time, costs and operation, or to safety. Safety impacts may also impact the GB public, who may be exposed to increased risk as a result of the change. For the change examples outlined in Table 1, potential impacts have been assessed. These are outlined in Table 2, below.

The findings indicate that the impacts relating to a change may be varied and specific, highlighting the need for a detailed process to assess each change individually taking into account the specific context of that change. However, categories of impacts worth further consideration have been identified.

Table 2: Impact considerations for example AV scheme changes

Change Area	Change examples	Impact considerations	
		Time, cost and operational impacts	Safety impacts
Legislation	Changes to authorisation requirements (e.g. data collected for detected collisions)	- Redevelopment of manufacturer monitoring systems and Safety Case - Increased data capture and storage requirements	- Changes to monitoring system introduce reliability issues with detecting collisions and recalling data
	Change or reallocation of roles and responsibilities for entities involved (approval authority, in-use regulator, manufacturer, operator, etc)	- Redevelopment of manufacturer and operator safety cases - Additional resource and expertise required to meet new responsibilities	- Unclear or miscommunicated change in safety responsibilities between manufacturer and operator, or in-use regulator and approval authority - Lack of expertise in new responsibility leading to poor safety management
Safety Case	Changes to guidelines/requirements for vehicle or deployment safety cases	- Significant changes to vehicle safety systems (may include redesign) - Operational downtime necessary to comply with new requirements	- Rushed changes and redesigns leading to worse AV safety performance
	Change to safety case audit process	- Additional resource and expertise required by regulator to conduct audit	- Safety issues that would violate approval not detected by regulator
	Change to Safety Management System (SMS) assessment criteria	- Organisational process and culture change which may take significant time and effort to embed.	- Poor safety management, failure to detect and resolve safety issues
Risk Framework	Addition/removal of defined safety goals and/or technical requirements	- Significant changes to vehicle safety systems (may include redesign) - Redevelopment of manufacturer Safety Case - Change to test ret requirements to accommodate new goals	- New safety goal improperly specified or communicated leading to a failure in meeting

	Changes to the safety standard or to risk tolerability acceptance criteria	- Significant changes to vehicle safety systems (may include redesign) - Redevelopment of manufacturer Safety Case - Approval requirements change to assess against new criteria - Regulator process to monitor AV safety performance against new standard	- New criteria or standard set without safety evidence. Inadequate or unachievable standards that cannot be complied with
ADS functional and behavioural requirements	New behavioural competencies defined	- New simulation testing and vehicle development	- Conflicts with existing behavioural competencies introduced
	Existing behavioural competencies redefined/ removed	- New simulation testing and vehicle development	- Conflicts with existing behavioural competencies introduced
	Changes to ODD specification guidance	- Redevelopment of manufacturer Safety Case - Operational restrictions leading to commercial impacts	- Inconsistent definition of ODD leading to operation outside of design limits
Test requirements	New scenarios added to simulation scenario set	- New simulation testing and vehicle development - Revalidation of all other scenarios - Operational downtime to revalidate	- Improper understanding or specification of new scenarios leading to undesired/ unsafe performance during operation
	Changes to sampling strategy for physical testing	- Greater resources and expertise required to conduct tests	- Critical test scenarios missed - Improper coverage of scenarios
In-use assurance	Changes to data elements for recall	- Redevelopment of manufacturer monitoring systems and Safety Case	- Failure to capture critical data required for investigation and learning
	Changes to reportable data type, format and frequency	- Redevelopment of manufacturer monitoring systems and Safety Case - Resources for storing and handling data for regulator and manufacturer - Change in regulator expertise needed to analyse data	- Failure to capture critical data required for investigation and learning

	Addition or removal of leading or lagging measures	- Redevelopment of manufacturer monitoring systems and Safety Case - Significant increase in false positive capture rate and thus data capture and storage issues	- Failure to identify critical safety scenarios and non-compliance events
	Change to trigger threshold value for measures	- Redevelopment of manufacturer monitoring systems and Safety Case - Significant increase in false positive capture rate and thus data capture and storage issues	- Failure to identify critical safety scenarios and non-compliance events

Impacts resulting from changes to the AV safety assurance scheme could be expected in

- **AV performance requirements** – changes to technical and safety requirements may result in manufacturers updating their ADS software or redesigning their vehicle to ensure compliance. This may involve retrospective changes to vehicles already in service or updated requirements for vehicles not yet approved. This has significant cost implication on the manufacturer as a result of redevelopment testing and validation. Where these impacts are identified, the change owner should consider the cost implication of conducting such a change against the proposed benefit. If only a small benefit to safety can be achieved, then the change may not be practical to implement. These changes may be more appropriate over longer timescales with early communication of the changes allowing manufacturers to adapt to the new requirements without introducing significant disruption.
- **Manufacturer/ Operator documentation and process**– The safety case(s) should be updated to reflect and comply with new requirements as a result of changes made to the scheme. Organisations writing a safety case should already have their own change control and continuous improvement processes for updating safety cases and so should be ready to adapt to changes. Nevertheless, significant changes to safety case and documentation may require the gathering of additional evidence or implementation of further risk mitigations to maintain compliance, which may have further impacts.
- **Approval, Authorisation and In-Use Assurance processes** – Changes to the AV safety assurance scheme will likely impact the activities undertaken by approval and assurance bodies. This could have impact on the effort (thus cost) on reviewing and accepting safety cases and test procedures as well as the efforts required in investigating, reviewing and analysing safety data. Changes may impact the approval authority, authorisation bodies, in-use regulator and independent investigator. The change owner should consult with stakeholders from these entities in order to better understand how each are impacted. Changes may introduce the need for specialist expertise or additional resources dedicated to investigating testing and implementing a change, as well as resources and capabilities once the change is embedded as standard. This may indicate new entities or external parties need to be introduced or specialist expertise acquired to address these changes.

Other impacts should be considered in relation to external factors and processes that they may be affected by. For example, a change to legislation will need to go through an amendments and consultation process, which has considerations for the budget and timescale required to enact the change.

An impact assessment should be conducted and documented by the change owner. The following should be considered and documented:

- A Change Reference Number (CRN)[2].
- Identification of key roles and responsibilities including the owner of the change, stakeholders that need to be informed, parties that need to be consulted, and authority for sign-off.
- The assessed impact of the change. This should include:
  - Details of what is involved to achieve the change and who it affects;
  - Justification for the change;
  - Risks and benefits of the change;
  - How the change defined impacts budget/timescales, research and safety.
- Implementation plan detailing the actions required to complete the change while minimising the impacts. This should be a continuation and documentation of the planning stage.
- Post-implementation monitoring plan.

5.3 Review and approval

Review of the change is required to ensure stakeholder involvement and approval. Following good practice, it is recommended to have a single person[3] appointed as change manager within the in-use regulator. The change manager will be the point of contact for anyone who wishes to propose a change to the AV approval scheme, appoint a change owner and act as the authority to review and approve changes. Given the AV safety assurance scheme involves a number of stakeholders who may all be impacted by a change, it is recommended that the change manager convenes a change control board regularly with participants from[4]:

- **In-use regulator,**
- **Vehicle Approval authority,**
- **Authorisation body,**
- Independent Investigator,
- Industry representation,
- Public representation[5].

[2] A Change Reference Number (CRN) is a unique document reference number that should be provided on all documentation relating to a specific change. The CRN should be referenced on all change documentation and should link to the central change control record/database.

[3] May be a single person or a single role split between multiple people

[4] Participants in **bold** are core attendees responsible for approval and decision making. Other attendees may be invited in order to provide additional expertise to aid in the review of changes.

[5] This may be special interest groups such as cycling associations and governing bodies

- Academia
- International regulators

The change control board is an opportunity to review and agree the change plan, scope and impact assessment with all potentially impacted parties. Once validated, the change is considered in the context of the wider assurance scheme including government policy, requirements, and resources required to enact the change. They will also discuss and agree a test and implementation strategy to mitigate risk.

A decision is then made as to whether a change is taken forward. The change manager should identify which stakeholders are directly impacted and seek approval from them as a minimum. A change approval matrix can be used as guidance to the change manager as to what approval needs to be given, however attaining acceptance from all stakeholders where applicable is recommended. A proposed change approval matrix based on the currently identified impact categories is provided in Table 3 below.

Table 3: Change approval matrix

	Change Approval Authority			
Impact category	Change Manager	In-use regulator	Approval Authority	Authorisation Authority
AV performance requirements	✓	✕	✓	✕
Manufacturer documentation and process	✓	✕	✓	✕
Operator documentation and process	✓	✕	✕	✓
Vehicle Approval	✓	✕	✓	✕
Authorisation	✓	✕	✕	✓
In-use assurance	✓	✓	✕	✕

The change control board can also act as a forum for leading or coordinating periodic reviews of safety data collected by in-use safety monitoring to proactively identify changes.

5.4 Test

In traditional change control processes, testing of a change is an important element to validate that the change effectively resolves the issue and/or identify and resolve any previously unforeseen risks. In the context of the AV safety assurance scheme, the scope for testing changes may be limited in some cases. This is because it may not be possible to pilot the change on a small scale within the scheme.

For changes to AV performance requirements, testing may be possible through simulation, or at a small scale with participating manufacturers prior to being changed in the scheme. Manufacturer/ Operator documentation and process or Approval, Authorisation and In-Use Assurance processes however are thought to be, being largely process based, a lot more difficult to test and validate prior to implementation. The degree of testing possible should be considered at review when determining whether a solution can be implemented. Greater emphasis may be placed on monitoring after implementation if there is less ability to test prior.

The Law Commissions, in their final report (Law Commission and Scottish Law Commission, 2022) believes that the in-use regulator should become a world-class source of expertise on the measurement of automated driving safety, by commissioning research on a range of possible measures. Research activities planned by the in-use regulator could feed into the change control process (where relevant to measuring AV safety) and vice versa, changes identified could be used to scope research which can provide evidence of proposed changes.

Any testing done should be conducted by (or on behalf of) the change owner and reviewed by the change manager. If there are no issues arising from testing and the expected result is achieved, the change manager may approve the change to move to implementation. If not, the change manager should escalate the test findings to the change control board to review and agree following actions.

5.5 Implement, Monitor, Close

Upon approval, the implementation plan must be implemented, with all identified impacts and risks mitigated for. At this stage, any relevant documentation should be updated, and changes communicated to all relevant stakeholders. The change owner should take responsibility for undertaking the change and collaborate with a team comprising of all parties necessary to enact a change effectively. It is necessary to monitor the success of the implementation to confirm all impacts and risks continue to be mitigated and there are no unforeseen issues. Data collected from in-use monitoring may help to identify any safety benefits achieved following a change and whether that is in line with expectation. Other monitoring of changes includes gathering feedback from change stakeholders as well as cost benefit analysis where applicable.

Change should be monitored until embedded as business as usual. Any issues arising from this should be reviewed further mitigations added or change aborted or reverted if the issues are intolerable. Closure of the change should be reviewed and approved.

6 Flexible application of the process

While this document sets out a formal, step-by-step process for managing change, it is important to recognise that not all changes are equal. The nature of the change, what elements of the approval scheme must change, and the significance of the impacts will vary. It is necessary then that the change management process does not impose unnecessary burden on regulators, manufacturers and operators using the scheme by being disproportionate to the type and significance of the change proposed.it is recommended that the Change manager role is responsible for deciding how strictly the change control process is applied. The process may be relaxed for changes that are simple to assess, have clear and relatively minor impacts, or the change is simple to enact. The change manager could be the point of contact for change owners to agree on the level of rigour needed for a specific change. This level of flexibility within the change process is necessary to ensure a fast and reactive safety assurance framework.

7 Summary and recommendations

This report identifies the key elements and considerations for a change process for the AV safety assurance scheme. Change control is an essential process for continuous improvement by ensuring positive changes are implemented with due consideration for the impacts and benefits of that change, as well as ensuring traceability as to what change was made, who made it and who authorised it.

This report identified 6 key elements of good practice change control processes from other industries, they are:

1. Identify/ Plan
2. Assess
3. Review
4. Test
5. Implement
6. Monitor and Close

These 6 elements were applied to the AV safety assurance context to develop a change control process for the scheme. Specific examples of changes were used to identify potential impacts and how they should be managed within the scheme. Broad impact categories were AV performance requirements, Manufacturer/ Operator documentation and process and Approval, Authorisation and In-Use Assurance processes. Specific requirements for these have been discussed. Figure 4, summarises the change control process proposed in this report.

This report has introduced three key process roles: the change owner, change manager and change control board. These roles have a responsibility to make a change, once identified, through the change control process, review and approve changes to ensure changes are made with consideration to their impacts and in line with wider priorities.

The change control process outlined in this report describes formal process and documentation requirements for managing changes to the AV safety assurance scheme. While the exact nature of changes that could be identified are unknown, a number of examples have been used to highlight how change could impact various elements of the scheme and affect different stakeholders. The process is intended to be applied flexibly. This allows change processes to be less resource intensive for more minor changes as less information is documented and change approval is less involved. Because of this however, this provides less traceability of the change due to a lack of an audit trial. Changes to the AV safety assurance scheme could drastically affect the performance of safety critical systems on public roads. As a result, careful consideration is required before deciding whether any change control processes can be relaxed.

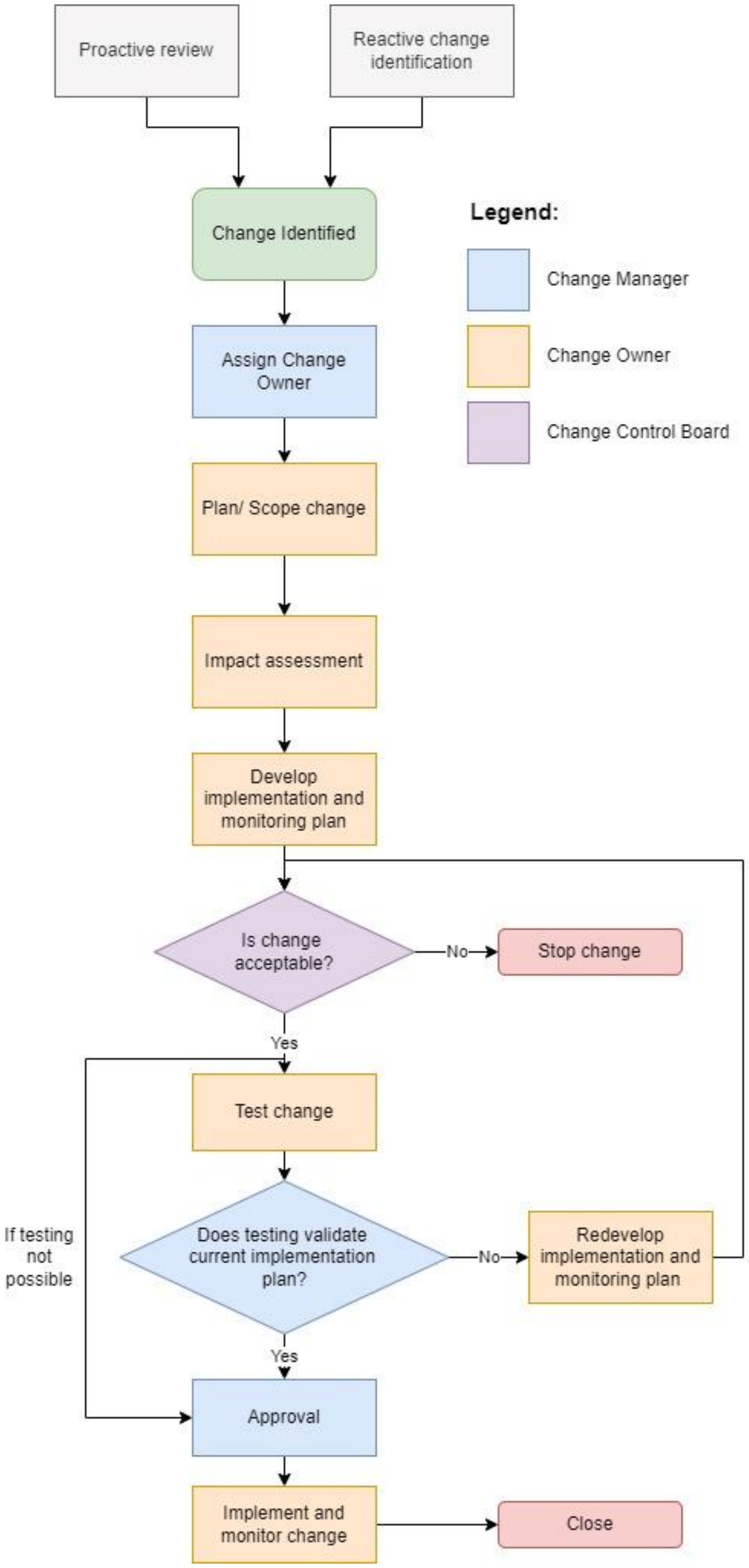

Figure 4: Change control process flow chart

8 References

Faruqe Hamim, O., Hasanat-E-Rabbi, S., Debnath, M., Shamsul Hoque, M., McIlroy, R., Plant, K., & Stanton, N. (2022). Taking a mixed-methods approach to collision investigation: AcciMap, STAMP-CAST and PCM. *Applied Ergonomics*, Volume 100.

ISO. (2015). *ISO 9001:2015 Quality Management Systems.* International Standards Organisation.

Law Commission and Scottish Law Commission. (2022). *Automated Vehicles - Final report.* London: HM Government.

Leveson, N. (2019). *CAST Handbook: How to learn more from incidents and accidents.* Massachusetts: Massachusetts Institute of Technology.

Leveson, N., Daouk, M., Dulac, N., & Marais, K. (2003). *Applying STAMP in Accident Analysis.* Massachusetts: Massachusetts Institute of Technology.

Monahan, E. (2019). *Engineering Documentation Control Practices & Procedures.* CRC Press ISBN 9780367401887.

Zenzic. (2020). *Safety Case Framework 2.0 - Guidance for Creators.* London: Zenzic.

Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring

Abstract

The proposed in-use safety and security monitoring scheme can serve as an essential feedback mechanism for continual improvement of how the AV safety assurance scheme manages safety. In-use monitoring data can support in identifying changes and assessing their impact. However, making a change without due consideration of the impacts to all stakeholders may lead to increased regulatory inefficiency, undue burden on manufacturers and operators and may ultimately lead to worse safety outcomes.

This document outlines a change control process to manage and implement change throughout the entire AV safety assurance scheme to formally capture all learnings and provide feedback to identify, assess and implement positive change.

Relevant Reports

- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 1 – Road Incident Taxonomy; https://doi.org/10.58446/mvuc1823
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 2 - Minimum Dataset Specification; https://doi.org/10.58446/nksn4732
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 3 - Safety Monitoring Framework; https://doi.org/10.58446/sgxq7004
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 4 - Post Event Investigation Process; https://doi.org/10.58446/egfa6491
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 5 - Outcome Reporting; https://doi.org/10.58446/qlpq9096
- Automated Vehicle Safety Assurance - In-Use Safety and Security Monitoring Task 6 - Data Privacy; https://doi.org/10.58446/dwll8689

TRL
Crowthorne House, Nine Mile Ride,
Wokingham, Berkshire, RG40 3GA,
United Kingdom
T: +44 (0) 1344 773131
F: +44 (0) 1344 770356
E: enquiries@trl.co.uk
W: www.trl.co.uk

ISSN: 2514-9652

DOI: https://doi.org/10.58446/bpdl3309

PPR2022