Off–Highway Automated Vehicles

Code of Practice

2021

TRL THE FUTURE OF TRANSPORT

Authors:	Ianto Guy, Rebecca Wilford, Peter Ball, Mark Courtier, Malcolm Palmer, Kirsten Huysamen and Peter Vermaat	
Report prepared for:	Innovate UK	
Project/customer reference:		
Copyright:	© TRL Limited	
Report date:	April 2021	
Report status/version:	Final	
Quality approval:	Richard Oliver (Project Manager	David Hynd (Technical Reviewer)

Disclaimer

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

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.

Contents amendment record

This report has been amended and issued as follows:

Version	Date	Description	Editor	Technical Reviewer
V1.0	14/04/2021	Published	Ianto Guy	David Hynd

Foreword

The off-highway sector encompasses a broad range of industries including mining, quarrying, agriculture, construction, and ports and airports. Automated vehicle technology has become commonplace within some of these industries, bringing with it many benefits for safety, efficiency and productivity. But it is important to keep in mind that the introduction of new equipment and the transition to new working practices should be carefully managed to ensure that unintended safety consequences do not cancel out the potential benefits.

Despite the widespread use of off-highway automated vehicles, there is currently no universal operational safety standard for all off-highway applications. Due to the wide range of use cases within the off-highway sector, there is substantial variation in the operational constraints and hazards encountered by automated vehicles. In addition, compared with on-highway, which has a highway code that can be applied to an automated vehicle driving system, there are no pre-defined rules for off-highway vehicles, such as speed limits or junction etiquette. The off-highway sector also has to deal with the challenge that many of the operations in this sector require automated vehicles to interact with a wide variety of objects in the environment, either because they block the vehicle's path (e.g. undergrowth or tree branches) or because engaging with them is part of the vehicle's primary function (e.g. harvesting or excavating). These factors present a significant challenge for developing specific safety standards for the use of automated off-highway vehicles.

To understand the different use cases, environments, and risks, TRL reviewed current relevant standards, literature and operating procedures for automated and manual workplace vehicles. Stakeholder engagement identified risks, current good practice, and potential safety requirements.

This draft code of practice seeks to provide high level guidance to organisations, in all sectors of the off-highway industry, on the ways in which working practices should be adapted to ensure that the adoption of automation is as smooth and safe as possible. The code is applicable to the broad range of environments in which off-highway vehicles are used and the different demands and risks of using automation in those settings. The aim is that this code will support safe practice, build public confidence, and encourage the cooperation between organisations across all industries employing off-highway automated vehicles. It is hoped that off-highway industries will use this code of practice as a starting point for discussion and build on the recommendations made here to develop comprehensive best practice guidelines.

Dr Ianto Guy
Project Lead, TRL

Contents

Using this Code of Practice

Section 1

Introduction

Understand how the code of practice can help you safely deploy off-highway automated vehicles

Section 2

Understanding off-highway automated systems

Defining how automation can be implemented safely. Understanding off-highway automated vehicle system capabilities, limitations, interactions, and identifying the safety protections that may be required

Section 3

Planning and implementing off-highway automated vehicle systems

Guidance for how to plan and implement off-highway automated vehicles with recommendations on the process; who to consult, changes to site design and activities

1. Introduction

1.1 Purpose of a code of practice

Automation brings with it many benefits for safety, working practices and productivity. As more sectors in the off-highway industry begin to adopt automated vehicles, it is important that the potential benefits are achieved, and that new risks are managed without introduction of unintended safety consequences. This code of practice is a practical guide to assist in delivering operational safety. It is relevant to any person who has a duty of care within the circumstances described in the code.

A code of practice outlines best practices. However, compliance with them does not ensure immunity from liability.

1.2 Scope and application

This code of practice provides guidance on:

- The implementation and use of off-highway automated vehicles (OHAVs) within work environments
- The identification and control of operational hazards introduced by these automated vehicles
- The development of safe working practices for these environments

This guidance can be applied to any size installation, from a single OHAV to highly automated sites where multiple and varied OHAVs are operating concurrently. The recommendations are relevant through all stages of development and use, from initial prototype and testing, through commissioning and validation, to operational use.

This code of practice contains high level guidance. It does not prescribe methods, techniques, or minimum performance requirements

1.2.1 Definition of an OHAV

For the purposes of this code of practice, an **off-highway vehicle** is defined in the following way:

- It primarily operates in any locations that are not an open public highway (this can be both outdoors and indoors)
- It is self-propelled – it has an onboard method of propulsion such as an engine or an electric motor
- It is land based

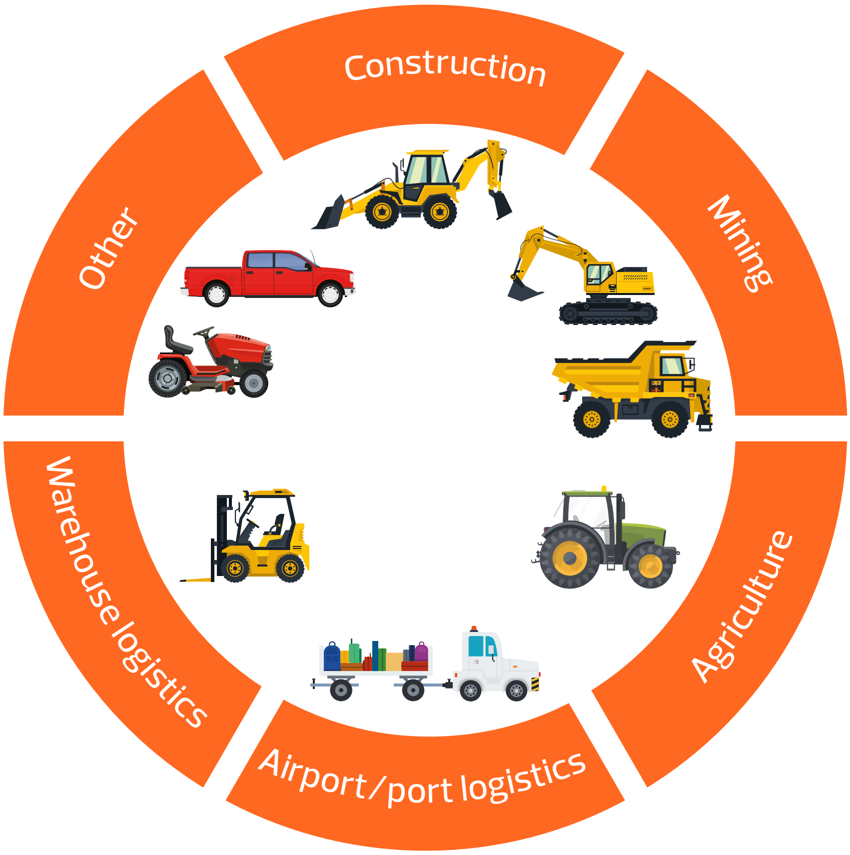


Figure 1 – Non-exhaustive examples of off-highway sectors and vehicles

Following on from this, an **off-highway automated vehicle (OHAV)** is defined as follows:

- It features an automated system that can fully or partially control at least one of the operational functions of the vehicle with minimal human intervention
- Automated control of the specified function(s) has the potential to cause direct harm to people
- The automated system controls the specified function(s) when required

Examples of an OHAV include:

- A fully automated haul truck operating in a mine – it has no on-board operator and the automated system can, with minimal supervision, perform all driving and operational functions.
- An agricultural machine with autosteering and automatic speed control, harvesting a field – it has an operator who monitors and adjusts the harvesting equipment to achieve the highest possible yield, whilst the automated system performs the speed and direction aspects of the driving task.
- A bulldozer with automated blade control – it has an operator who controls the driving functions, but the blade height is controlled by the automated system
- A fully automated vineyard pesticide sprayer – it has no operator and the automated system can perform the driving function and, optimise the pesticide application through management of the spraying operation.
- A fully automated warehouse racking picker – it has no operator and is capable of driving on the ground, climbing racking and placing/retrieving containers.

As the use of automated technologies expands, there may be new applications that need considering on a case-by-case basis. Even if they do not strictly fall into the definition in this section, the recommendations made in this document may still be relevant.

1.2.2 Exclusions

This code of practice only relates to activities conducted off-highway. For any activities performed on open public highways, the relevant on-highway legislation and guidelines should be applied. Also, this code of practice does not apply to:

- Aerial vehicles
- Water-based vehicles
- Any vehicle being used on an open public highway
- Remote controlled vehicles (unless they feature automated systems)

1.3 Who should use this code of practice?

This code of practice should be used by anyone who has a duty of care within a work environment featuring at least one OHAV. This includes any person who has functions and responsibilities for planning, designing, implementing, operating, or maintaining systems within the work environment. The code of practice may also be useful to developers and manufacturers of OHAVs, to gain a better understanding of the operational practices under which their machines should be used. Additionally, other groups of people may find this code of practice informative, such as:

- Emergency services
- Insurance providers
- Regulatory authorities
- Health and safety authorities

1.4 How to use this code of practice

This code of practice includes both recommendations and legal requirements. The use of the word "must" indicates the existence of a legal requirement, whilst the word "should" indicates a recommended practice.

The code of practice has been written to cover all implementations of OHAVs. As a result, certain recommended practices may not be relevant to specific implementations. Organisations should identify and evaluate all recommendations that are applicable in their circumstances.

1.5 Assumptions

This code assumes that users will have understanding and experience of:

- Health and safety management systems and reporting requirements
- Risk assessments and safety cases
- Off-highway vehicle operations

2. Concepts to support safe implementation of OHAVs

This section provides key concepts for aiding the safe implementation of OHAVs into a work environment. There are essentially two mechanisms for the introduction of an OHAV into a new or adapted worksite:

1. The integration of an available automated vehicle or vehicle system
2. The development of a new automated vehicle system

The approach to implementation may vary and, in each case, the vehicle may either be expected to operate in a permanent fixed work site or regularly transfer between sites. In the first mechanism, introducing an already available OHAV requires the organisation to understand the system's limitations and capabilities and tailor procedures, the worksite, and any supporting systems to accommodate safely the use of the new technology. The second mechanism may allow a top down approach where the overall objective for implementing the OHAV will define the system design and requirements. In most cases there are no standards or specifications for the development or approval for sale of these vehicles, so it is essential in both cases that the organisation operating these vehicles understands the operational design domain, the limitations of the systems, and how changing the responsibilities of the human operator changes the risks. These should then inform the acceptance testing for permanent installations or the preparatory activities when changing sites. Further details are given in Section 3.

Organisations looking to implement an OHAV should develop a safety case which provides evidence that the change or introduction of new hazards has been assessed and how the risks will be managed to be as low as reasonably practicable. Where information or guidelines are available and appropriate, best practice from other industries should be followed. Where it is not feasible to develop a full safety case, organisations are strongly recommended, as a minimum, to conduct and record a risk assessment identifying all the hazards and associated control measures. In the UK, it is a legal requirement for companies to perform risk assessments and, for companies of more than 5 people, the risk assessment must be recorded.

2.1 The operational design domain

An OHAV will be designed to operate under a specific set of circumstances. This is defined in the Operational Design Domain (ODD) of the vehicle and will be part of the product specification. The ODD will cover several aspects including: the acceptable terrain, operating conditions, presence of people or other machines, and any further information required to give a full description of the circumstances in which the OHAV can safely operate.

The term Operational Design Domain (ODD) has typically been used solely to describe the constraints under which driving tasks of on-highway automated vehicles may be undertaken. For the purposes of this document it is assumed that those driving tasks might include any vehicle operation that would previously have been under the control of a human operator, e.g. controlling the movement of an excavator bucket or the tipping of a dump truck. The ODD is a property of the OHAV and its related systems and should be considered fixed unless modified or changed, e.g. by the addition of functionality through updates to hardware or software. The following elements should be included in the definition of the ODD.

Static elements	Non-movable elements of the operating environment, such as a roadway or a fence.
Driveable area	Characteristics of the terrain the vehicle can operate on.
Environmental conditions	Environmental elements, such as weather, illumination, and connectivity.
Dynamic elements	Movable elements of the operating environment, such as the OHAV itself or people.

The table below presents examples of ODD considerations for each of the categories:

Category	Operational design domain considerations
Static elements	· Is the OHAV able to detect static obstacles? (e.g. buildings, rocks, lampposts) · Is the OHAV able to interpret static objects? (e.g. signs, markers)
Driveable area	· On what terrain is the OHAV able to drive? (e.g. dirt, asphalt, a field) · On what surfaces is the OHAV able to perform operational tasks? · What are the limits of the geometry of the driveable area such as incline, radius of the corner, width and height?
Environmental conditions	· In which weather conditions is the OHAV able or unable to operate? (e.g. high winds, rainfall, snowfall, fog) · Is there a minimum level of illumination required for the OHAV to operate? · To what level can the OHAV be exposed to different particulates? (e.g. sand, dust, smoke) · What are the connectivity requirements of the OHAV?
Dynamic elements	· Is the OHAV able to detect dynamic objects? (e.g. people, animals, other vehicles) · What speed can the OHAV travel at?

To implement an OHAV safely, the ODD should be compared with the expected circumstances in which the vehicle will operate. This is sometimes referred to as the use case and describes how the vehicle will be used, by whom and where. By comparing how the OHAV will be used and the ODD of the system, any limitations in capability can be detected and these will identify potential hazards or unsafe operations. Developing a full understanding of the ODD of an OHAV system will inform the other elements, systems, processes, or safety protections that need to be in place for safe operation. This process of understanding the system limitations needs to be repeated every time the activity or location of the activity (worksite) is changed.

Understanding the capabilities and limitations of an OHAV system for the specific worksite it will operate in is significantly more important with an automated vehicle than with a manned vehicle. With a manned vehicle there is the reasonable assumption that the driver or operator will be able to detect hazards and react appropriately when needed. With an automated vehicle, this has to be considered as part of the design of the system and operational controls, this is discussed further in Section 2.3.

Example

The ODD of an OHAV states it is able to detect static objects and stop. It is not, however, able to detect dynamic objects such as people or other vehicles. Understanding the specific scenarios where the OHAV is to be used will determine whether this is adequate or if additional safety measures are needed. If, for example, there is an access control system which keeps the OHAV and other dynamic objects separate, the existing capabilities of the vehicle may be sufficient. If this is not the case, then another automated system or human operator will be required to detect and respond to the dynamic objects.

2.2 Systems approach

To fully assess the risks associated with introducing an OHAV to a worksite, first decide how it might interact with other elements of the worksite. If there are other elements, then a systems approach is needed, where interdependencies between those elements are identified and fully understood. Each element (which is any component, system, structure, or actor) that is required to enable the complete system to function correctly and safely will have their own operational requirements, limitations and failure modes. These should all be considered in the context of the whole system, see Figure 2.

It is important to understand the impact of incorrect behaviour, or failure of any one element of the OHAV system and, where possible, use multiple layers of safety or redundancy. This should be proportionate to the possible risk of harm. For example, a worksite with a risk of collision between two unmanned vehicles may be considered to require fewer safety measures than that where manned and unmanned vehicles are operating together and, therefore, there is a significant risk of harm if a collision occurs.

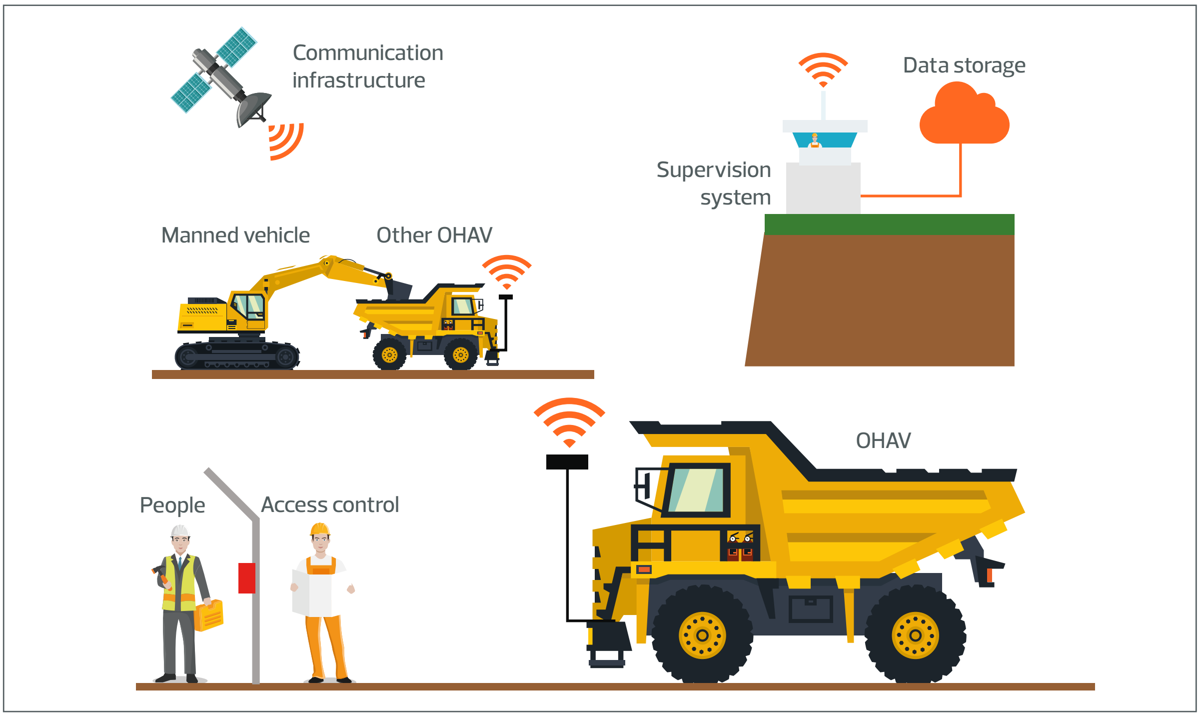


Figure 2. OHAV operating within an overarching system

Manned vehicles or machines	OHAVs may operate alongside, or interact with, vehicles or human controlled machines in the same worksite. These manned vehicles may be connected, allowing them to be monitored or to provide an information link with the OHAV. E.g. A manned excavator operating with an automated haul truck or a partially automated harvester transferring grain to a manned tractor and trailer.
Other OHAVs	Multiple OHAVs may operate in the same worksite without segregation. OHAVs may need to interact or cooperate on a task.
Staff	Workers that are directly supporting the OHAV or working independently may be operating in the same space
Visitors	There may be people that have access to the work site on a limited or temporary basis such as contractors or visitors. E.g. An OHAV operating on land with a public footpath.
Communications infrastructure	The hardware and software which enables data to be transmitted between vehicles (V2V), infrastructure (V2I) or any other system (V2X). This may allow one- or two-way communication. E.g. Wi-Fi, a Global Navigation Satellite System (GNSS) or mobile networks.
Access control systems	Methods of restricting the movement of people, vehicles or machines to a certain area. E.g. Fences, ditches, geofences or key-card controlled areas.
Supervision stems	Systems which plan, direct, monitor or inform the actions of other parts of the overarching system. E.g. Control rooms, task planners, mapping services, fleet management systems, CCTV systems or analytical monitoring systems.
Data storage	Systems which record information from any, or all, of the overarching system. E.g. On or off board data recording systems for vehicle, systems, driver or camera data; incident and near miss recording systems; maps; or CCTV recordings.

2.3 Safety protections

In a traditional off-highway vehicle, the operator is responsible for performing operational tasks as well as monitoring the vehicle and the environment to ensure safe operation. In most cases, they are therefore the safety protection. When automated systems take control of some of these tasks, the automated systems become the primary, and potentially only, safety protection. Therefore, understanding the capabilities and limitations of the automated system is key to understanding what safety protections are required for all hazards that may occur. In the case of an automated vehicle there may be no human present to monitor for these hazards or to react in the case of an event. Even when there is a person present, they may not be able to respond appropriately and in time if their attention is elsewhere and, therefore, should not be relied on as a safety protection.

Example: A system for collision avoidance involving a person

Although an automated tractor can drive and steer itself, it carries an operator whose primary task is adjusting a towed harvesting implement to maximise yield. A safety system is required in case someone walks in front of the tractor. One option is for the operator to be vigilant and ready to push an emergency stop button. A second option is that the OHAV could have a hazard detection system which can detect the person and stop the tractor to prevent a collision. Another option, incorporating the wider worksite system, is a suitable barrier to prevent the person from gaining access to the worksite and therefore being able to step in front of the tractor.

The operator

OHAV collision detection and avoidance system

Barrier

Each individual task carried out by the OHAV's automated functions should be reviewed and at least one safety system applied to mitigate any hazards associated with the task, failure of the components involved in the task, degradation of performance or misuse. Where practical, and when the risk of harm is significant, multiple safety systems should be applied to introduce redundancies. For each hazard, safety protections should be identified. These may be human, automated, physical or a combination thereof. They may be located on the vehicle or remotely. Where safety protections are remote and rely on a communication link, the OHAV should still be able to respond safely should the link fail.

Tasks that may be undertaken by the automated functionality of the OHAV and which require a safety protection to be established include:

- Dynamic driving tasks (e.g. steering, forwards or backwards motion)
- Object detection
- Collision avoidance
- Monitoring environmental conditions
- Securing load
- Route or task planning
- Operational tasks (e.g. harvesting, drilling, lifting)
- Incident detection (e.g. impacts, near misses, fire)
- Monitoring the correct functioning of the OHAV

3. Planning and implementation

There are many aspects that need to be considered to achieve the safe implementation of an OHAV system. These apply for the use of vehicles on both new and existing worksites. This section discusses the many new considerations that are required and new processes and procedures that will need to be created during the planning and implementation phases. The areas discussed are:

- Considerations during the design, definition and creation of the worksite
- Consideration of the operations and activities to be conducted
- Activities required during initial implementation or introduction of an OHAV system
- New processes and procedures that will need to be created for incident management, performance monitoring and managing changes
- Who should be consulted throughout this process

3.1 Consultation & review

For successful and safe implementation of new automation technology or systems it is important that developers and implementers discuss the implementation with all relevant parties. This should be as part of the planning phase, throughout system development and implementation stages, and during subsequent use. Consideration should be given to how all staff, and others who may be on-site, will be affected. Therefore, communication and co-operation are essential.

3.1.1 Workforce

The implementation of vehicle automation may affect the workforce at all levels from managerial to operational, whether or not they are directly involved with site activities. Part of the implementation process should include consultation with the workforce who can provide a good source for the practical understanding of the new or changed hazards and to help identify aspects that have altered such as:

- Roles and responsibilities
    - New roles and responsibilities (identify appropriate staff requirements)
    - Roles which will change or be affected (identify appropriate staff requirements)
    - Roles no longer required
    - Management activities which will change
- Working practices
    - New methods which may create new hazards
    - Processes which will change (in particular, hazards)
    - Methods which will no longer be used
    - How new and modified methods will be managed (skills development)
- Risk management or control interventions
- Requirements for site design
- Requirements for training, supervision and awareness
- What standards and statutory obligations (existing or new) affect working methods

Management should ensure the required resources (time, budget, skills, materials) are available during the development and operational stages to ensure a safe and successful implementation. The following activities should be conducted:

- Education for all personnel to give them awareness of the implementation, the changes to risks, working practices and supervision that may be required.
- Education for all relevant staff on the safety protections required by the automated system and how and why these may differ from those required by manned vehicles.
- Implications for visitors to the site, such as briefings and supervision, where there is potential for interactions between visitors and automated vehicles.
- Staff whose roles change will need appropriate training for altered or new working methods and responsibilities. Competency should be assured for those roles.
- Supervisory and managerial staff will need to understand the implications of the new technology and the altered responsibilities that staff will have.
- Senior staff should commit sufficient time and resource to ensure that competence and awareness has been achieved and is maintained.
- Health and Safety staff will need training and awareness for development of and changes to operational policy and procedures, and for any incident investigations required.

3.1.2 Other stakeholders

Consultation should involve any other stakeholders who might be affected by the implementation of automated vehicles to the worksite. These could include:

- Contractors working within the site
- Emergency services who may require access to the site
- Local and regional councils, if affected
- Landowners
- Other local parties affected

OHAVs are a new, and rapidly developing, industry. Therefore, worksite and operations developers should engage with other parties during development. Key parties are the manufacturer of the OHAV and of all related subsystems. Manufacturers are best equipped to explain the requirements and limitations of their products. Some manufacturers will also require worksite and operations developers to collaborate in the design phase to ensure that a specific product or system under development is suitable.

3.2 Design & planning of worksite

3.2.1 Assessment of site and existing infrastructure

As part of the planning and implementation phase, developers should assess the worksite's suitability for OHAV implementation. This should include work-specific and other physical infrastructure, and communications infrastructure.

Hazard and risk analysis may identify that changes to existing worksites are required to control the risks introduced by an OHAV system. The following may be needed:

- Introduction of new infrastructure.
- Changes in the specification of infrastructure.
- Changes to the importance of suitable infrastructure that is already present because it has become a safety control (e.g. as a barrier).

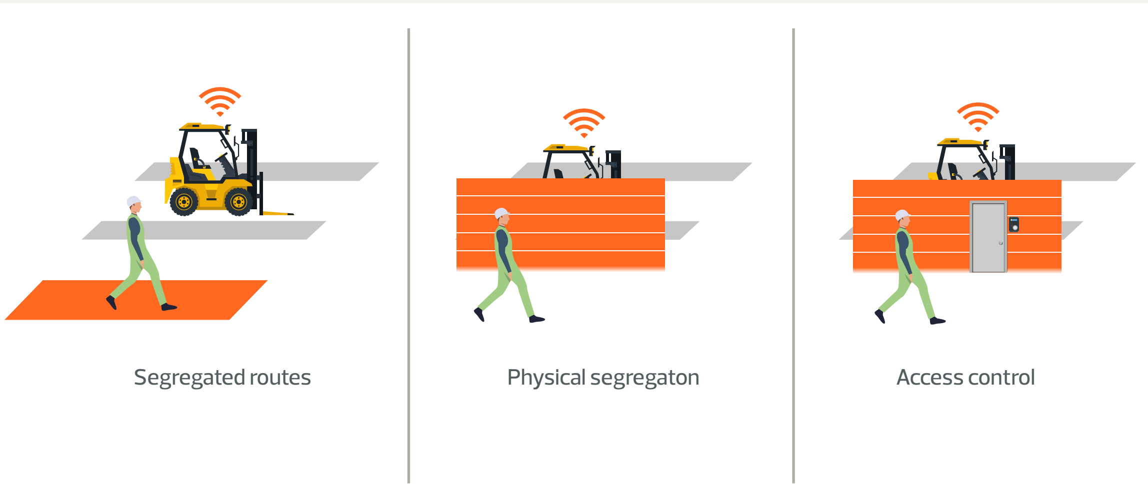
Safety controls for automated systems may include:

- Infrastructure
    - Barriers
    - Signs, markers or cones
    - Access control
    - Communication and GNSS systems
- Layout
    - Segregated areas including for works activity, storage, maintenance or testing
    - Fixed or defined routes which may reduce the risk of collision with manned vehicles and people

3.2.2 Minimising interactions with workers

Wherever possible, worksite and operations developers should aim to minimise interactions that OHAVs have with personnel and manually driven vehicles. Creating a system that contains only OHAVs results in many safety issues being eliminated, because there are no people in the primary work area who can be injured. Whereas, introducing personnel and manually driven vehicles into an OHAV environment typically increases the complexity of the system, and therefore the likelihood of conflict. Whilst complete removal of interactions cannot always be achieved, depending on the worksite and works activities and processes, interactions should be minimised to create a safer work environment. This can be achieved using infrastructure, operational processes, or a combination of the two.

Infrastructure methods for minimising OHAV interactions with workers



3.2.3 Communications network requirements

Many OHAVs will depend on external data communicated wirelessly via local wireless systems, mobile data networks and satellite data networks. System and network requirements will vary significantly between implementations. If an OHAV requires communication links to maintain operations, it should be designed so that there will be a safe outcome if that link is lost. Communications requirements should be considered during site design to maximise system uptime. This benefits both the operation of the OHAV and the safety of the system by reducing the need for human intervention to restart or recover vehicles and thereby the hazards associated with these activities.

The performance of any wireless communication system (including wi-fi, 3G, 4G, 5G, satellite networks, GNSS) will vary depending on location around the site, local climatic conditions and, in many cases, other competing demands placed on communication system, especially if it is a public shared network. The demands on public networks may vary unpredictably depending on local events. During site design and planning, consider how to prevent or mitigate problems they might cause the operation of the OHAV.

Example

An OHAV operating on a farm uses a 4G mobile network to stream video to a control room for monitoring purposes. A music festival is held nearby over one weekend, causing significantly greater demands to be placed on the 4G mobile network in this area, limiting the bandwidth available to the OHAV. This causes the quality of the monitoring video stream to decrease significantly, to the point where the monitoring can no longer be successfully performed. The OHAV has to be stopped for the weekend because monitoring is required for its safe operation.

Temporary installation, for the duration of the event, of additional capacity base stations could meet demand. However, this places the onus on the mobile network/event organisers. A temporary solution within the control of the OHAV operator would be to install a Wi-Fi connection from the vehicle to a nearby base station (e.g. at the side of the field), using a directional connection to stream to a fixed broadband connection.

3.2.4 Change of site design

Work sites are likely to alter over time and the capabilities of OHAVs are likely to change as the technology matures; therefore, changes to site design may be required. Ideally, predictable, or routine changes should be captured in the planning and implementation phase. Changes not foreseen, or reactive should be undertaken through the change management process, as detailed in Section 3.7.

3.2.5 Physical infrastructure

3.2.5.1 Safety Barriers

Barriers can be used to achieve two safety critical objectives: restricting runaway OHAVs and restricting access of people and manually driven vehicles to the OHAV operating area. Whilst physical barriers such as fences or walls may provide a simple solution, they are not the only type of barrier available for controlling OHAVs, as illustrated in Figure 3. Unlike a physical barrier, virtual barriers can be used to trigger the emergency brakes on an OHAV that attempts to leave its area, preventing potential damage to the machine from impact into a physical barrier. Natural barriers can also be used in place of fences or walls, these might provide a cheaper and more effective system. When considering safety, economic cost and operational performance, a combination of these barriers may provide the best overall system.

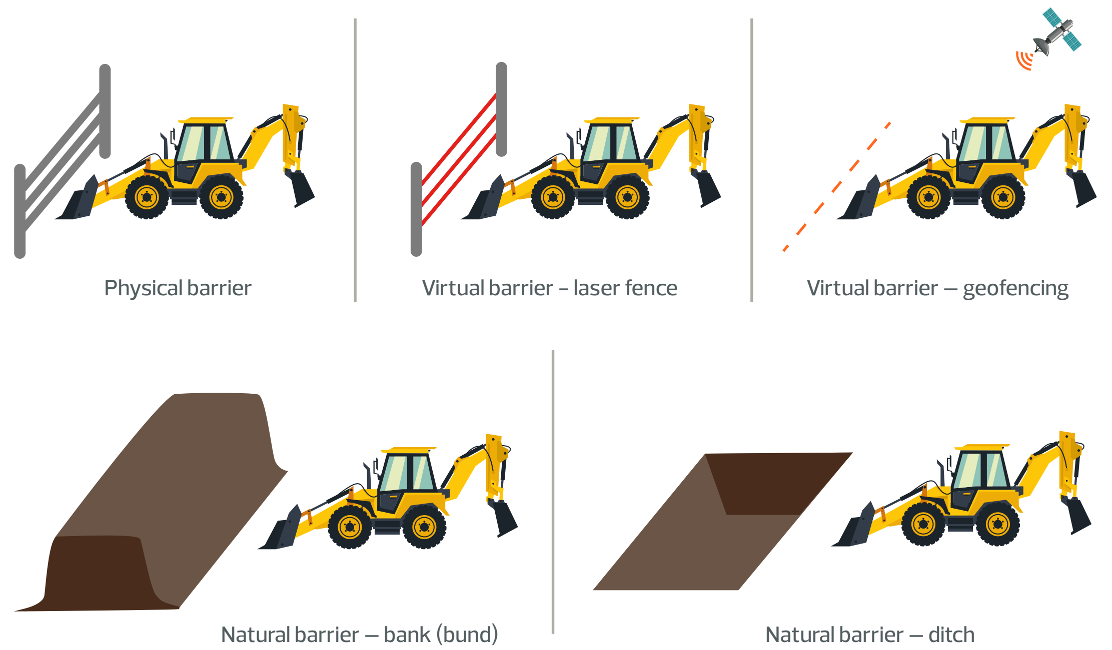


Figure 3: Potential safety barriers to be used on OHAV worksites

The procedure should be considered for when barriers are breached by OHAVs, manned vehicles or people. Virtual barriers may be easy for a human to cross without realising they have done so. In that situation, a lighter weight pedestrian fence might be used in parallel with the virtual vehicle barrier. Also, consider whether:

- Multiple breaches of barriers could occur simultaneously
- How to confirm an area is clear
- Whether an in vehicle human operator might be harmed when the vehicle reaches the barrier

3.2.5.2 Roadways

Roadways within a worksite should be suitable for the OHAVs using them, based on the machine itself and the operating parameters of the system as a whole. For example, designers should ensure that there is adequate space for OHAVs passing in different directions. Good OHAV performance is dependent on the roadway or vehicle path satisfying the operating parameters of the Automated Driving System (ADS), so care should be taken to achieve this during implementation and use. Within a worksite, temporary infrastructure may be required, for example buildings, barriers and signs. These should be installed so that required clearances are maintained and, where necessary, they can be identified correctly by automated sensors. Site audits should be undertaken before operations commence, to ensure that roadways and other infrastructure has been constructed to the intended layout and materials, etc.

Example

An OHAV is required to travel between two parts of a worksite through a narrow gap. The OHAV has a minimum operating width of 5 m but some overgrown bushes mean the gap is now 4.9 m. A manually driven vehicle would proceed through the gap without issue. However, the OHAV stops at every pass and has to be given permission by a remote operator to proceed.

The requirement on the remote operator to habitually give permission creates a risk of complacency which could result in instructing the vehicle to continue without thoroughly checking the path is still safe.

Where possible, separate routes should be provided for automated vehicles, to minimise interactions between automated and non-automated vehicles.

3.2.5.3 Pathways

To minimise interactions, pathways should be utilised whenever personnel are required to be within the OHAV area. Where possible, there should also be safety barriers between the pathways and OHAV roadways. In areas where it is necessary to have interaction between personnel and OHAVs (such as within service areas) pathways should be incorporated which only allow the necessary interaction.

3.2.5.4 Access

Access requirements into automated worksites should be evaluated to ensure a safe worksite design. Consideration should be given to the types of person who may access the area (e.g. personnel, contractors, public) because this will affect the safety requirements. It may be appropriate to use access control systems to restrict and log any people or vehicle access.

In some circumstances, manually controlled vehicles may need to enter or pass through automated worksites. If so, a dedicated crossing point should be considered to better control the process. Depending on the frequency that these events occur, the crossing point could be temporary, for example incorporating movable barriers

3.2.5.5 Placement of other infrastructure within the OHAV area

Consideration should be given to other infrastructure within the OHAV area. The placement of areas such as fuel facilities and service zones should be appropriate, based on the OHAVs involved and the road layouts. In some cases, it may be required that facilities (buildings or other areas such as supervisor control rooms and service areas) where personnel work will need to be located within the OHAV operating area. These facilities should be located to ensure adequate operational performance whilst maintaining safety for the personnel using them. Additional safety protections may be required around these facilities.

Design of infrastructure should also consider the safety and communication systems involved with OHAV operations. For example, the placement of a building could affect the GNSS accuracy of an OHAV or reduce its field of view.

3.2.5.6 Signage

Signage should be incorporated around an OHAV worksite to inform people of the automated vehicle operations, and the safety processes that need to be followed. However, signage alone should not be relied upon as the only safety protection.

3.3 Operations & activities

A fundamental concept that should be applied when introducing an OHAV to a site is to plan and prepare for the different hazards associated with the automated activities. A manually driven machine cannot simply be replaced by an OHAV. When developing new or updating an existing worksite for the introduction of OHAVs, working processes and procedures will require revision or creation, particularly those that influence safety. Sufficient planning and consultation should ensure problems are identified pre-emptively, staff know what actions they need to take for work activities and activities are performed consistently. Also, planning will identify the information that should be collected as part of ongoing monitoring and inform continuous improvement programmes (see Section 3.6).

Existing worksite guidance and procedures for operations are likely to require extensive review and updating, to ensure that they are suitable for:

- How automated vehicles operations are different to manual vehicle operations (if relevant)
- The capabilities and limitations of new automated vehicle operations
- Staff, visitors and vehicles within the site where
  - Intentional interactions occur
  - Unintentional interactions could occur
- Changes in how to respond to events and, in particular, incidents

To design and operate OHAVs safely will also require new processes and procedures to be created and implemented. The following should be considered:

- Operator training
- Regular checks such as daily vehicle checks
- Fail safe strategies and abort criteria
- Visitor procedures
- Travel to and from the site
- Data and cyber security controls
- Maintenance and repair

Processes should be developed in collaboration with staff, OHAV manufactures and developers, and other relevant stakeholders. They should be reviewed periodically and outline each party's responsibilities. All processes should be supported by training.

3.3.1 Training

Staff consultation on the implementation of automated systems, and liaison with system providers, will have identified the training that will be required to implement the new or revised working practices. The required outcomes are that staff can, where appropriate, demonstrate competency:

- To operate the automated equipment safely
- To work in proximity to the automated equipment
- To monitor and supervise other staff involved with, or working in proximity to, the automated equipment

Training needs will vary according to whether the staff have direct interaction with the automated vehicle or are monitoring, supervising, or managing systems or personnel. Competency for all roles should be evidence based and verified before work commences. Training content is likely to cover areas including:

- Hazards and risks, the controls to be applied, and the job steps necessary to complete tasks safely and correctly;
- Safe operations of systems, including functionality, capabilities and limitations;
- Specific tasks to be undertaken;

- Anticipating the need to intervene and, if necessary, take manual control;
- Worksite and work procedures, for example: routes, particular dangers, speed limits, parking and loading areas;
- Emergency procedures;
- How and where to report faults, hazards or incidents;
- Structures that will apply for management, monitoring and supervision.

Refresher and update training should be considered, particularly when system updates are planned which will affect operations or introduce new hazards. Maintaining training records may help identify when refresher training might be needed.

3.3.2 Daily checks, inspections and resupply

Automated vehicles are likely to require daily checks and inspections, covering vehicle-related elements, any additional checks required for the automated systems, and checks of operational mechanisms. Also, there may be a requirement to resupply consumables (e.g. fuel, water). Electrically powered automated vehicles may require connection to charging units. The scope and extent of these checks and inspections is likely to be specified by the system provider or developer.

These checks and inspections are likely to require direct access to the vehicle by the maintaining staff. Therefore, it is essential that there is a thorough procedure in place to confirm that the staff member is not exposed to risk from unanticipated action or movement by the vehicle. Potentially, the procedure will involve control room operators or system supervisors and should ensure that no automated activity can be initiated, either remotely or by the vehicle, without awareness and agreement by the maintenance staff member. To maintain the safety of personnel, consider appropriate use of safeguards such as:

- Interlocks
- Lockouts
- 'Permit to work'

Routine checks, inspections and maintenance may take place within limited and defined areas of the work site, potentially with controls restricting access. Where any checks, inspections and maintenance work are carried out away from these defined areas, the staff involved should not be at risk from the movement of other automated vehicles. For further details on maintenance, see Section 3.3.7.

Checks of vehicle systems may be carried out remotely. If this will happen, there should be clear measures in place to ensure and confirm that the vicinity of the automated vehicle will remain clear to prevent any unintended interactions.

3.3.3 Human involvement in control

Automated vehicles reduce the involvement of humans in the automated tasks but, in many cases, do not remove the human completely. Like all machines, OHAVs will suffer failures which will need to be handled safely. Additionally, OHAVs may operate on challenging terrain where the vehicle may get stuck or find a route or operation impossible to complete. A person may be required to monitor or assist the automated systems for specific tasks or in the case of an event such as a failure or incident. The system failure mode, abort scenarios and potential actions thereafter, of the automated vehicle should be understood as part of planning for implementation. In many cases the role of the human will be part of the safety system and risk mitigations. Where this is the case, the design of the operations and activities involving humans should consider human factors limitations and not place unrealistic demands on staff.

- The change in role from being in control of the driving task to monitoring it has proven to reduce attention and alertness (i.e. increased drowsiness). This results in a loss of situation awareness and the driver becoming out-of-the-loop, so they are less likely to respond quickly and accurately to safety critical events. This should be considered when assessing the appropriateness of monitoring activities as a safety measure. The risk of inattention can be reduced by systems that require interaction or provide stimulation such as responding to simulated alerts. Alternatively, an automated system may need to verify the presence and readiness of the human operator to be able to continue with its operations.
- When transferring control, the OHAV should provide sufficient time for the human operator to be able to achieve situational awareness.
- The working hours and shift durations for staff involved in these activities should be appropriate to the demands of the task and the level of stimulation the task provides. This might be significantly different between similar activities using a manned or automated vehicle.
- An operator controlling several OHAVs, or independent automated activities, may become overloaded if many require attention at the same time. If this is a possibility, a method of handing over control of some activities to another operator should be considered.
- Implications for continued safe operation of the worksite should also be considered, potentially requiring an escalation plan. If multiple, simultaneous, failures occur, it may be necessary to implement a system stoppage.

Where human monitoring is required, staff will need to remain attentive and alert to respond to any failure. During planning for implementation, consideration should be given to human factors limitations with this type of monitoring. For example: if an OHAV exhibits a high rate of false positives it may regularly abort its activities and require restarting by a remote operator. This requirement to habitually give permission to restart creates a risk of complacency, which risks the vehicle being incorrectly restarted when the safety critical object is genuine.

The system should notify monitoring staff that it has failed or has halted. Additionally, other staff should be permitted to initiate a system stop should they identify a failure, an imminent failure or incident that had not, so far, created a warning to operators. That system stop should create a notification to system operators.

All staff should be aware of the procedure for initiating an emergency response if they identify that harm has occurred to people on-site. For details on emergency procedures, see Section 3.5.2. For considerations on vehicle recovery after failure or an incident, see Section 3.5.4.

Example

A tractor has automated speed and longitudinal steering control but requires a human operator to:

- Drive the tractor manually to and from the field
- Monitor the OHAV in automated mode to ensure it is operating effectively (e.g. monitor an interface)
- Monitor the environment when the OHAV is in automated mode to determine when to override the system and take back manual control (e.g. reaching the boundary of the field and avoiding collision with static or dynamic elements such as pylons or people)

If the human operator does not fulfil these requirements, an undesirable event such as a collision may occur. To prevent this, the OHAV should ensure that the driver is fulfilling their role and responsibilities (e.g. by checking the operator is present with a seat pressure device, monitoring the operator's alertness with a camera-based system or warning the operator if they are exceeding the appropriate working time for the task). If the system believes the human operator is not adhering to one or more of the operator requirements, the system should act by shutting down or alerting the human operator to revert their attention back to the task.

3.3.4 Visitors

Site constraints may not prohibit or prevent public or other unauthorised access to the works site. That level of access will have significant implications for the capabilities required of the OHAV and for monitoring requirements.

Even where access is restricted, there are likely to be instances when visitors are allowed onto the site. These visitors might include:

- Regular contractors working on-site
- Contractors occasionally working on-site
- Visitors, such as inspectors or observers
- Emergency services

Where segregation (site demarcation, access routes separate from automated vehicle routes, etc.) cannot be maintained, part of the implementation risk assessment and staff consultation exercise should involve identifying likely visitors to the site and developing appropriate procedures, in particular determining whether unsupervised access will be permitted. All site visitors should undergo a briefing or induction session as appropriate, and any staff hosting visitors should be aware of their additional responsibilities, including emergency procedures.

Consideration should be given to how effective real-time communication with visitors can be maintained.

3.3.5 OHAVs travelling to and from work sites

The automated vehicle may not remain permanently within defined areas of the works site. It may need to travel outside of that area of the site, for various reasons, particularly if routine maintenance, storage, etc., is required. Therefore, protocols should be developed to maintain low risk operation during these transit journeys.

- If the journey involves use of a public highway, then the automated vehicle must either be under direct human control or be operating in accordance with relevant standards or regulations
- For other journeys, appropriate planning will require that either the vehicle is operating under direct human control or, if operating automatically, that the ADS is suitable for any additional hazards outside of the usual work area

3.3.6 Data and cyber security

Data and cyber security are a substantial topic and this code of practice cannot cover all risks and potential control mechanisms. Instead, it outlines key types of data and security considerations.

Any automated system is likely to need regular access to data external to the system. The security of this data interchange will depend on the use and content of the data. Examples include:

Strategic operational data	External inputs providing instructions to the automated system, for example: operational limits (e.g. extent of field to be harvested), start and stop times, etc.
Tactical operational data	Data assisting the automated system in the performance of its intended task. This could include data from sensors, e.g. using GNSS positioning data to locate the system.
Operational output data	Data generated by the automated system. This may be performance data or diagnostic data to be used should an unexpected event occur. In some cases, data output may be the product of the automated system, for example automated survey machines.
Data for maintenance	For example, software updates.

This data may vary with respect to its importance in maintaining the safety and security of the OHAV or the organisation's operations and may be classed as:

Safety critical data	Data which, if manipulated, could lead to the automated machine acting in a way that could endanger life or property. This would include any data that would affect the software controlling the automated system.
Operationally critical data	Data which, if manipulated, could compromise the operation of the automated system.
Commercially sensitive data	Data which, if revealed to parties other than those who have the right to access it, could compromise parties using the automated system.
Personal data	Data which relates to individuals. Personal data are subject to significant legal restrictions which vary between jurisdictions. Probably the best known of these is the EU General Data Protection Regulation (GDPR) (EU, 2016).

In all the above cases, an interface is needed to the automated system to enable and control the flow of information. These interfaces could be:

Physical	A socket to which an external device can connect explicitly for the purposes of data transfer, an example being the On-Board Diagnostics (OBD) port required in modern passenger vehicles.
Wireless direct	Where an external device connects using a point-to-point wireless connection like Wi-Fi or Bluetooth
Wireless indirect	Where an external device connects using a public network, most typically a cellular data connection.

This diversity of interfaces and data types exposes multiple potential attack surfaces which could be used to mount a cyber-attack.

3.3.6.1 Securing data interfaces

It is highly likely that OHAVs will require a means for external systems to access the on-board systems, which in turn will require one or more external interfaces to be present. These interfaces are vital to the long-term function of the vehicle and include providing access to on-board diagnostic and maintenance data, access to data gathered by the vehicle during operation, updates to parameters used by the vehicle, and software updates to the on-board systems. Any unauthorised alterations made could adversely affect system operation and, potentially, include the introduction of new risks or taking direct control of the system.

By their nature, data interfaces allow access to the systems being interfaced, so are a natural attack surface for those wishing to gain unauthorised access to system data. It is therefore imperative that the interfaces are secured to a level appropriate to the potential harm that interference (accidental or intentional), or malicious access, could cause.

Irrespective of what interface is used, system developers should provide security measures on these interfaces. Measures which should be considered include:

- Limiting physical access to interfaces, for example placing connectors behind locked or screwed down panels. Note that this provides some protection against casual or unintentional access but is wholly insufficient as a prime means of preventing malicious access.
- Use encrypted access, to a reasonably high standard and following industry standard guidelines, is now commonplace and easy to implement.
- Authenticate users and devices attempting access, using industry standard authentication processes.

- Audit-trail all accesses to internal systems in the vehicle, particularly those which are considered safety critical.
- Use bands designated for specific use cases, for example the ITS-G5 band reserved in Europe for vehicular safety applications. Most wireless interfaces use one or more of Industrial, Scientific and Medical (ISM) bands, e.g. Wi-Fi, Bluetooth etc. These bands are of necessity shared access and cannot guarantee easy access.

To ensure that best practice is followed, it is recommended that a Cyber Security Management System (CSMS) is implemented during development. This is a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks. More information on the use of a CSMS can be found in Section 7 of the UNECE regulation 155 (UN, 2021a).

3.3.6.2 Updating software securely

The data used by an automated system during its operation should always be considered safety critical to the extent that the OHAV itself is considered safety critical. This is particularly important where the operating software can be remotely upgraded (so-called Over-The-Air or OTA updates). An appropriate level of security should be designed into the whole system from the start of development, for example as defined in PAS 1885:2018 (BSI, 2018). Section 7 of UNECE Regulation 156 (UN, 2021b) specifies requirements for OTA updates for type-approved vehicles and is also a useful source of information.

- Operating software should always be digitally signed, and the digital signature checked every time the software starts up
- All updates should be audit-trailed and recorded, with a facility to roll-back any updates. OTA updates should only be via an authenticated connection
- The design of the on-board systems should apply a defence-in-depth approach, with a layered security architecture designed in from the start

3.3.6.3 Data protection

Any data stored on the OHAV may fall under the legal protection of private data if the data can be linked to an individual, as defined in various pieces of legislation, e.g. GDPR in Europe (EU, 2016) or the DPA (Data Protection Act) 2018 in the UK (Great Britain, 2018). Details of relevant documents are provided in Section 4.2.

3.3.7 Maintenance and repairs

OHAV's are multi-system technologies incorporating mechanical, electrical and electronic hardware, on-board software packages, and communications systems. They are potentially integrated into a system containing other external infrastructure including barriers, and communication and control networks. All aspects will require frequent and scheduled maintenance and are likely to require ad hoc repairs while in service.

Despite the practicalities of the two being potentially quite similar, maintenance and repairs are different to changes which may occur to improve the system. Maintenance and repairs keep, or return the OHAV to, the expected level of performance. Changes can introduce new functions, responses or behaviours which cause the OHAV to exhibit a new type of performance. Maintenance and repairs should have documented processes and procedures whereas changes should use a change management process (see Section 3.7).

In many cases, the OHAV will not have a human on board. This means there is no human to report poor performance, unusual noises, excessive vibration, or other triggers for maintenance and repair. A combination of scheduled maintenance, diagnostic information from the OHAV and human observation will be required to keep the OHAV in good condition. This is important for productivity and safety through reliable operation but also by reducing the number of vehicle recoveries required, which may be a hazardous activity.

All maintenance and repairs should be conducted by trained operatives only. Their training should consider the location where the maintenance and repairs are conducted.

3.3.7.1 Physical maintenance and repair

The OHAV should be maintained in a physical state which is safe, reducing risk to a level that is as low as reasonably practicable (ALARP), and suitable for the operation in which it was designed to be used, and will not cause the OHAV to fail in achieving the designed performance specifications.

All OHAVs should be routinely scheduled for servicing or monitored by appropriate technology to determine the level of wear or damage to physical components, the likely date for their replacement and functional safety. All repairs, maintenance tasks and scheduled services should be logged and processed by the organisation for future reference. Calibration and testing should be conducted after each inspection or scheduled service. These processes should be established within the organisation.

3.3.7.2 Software updates and maintenance

OHAVs rely upon the integrity of their control and communication software and, over time, this software will require updates or upgrading. Software updates and maintenance should be treated as routine as physical servicing. Testing to confirm the performance after a software update should be integrated within the OHAV servicing procedure. This should include the whole system including any communication and worksite systems to ensure that the hardware and software systems are correctly set-up, calibrated and function together as specified.

Any software update could potentially affect the expected behaviour and therefore safety of the OHAV. Where there is a written procedure with clear confirmation testing, some software updates may be considered as a maintenance activity. If there is any doubt on the safety implications of the software update or additional assessment or testing is required then a change management procedure should be applied (see Section 3.7).

Software package updates from a third party should not be ignored or delayed unless an assessment has been undertaken revealing reduced performance or an increased risk to life and property. To reduce risks to ALARP, software updates should be scheduled for when the vehicle is not in operation and, preferably, is in a service or maintenance area.

All software updates and versions should be logged for future record.

3.3.7.3 Maintenance, repair and service areas

Repair of the OHAV may be required while the vehicle is within its designated area of operation. A procedure should be developed, alongside the safety case and risk assessment, for such an eventuality. The area where the repair is conducted should be isolated temporarily from the operational area to prevent other vehicles encroaching on the repair area. This area should be clearly marked and this change should be communicated to all relevant personnel.

For some operation areas and sites, it is likely to be safer to retrieve the vehicle and place the OHAV in a service or maintenance area for dedicated support. For information on vehicle recovery, see Section 3.5.4. Retrieval to a segregated area minimises the likelihood of an interaction between personnel or other site vehicles and machines with the faulty, stationary, or malfunctioning OHAV. These areas may have the added benefit of including dedicated OHAV maintenance equipment, which might not be portable or safe to use in the operational area.

3.3.7.4 Maintenance and repair of infrastructure

The operation of, and the safety protections for, the OHAV may be dependent on infrastructure external to the vehicle. The maintenance and repair of this infrastructure will therefore be as important as the maintenance and repairs to the vehicle itself. This infrastructure may include:

- Safety barriers
- Roadways
- Communications systems
- Access controls
- Signage

Processes and procedures should be developed to monitor the condition of, maintain and repair this infrastructure.

3.4 Initial implementation

3.4.1 Validation

The initial implementation should include a thorough validation process to ensure that the OHAV and all related systems meet the operational needs. Validation is separate to verification, which checks that something was built as designed.

For systems as complex as OHAVs, validation is very challenging. This is due to the number of subsystems, the potential complexity of each subsystem and the wide variety of scenarios that can occur in the real world.

When an OHAV has been developed for a specific organisation or will be used on a permanent site, there should be initial acceptance testing where the expected operations and safety systems are tested on site(s) as they will be deployed. The outcomes of these tests should be documented and any shortfalls in the OHAV system, operational processes, or training, should be identified and addressed. This should then be followed by ongoing performance monitoring (see Section 3.6) and reacting to incident reports (see Section 3.5.5) to detect and act on flaws in the system that occur in operation. These might be caused by unforeseen real-world scenarios or the vehicle not performing as expected.

The provider of the OHAV and supporting systems may be engaged in both the initial acceptance tests and the outcomes of ongoing performance monitoring and incident reporting. This may be of particular mutual benefit for less mature systems or where OHAVs are operating in new or unusual environments.

3.4.2 Multiple worksites

For some use cases, the normal operation of the OHAV will involve it regularly being deployed on new worksites. Before operation on a new worksite commences, the suitability of the site should be assessed. This process should consider the site, the ODD of the OHAV, the scenarios for which the OHAV has already been validated and how the new site differs to previous sites. Ideally this should be conducted in tandem with the design of the worksite and should identify what adaptions to the site, safety protections or additional validation tests are required for safe operation for the OHAV. Assessing the suitability of the site is likely to be a combination of desk-based planning and a survey of the site to check real world conditions. This may include the ground conditions, weather, lighting, and the radio frequency environment.

3.4.3 Transition between manned and automated operations

Where automated operations replace manned operations there will be a transition period where the switch between the two approaches occurs. Even if this occurs as a single process where the whole manned operation is replaced by an automated operation, a period of adaptation and familiarisation will be required. Alternatively, it may be a staged process where activities, functions, or the extent of the worksite change over a long period of time and in many separate steps. In either case, the safety of the new operation should be assured. Where there are many small incremental step changes, care should be taken to ensure the vehicle continues to operate within its ODD and the safety protections remain sufficient.

3.4.4 Communication throughout implementation

As part of the implementation process, it will be essential to develop a communication plan ensuring that all essential partners and stakeholders are involved in developing and delivering the implementation. These include:

- System operator
- Implementation project team
- Worksite management team
- System designer, developer, supplier, or manufacturer
- Site workforce (including contractors)
- Health and Safety team
- Potentially additional stakeholders previously consulted (see Section 3.1)

During initial implementation, staff may have limited experience with the new system so additional support may be required from the developer or supplier of the OHAV system.

During the initial deployment of the OHAV system, engaging with the emergency services and other local authorities should be considered. It may be appropriate to discuss emergency response procedures (see Section 3.5.2), explain site access or inform them of the activities which are being conducted. This is to ensure both that the emergency services can respond effectively and safely should the need arise, and that all local authorities are fully informed in case of public enquiries or incidents.

3.5 Incident management

3.5.1 Definition of incident

This code considers an incident to be:

An unexpected occurrence where there is the possibility that it could cause injury to humans, damage to other vehicles or infrastructure, or damage or loss of capability of the OHAV beyond normal wear and tear.

Incidents could include near-misses where these consequences could have occurred but did not due to good fortune. The causes of the incident could include, but is not limited to, an unexpected response by the OHAV, unexpected environmental conditions (e.g. landslide, rock fall) or an unexpected human intervention.

Incidents with more severe consequences are likely to require the most consideration and have the most stringent response requirements. Response time to incidents could be reduced if the system provides operators with warning of imminent failure.

3.5.2 Incident response plans

When OHAVs are introduced to a worksite, or used for a new task, they may create new types of possible incident which may affect existing incident response plans. Plans for conceivable incidents involving OHAVs should consider the whole scenario, not just those risks and responses required which directly relate to the OHAV. Incident response plans should be written as a live document and kept up to date. An organisation should rehearse their incident response and test their plan with any learnings used to update their plans and procedures.

OHAVs may be used in environments that are more hazardous than would be accepted for manned operations. This may cause additional challenges when incidents occur and during post-incident recovery.

Example

An OHAV is operating within an underground mine shaft. The positioning technology used does not require installation of lighting and the drive mechanism does not require that the shaft is ventilated.

Any staff entering the operating area would require temporary lighting, such as torches, to navigate through the shaft to locate the OHAV and, if repair or recovery activities are necessary, may need additional portable lighting.

If adequate ventilation has not been maintained or cannot be ensured temporarily, breathing apparatus may be required. These are likely to have implications for the duration that staff can remain in the area.

The use of lighting equipment and breathing apparatus is likely to require additional training. Contingency plans will be required for any subsequent incidents involving the staff involved and should involve the emergency services.

Where OHAVs are used, there should be plans for how to safely stop all, or part of, automated operations. Personnel should be aware of these plans and their roles and responsibilities within them. Those personnel potentially affected should be made aware of any refuges, or places of relative safety, that might be used during an incident.

External parties should be considered during incident plans and consulted where necessary. These may include contractors, employees of other companies working nearby, landowners and emergency services. For example, the incident response plan should include how to confirm that it is safe to approach a system that has automated functions. If requested, additional technical information should be readily available and provided to emergency or rescue services, such as how to bring an automated system to a safe stop or the location of power, fuel, or hydraulic lines in the OHAV.

3.5.3 Post-incident vehicle behaviour

Whether or not an incident is caused by external factors or the vehicle itself, to ensure safety it is vital to understand how the OHAV will behave after the incident. This should be considered in the design of the OHAV, the worksite, and operational procedures, then should be checked through testing.

When an incident occurs, the vehicle should go to a safe state. The vehicle may perform an emergency stop, although there may be scenarios where this is either not practicable due to the existing momentum of the vehicle (e.g. a vehicle moving at high speed or a swinging bucket on a drag line excavator) or could cause further danger (e.g. if the lead vehicle of a close moving convoy performs an emergency stop). In these cases, the OHAV, and other parts of the system, should go to a safe state via further manoeuvres with the minimum risk. The OHAV, and any system it is part of, should be able to achieve this safe state even if there are electrical, electronic, mechanical or software malfunctions or damage.

During incident response, it may be necessary for personnel to approach and come in physical contact with the OHAV. How personnel can identify the current automation, power system and mobilisation states of the vehicle, then make the it safe, should be considered both during the design of the system and in the incident response plan. It is essential that personnel both outside and inside the vehicle can deactivate the vehicle easily to prevent it from unexpectedly restarting during incident response. This should be included in staff training and be tested as part of the incident response drills.

3.5.4 Vehicle recovery and recommencing operation

As part of the incident response, the OHAV may need to be recovered. Where possible, a process for vehicle recovery should be developed as part of the implementation phase. Recovery plans will vary depending on the scenario, but should consider:

- How the location of the vehicle and the environmental conditions may impact a safe recovery
- What damage has or is suspected to have occurred to the vehicle and/or its surroundings
- How to handle the vehicle safely, particularly if damage is known or suspected to have occurred

Before a vehicle recommences operation, particularly in an automated mode, it should be thoroughly inspected for damage, repaired if necessary and tested to verify it is fully functioning by competent personnel.

3.5.5 Incident reporting and investigation

Depending on the severity of an incident, there may be a duty to report the incident externally. An organisation operating OHAVs should, prior to commencing operations, understand their legal obligations and the external reporting requirements. For example, as well as a requirement to report an incident that results in a death or severe injury, there may be a requirement to report incidents impacting critical infrastructure (e.g. striking overhead powerlines). In the UK, reporting requirements are defined in RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations Great Britain 2013). Certain industries, organisations and/or locations may also have additional reporting requirements.

A procedure for incident reporting should be defined, including:

- Which incidents are reported, how, and to whom
- What information should be recorded, including the details of the event and what electronic data is captured
- The personnel responsible for ensuring reporting is done correctly and the necessary follow-on actions are taken

Responsibility for compliance with this procedure should be assigned to a nominated role within the organisation. Personnel should be aware that they need to identify and report incidents and aware of how they use the procedure to do this. Reporting of any incidents should be broader than just that required by legislation. Incidents should be reported internally and to other relevant stakeholders which may include vehicle manufacturers, automated system developers or landowners.

Data from the vehicle and automated systems should be stored automatically when an incident occurs, including data recorded immediately before, during and after the incident. The data should be of sufficient detail and cover sufficient time duration to allow the identification of the root causes of the incident. The data should include the automation state of the vehicle and be of sufficiently high resolution. Plans should be made to enable the police, or other external organisations, to be able to access data recorded during an incident in a way which preserves data and maintains its security and forensic integrity. Wherever possible the data format should be readily readable and if this is not possible, the operator of the OHAV should aid investigators in understanding the data.

Incident reports should be reviewed to identify any actions that are required to improve current practice, including recognising where an activity is not safe to continue in its current form. Periodically, incident reports should be reviewed collectively to identify any recurring trends which require attention.

3.6 Ongoing performance monitoring

3.6.1 The purpose of monitoring

The performance of the automated functions of the OHAV should be monitored throughout operations to ensure the systems are behaving correctly and as expected to identify undesired events which may indicate a safety concern. Undesired events could include the OHAV exiting the ODD, moving unexpectedly, performing a task poorly or requiring unplanned human intervention. Any undesired events should be assessed and if necessary analysed to understand the cause and what remedial action may be required.

Methods of monitoring could include human observations, onboard data and external data (e.g. video or via other components in an overall system). From these recordings, a good understanding of the real-world performance of the OHAV can be gained. This can be used to update operations, which can improve both safety and performance, and inform future developments.

Where OHAVs or systems involving OHAVs operate alongside humans or require human input, the performance of the staff involved in these tasks should be monitored. This is to ensure that people interact with the OHAVs in the way intended, to check if an environment with OHAVs encourages new risky behaviour, to check compliance with and inform training and to ensure access and security measures are maintained.

The level of detail for monitoring should be appropriate to the maturity of the OHAV and the level of risk. A greater level of detail of monitoring for system performance purposes may be required for a system under active development or operating in a site with many potential human interactions than a mature system that is known to perform well or with robust restricted access.

3.6.2 Human monitoring

With conventional vehicles, the driver is actively in control and engaged in the driving task. This will no longer be the case with OHAVs. There may be some cases where the OHAV will be fully automated requiring no human interactions or supervision (i.e. can do the task completely and safely on its own), whilst there may be other cases where the OHAV needs to be continuously monitored and supervised by a human (e.g. safety driver, remote operator supervisor). The change in role from being in control of, for example, the driving task, to monitoring it has proven to reduce attention and alertness (i.e. increase drowsiness), resulting in a loss of situation awareness and becoming out-of-the-loop (OOTL). A driver OOTL or with a lack of situation awareness is less likely to respond to safety critical events. Therefore, it is important that the attention and alertness of an individual required to continuously monitor an OHAV is monitored and managed. If their attention and alertness is significantly impaired, the OHAV should cease to operate, only resuming once the individual's attention and alertness levels are within safe limits. Alternatively, another individual may be able to take their place so long as their attention and alertness is not impaired.

3.6.3 Monitoring plans

To ensure monitoring is conducted it should be planned. The plan should include:

- What events trigger data being recorded
- What data is collected
- How the data is collected and recorded
- Who is responsible for collecting the data
- How the data is stored, transferred, and kept secure
- Who analyses the data
- How issues are reported and acted upon

All relevant staff should be made aware of the monitoring plan and their role and responsibilities within it.

3.6.4 Empowerment culture

An effective monitoring process can only occur if staff understand it is their responsibility to report issues and feel supported when doing so. Management should enable this culture and ensure addressing issues, particularly those related to safety, are prioritised over immediate productivity goals

3.6.5 Engaging stakeholders

Addressing issues and making improvements identified during monitoring may need to involve stakeholders outside of the operator of the OHAV. These may include vehicle manufacturers, ADS developers, system integrators, workers, landowners, industry bodies and government bodies. It may be that some of these stakeholders are part of one company or they may all be individual entities. Channels for communication should be created between the stakeholders to enable issues to be reported to the people who can address them, and all relevant parties can be involved in creating a solution. Best practice and lessons learnt should be shared widely so that all stakeholders can benefit from them and similar mistakes are not repeated by others. Involvement of system developers and manufacturers may provide additional information on an issue which has occurred on systems operating on other sites. This may highlight where changes to the system or operational procedures are required.

An operator may need to initiate engagement with stakeholders, for example:

- Following vehicle manufacturer, ADS developer or system integrator bulletins
- Providing feedback about an ODD breach, human factors limitation or common false positive to an ADS developer
- Contributing to consultations from industry or government bodies
- Updating worker training after a new risky behaviour has occurred

3.7 Change management

Due to the maturity and nature of automated systems, it is very likely that changes will be made to an OHAV system or its operations over its lifetime. Due to the transition from relying on a human operator for the correct and safe operation of the vehicle to an electronic system, it is vital to assess the safety impact of any change. This is to minimise any potential risks of harm that may arise as a result. The most efficient and safest method to manage change is to develop a change control process. Organisations operating automated vehicles should develop a change control process and this should be included in the safety case. Even if an organisation has an established change control process, it will need to be reviewed for appropriateness to automated vehicle systems.

An organisation's change control processes may also incorporate business risks such as harm to reputation, quality, or profit.

Types of changes that may affect the safety of an off-highway automated vehicle system include:

- Changes to the OHAV system's software, hardware, set-up, or calibration, where these changes alter the base vehicle, additional equipment, or supporting systems
- Changes to operations such as what the OHAV is doing, where, and in what conditions
- Changes to staff roles, responsibilities, or necessary levels of experience or ability
- Changes to documented processes

Changes can be proactive requests, such as improvements, or result from an event such as a failure. Routine maintenance activity would not need to follow a change control process if there was a defined process of how to conduct that activity (see Section 3.3.7).

It may be appropriate to grade changes according to the severity of the safety impact which would influence the response. Existing change management processes should be reviewed as the impact of the change may have become more severe with an automated vehicle compared to one with a human in the loop.

Example

Types of changes which may have a more significant safety impact with an automated vehicle compared to a manned vehicle:

- A failure of a sensor that was previously used to advise the operator of an issue, but which is now used as a control input for the automated system
- A change in specification of a barrier which is now being used by the automated system to denote the operational design domain

4. Support Materials

This section has additional materials to support planning and decision-making, including:

1. Glossary of terms and abbreviations used in this code of practice
2. Details of, and links to, other resources
3. Case studies of successful off-highway automated vehicle implementations

4.1 Glossary of terms and abbreviations

The definitions here are from (or adapted from) BSI Connected and Automated vehicles – Vocabulary (BSI, 2020a) unless otherwise stated.

As Low As Reasonably Practicable (ALARP)	A statement which outlines that all reasonably practicable mitigations and measures to manage the risks of an activity have been implemented. Reasonably practicable measures are those that can control the risk and that are not grossly disproportionate to the sacrifice, time and money needed to implement them. BSI PAS 1881 (BSI, 2020b)
Automated Driving System (ADS)	Hardware and software that are collectively capable of performing the dynamic driving task on a sustained basis, regardless of whether it is limited to a specific operational design domain.
Automated System	Hardware and software that are collectively capable of performing an activity on a sustained basis, regardless of whether it is limited to a specific operational design domain.
Cyber Security Management System (CSMS)	Organisational processes, responsibilities, and governance to treat risk from cyber threats to vehicles and protect them from cyber-attacks. Defined for this document
Global Navigation Satellite System (GNSS)	A GNSS is a constellation of satellites providing signals from space that transmit positioning and timing data which is used by receivers to determine their geographic location. Defined for this document
Off-Highway Automated Vehicle (OHAV)	A vehicle which features an automated system that can fully or partially control (when required, with minimal human intervention) at least one of the operational functions of the vehicle. The automated function has the potential to cause direct harm to people. See Section 1.2 for further details. Defined for this document
Operational Design Domain (OD)	The operating conditions under which a given driving automation system or vehicle feature is specifically designed to function. Defined for this document
Over-The-Air (OTA)	OTA is wireless transmission of information often used to deliver software, firmware or configuration updates. Defined for this document
Remote operator	An operator who oversees the operation of an automated vehicle from a remote location.
Safety case	A structured argument, supported by evidence, intended to justify that a system and activity is acceptably safe for a specific application in a specific operating environment. A safety case is a useful tool to provide safety assurance to stakeholders involved in the activity.
Safety operator	A person who is trained and able to supervise the function of an automated vehicle and intervene at any time it is required.

4.2 References and other resources

BSI (2018). PAS 1885:2018. *The fundamental principles of automotive cyber security – Specification.* London, GB: British Standards Institution (BSI)

BSI (2019). BS ISO 17757:2019. *Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety.* London, GB: British Standards Institution (BSI)

BSI (2020a). BSI Flex 1890 v3.0:2020-10. *BSI connected and automated vehicles – Vocabulary.* London, GB: British Standards Institution (BSI)

BSI (2020b). PAS 1881:2020. *Assuring the safety of automated vehicle trials and testing – Specification.* London, GB: British Standards Institution (BSI)

BSI (2020c). PAS 1883:2020. *Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification.* London, GB: British Standards Institution (BSI)

CCAV (2019). *Code of practice: Automated vehicle trialling.* London, GB: Centre for Connected and Autonomous Vehicles (CCAV)

Department of Mines and Petroleum (2015). *Safe mobile autonomous mining in Western Australia – Code of practice.* Western Australia, AU: Resources Safety, Department of Mines and Petroleum

EU (2016). Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

GMG (2019). *Guideline for the implementation of autonomous systems in mining (version 1, revision 1).* Global Mining Guidelines Group

Great Britain (2013). No. 1471. *Reporting of injuries, diseases and dangerous occurrences regulations 2013.* London, GB: The Stationery Office

Great Britain (2018). *Data protection act 2018.* London, GB: The Stationery Office

HM Government (2017). *The key principles of cyber security for connected and automated vehicles.* London, GB: HM Government

ISO (2019). ISO/PAS 21448:2019. *Road vehicles – Safety of the intended functionality.* Geneva, CH: International Organization for Standardizion (ISO)

SAE International (2018). J3016_201806. *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles.* SAE International

TRL with FiveAI (2019). *StreetWise Abridged Safety Case.* Crowthorne, GB: TRL Ltd.

UN (2021a). UN Regulation No.155. *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.* Geneva, CH: United Nations Economic Commision for Europe

UN (2021b). UN Regulation No.156. *Uniform provision concerning the approval of vehicles with regards to software update and software updates management system.* Geneva, CH: United Nations Economic Commision for Europe

4.3 Case studies

The case studies provided here are examples of:

1. An initial, single-vehicle, trial
2. An extensive, multi-vehicle, set of trials

This information has been provided by those directly involved in undertaking the development and implementation of the OHAVs.

Blackwell Autonomous Articulated Dump Truck (AADT) Trial for Earthmoving on A14 Cambridge to Huntingdon Improvement Scheme

This trial of an Autonomous Articulated Dump Truck (AADT) on the A14 highways project in 2018 was undertaken by Blackwell on behalf of the A14 Integrated Delivery Team and benefited from Innovation Designation Funds from the Scheme Employer, Highways England.

The main challenges were to:

1. Assess whether the command-and-control mechanisms for autonomous Articulated Dump Truck (ADT) operations, as developed in the mining sector, could be applied in a civil engineering earthmoving context.
2. Assess whether the mining codes of practice and standards (particularly ISO 17757 and associated documents, and the West Australian Department of Mines & Energy Code of Practice) were applicable to a civil engineering earthmoving context.

Photos courtesy of Blackwell Earthmoving

We equipped an existing 40t payload ADT with technology and associated command and control to make it fully autonomous. This was an existing R&D kit that had been developed 7 years previously for a demonstration project in a mine in South Africa and so represented old equipment.

The truck was assessed on a proving ground that had been constructed for the training of human operators and performed all the expected functions of a dump truck autonomously including, pathing, steering, interaction with other equipment such as excavators loading, tipping and so on.

The command-and-control system was assessed at the same time by conducting simulated cut to fill activities including drawing maps showing revised haul paths etc for the truck to autonomously use.

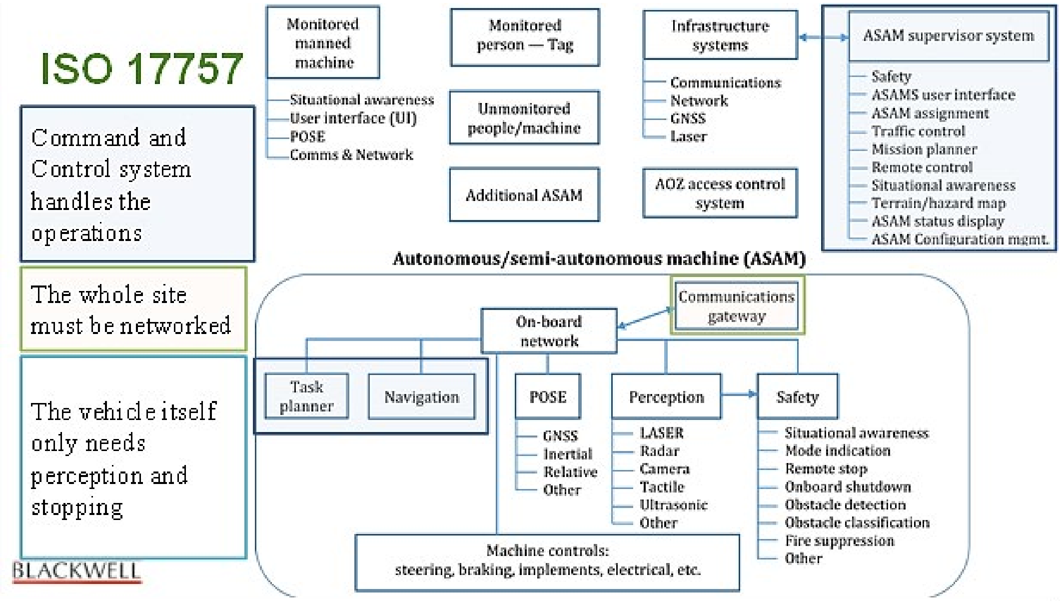
What equipment was implemented?

A fully autonomous ADT from ASI Robotics (USA based company). The system comprised their Mobius command-and-control system as well as the equipment necessary to make the truck fully autonomous. The system, as a whole, included:

- The truck plus the sensors, actuators, processors, etc., to make it capable of full autonomy
- The local Wi-Fi network, including all antennae's etc., to provide an extremely stable local area network for the system to run on
- Server to run the central autonomous system
- Field tablets to interact with the system including interactions with other items of equipment such as the excavator

Safety case

This was one of the major objectives of the trial – to assess whether a system and equipment that had been developed under the mining standards would perform adequately within a civil engineering context. As a result, this followed the general recommendations laid out by the West Australian Department of Mines and Energy. This process worked well with the general requirements for risk assessment in civil engineering. The main safety case for our trial was built around the 'if in doubt, stop' principle as codified within ISO 17757. Technically, the equipment pre-dated the issuance of this ISO, but it was developed within the environment that gave birth to the ISO and hence was generally compliant.



As a result, 'technical' safety issues were largely dealt with by the equipment design including:

1. Geofencing to avoid 'run-away' equipment and allow restrictions on behaviour by location
2. 'Heartbeat' signal triggering auto-stop in case of network failure
3. 'On-board' ODAS (Object Detection and Avoidance System) including LiDAR-based 'vision' with object detection by reference to an estimated ground plane (detection signal strength by use of a Kalman filter)

We found that we needed to pay particular attention to the design of the area because the truck would behave more conservatively than a human driver in tight confines and so providing sufficient working width was important.

Implementation

The key challenges were to get the truck to work rather than to stop. As the default behaviour in the safety case was to stop and safe, the default system state was 'stopped'.

Because the equipment was old, we had challenges that flowed from this, particularly with the resolution of the LiDAR scanner and hence the adequacy of the ground plane estimate for the ODAS system. The truck algorithm was inherently conservative and had too many 'false positive' object detections (and subsequent avoidances or stoppages) for a productive system. We don't consider this to be an issue as the current state of the art in LiDAR is at least a 4-fold improvement in resolution and frequency compared with the one we used. With these higher precision current sensors, the ODAS problem has been largely solved in the field at least as far as false detections due to the sun being low in the sky, etc.

Secondly, we faced challenges of habit. Traditionally, temporary works such as haul roads would be constructed to fairly loose tolerances to suit human operators' requirements. We found that the autonomous system wasn't suited to this type of ambiguity. If it expected a certain width, then you had to provide the full width. Any feature within the site that was unexpected would often cause it to default to a 'safe/stop' state. The key 'takeaway' was that for the practical deployment of an autonomous system the temporary site access works would need to be constructed more precisely.

Results

We feel we achieved the aims of the trial and established the following learnings:

1. The mining-based command and control system Mobius as supplied by ASI robotics is sufficiently adaptable to be of use in a civil engineering context
2. We identified key system feature requirements for the assessment of any alternative systems.
3. The document 'Safe mobile autonomous mining in Western Australia - Code of Practice', on the whole, provides a pragmatic and useful guide, with ISO17757 providing the technical safety assurance for equipment.

BLACKWELL
Earthmoving

We were able to progress to the point of making a draft business model assessment of autonomous ADTs in general such that we now understand where they would make sense.

Next steps

Find a suitable worksite to establish a full team scale field trial including production trials on a live project

Hands Free Hectare : Conducted at Harper Adams University, in collaboration with Precision Decision Ltd

The project aim was to complete the world's first autonomous cereal cropping cycle utilising open source UAV systems and commercially available agricultural equipment. The project started by adapting the commercial machinery (tractor and combine harvester) with the addition of UAV control system, RTK high precision GNSS positioning and safety systems. The autonomous cropping cycle was then completed from seed establishment through to harvest within the Hectare test field. Drones and ground rover systems were utilised to monitor the crop's development.

Photos courtesy of Harper Adams University

What equipment was implemented?

- Open source drone control hardware and software (mission planner)
- Iseki TLE tractor
- Sampo Combine harvester
- UAV crop imaging drones

Safety case

Safety was considered with multiple levels of redundancy:

- Controlled operation environment inside a fenced field
- Remote system monitoring by dedicated "control operator"
- Single plane LIDAR with predetermined safety boundary (2m)
- Vehicle mounted e-stops and remote fail-safe e-stop held by dedicated "safety operator"
- "Pre-flight" safety checks of all systems conducted prior to any autonomous operation by trained staff

Implementation

The initial control accuracy, reliability and repeatability of the open source system were not to the standard required for agriculture and the first field operations did not provide the best coverage, for example overlaps, or missed areas, during drilling.

Appropriate safety systems are required. On-road autonomous cars should only drive ahead if the way is clear, but in agriculture the vehicle may often be required to drive into vegetated conditions, so any forward sensing systems require a higher level of intelligence.

Results

From 2016-2018, the project was successful in conducting two complete cropping cycles within the Hands Free Hectare. The project was also successful in changing the perception of automation in the agricultural sector with the high levels of media attention that was generated with it being reported in over 85 countries worldwide. Economic analysis of the work showed a significant potential financial benefit if the system was adopted against conventual mechanised agriculture, with a reduction of cost of production in the order of £20-30/tonne of wheat.

Next steps

The project has grown to a Hands Free Farm with autonomous farming across five fields, totalling 35 ha. This project is working with further commercial partner Farmscan Ag to develop the control system to the point of pre-commercial production.

The off-highway sector encompasses a broad range of industries including mining, quarrying, agriculture, construction, and ports and airports. Automated vehicle technology has become commonplace within some of these industries, bringing with it many benefits for safety, efficiency and productivit. But it is important to keep in mind that the transition to new working practices should be carefully managed to ensure that unintended safety consequences do not cancel out the potential benefits.

This draft code of practice seeks to provide top level guidance to organisations, in all sectors of the off-highway industry, on the ways in which working practices should be adapted to ensure that the adoption of automation is as smooth and safe as possible. The code is applicable to the broad range of environments in which off-highway vehicles are used and the different demands and risks of using automation in those settings. The aim is that this code will support safe practice, build public confidence and support the cooperation between organisations across all industries employing off-highway automated vehicles.

TRL would like to thank all of the organisations and individuals who gave time to support development of this draft, their help has been invaluable.

ISSN 978-1-913246-64-8

ISBN 2514-9652

PPR 994

t +44[0]1344 773131
e enquiries@trl.co.uk
w www.trl.co.uk

TRL Crowthorne House, Nine Mile Ride,
Wokingham, Berks, UK, RG40 3GA

THE FUTURE
OF TRANSPORT