# Overview of Operational Safety Concepts for Level 4 Automated Driving System Fleets

## Risk Mitigation Activities

## Methodology

### Development of Risk Mitigation Activities

The development of the risk mitigation activities follows the methodology depicted in Figure 1. The activities describe what the fleet operator should provide to the agents involved in the operation so that they can perform their safety responsibilities. The activities comprise four main types of support for the agents: training, work conditions, operational procedures, and hardware and software tools (Table 1). The activities are categorized according to their safety impact, resources, frequency, and business impact as described in the appendix.

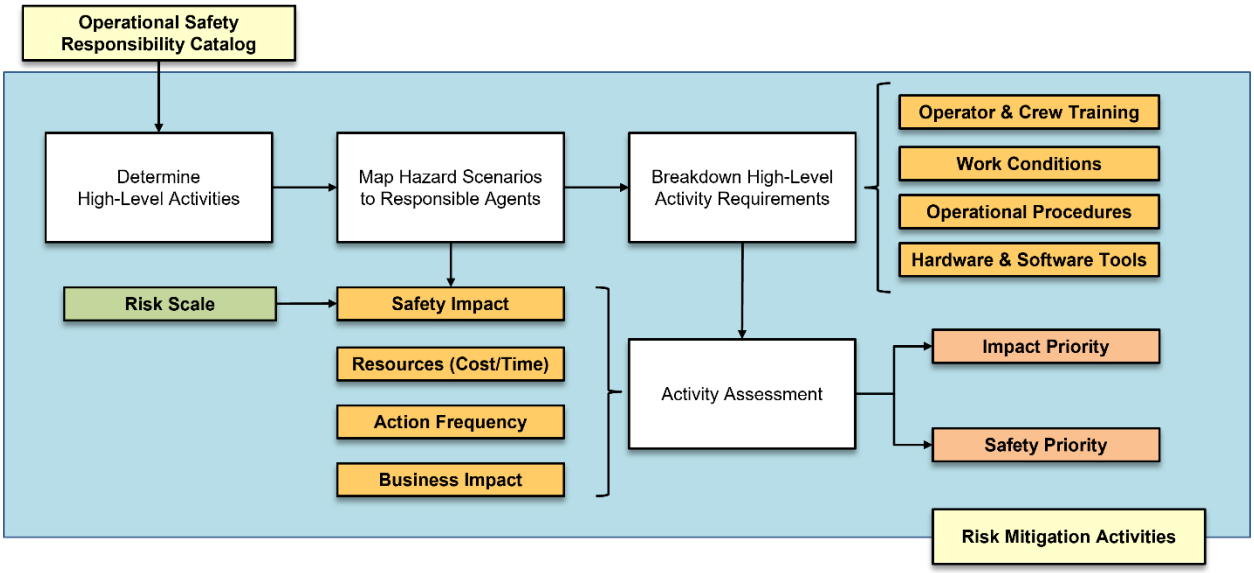


*Figure 1: Task 6 Derivation and Assessment of Risk Mitigation Activities.*

*Table 1: Risk mitigation activity types considered.*

| Activity type | Description |
|---|---|
| Operational Procedures | Operational guidelines to support the activities of the human operators and the operating conditions of the ADS vehicle. These refer to both emergency operating procedures and standard operating procedures. These procedures include the content, frequency, and requirements for communications, activities, and interactions between the agents and external entities. |
| Operator & Crew Training | Training provided to the FOC operators and MOC crew. The training content includes familiarization with the operational procedures, required |

| Activity type | Description |
|---|---|
| | Human-System Interface (HSI) functions, emergency procedures, and workplace safety guidelines. |
| Hardware & Software Tools | Hardware and software tools necessary for the agents to perform expected tasks. These include required communication devices, reliable connectivity conditions, passenger interaction devices, and tools to support maintenance activities. |
| Work Conditions | General policies and equipment designed to improve multiple aspects of workplace adequacy for expected crew performance. |

The activities derived from each safety responsibility respond to the related hazard. For instance, Table 2 presents an example high-level safety responsibility read as:

"*The main role of the fleet operator is to implement operational procedures addressing monitoring and intervention tasks. These procedures may be developed internally and with input from the ADS developer and will target the FOC safety operator's tasks which aim to mitigate hazards derived from failures of the ADS software*."

To identify the risk mitigation activities associated with implementing the FOC safety operator's operational procedures, Table 3 lists all the hazard scenarios for which this safety responsibility is relevant. Finally, Table 4 lists the activities required to support the FOC safety operator detect and mitigate hazards caused by the ADS software's failures. Note that the information on which hazard scenarios are affected by the activities is preserved, as is the highest risk level associated with each scenario.

*Table 2: Risk mitigation activity derivation example – safety responsibility.*

| Fleet Operator Role | High-Level Activity | Support | Target Agent | Agent Action Type | Risk Contributor |
|---|---|---|---|---|---|
| Implement | Operation procedures (monitoring, intervention) | Mixed | FOC safety operator | Mitigation | ADS software |

*Table 3: Risk mitigation activity derivation example – hazard scenarios that target agent (FOC safety operator) and risk contributor (ADS software) interact.*

| ID # | Hazard Scenario | | | Highest Risk Level |
|---|---|---|---|---|
| 1.1.3 | ADS | fails to | perform DDT-fallback correctly | 5 |
| 1.1.6 | ADS | fails to | request post-incident management procedures | 3 |
| 1.2.1 | FOC | fails to | detect DDT fallback is required | 5 |
| 1.2.2 | FOC | fails to | send correct DDT fallback command | 5 |
| 2.1.1 | ADS | fails to | detect DDT-fallback is required | 5 |
| 2.1.2 | ADS | fails to | perform DDT-fallback correctly | 5 |
| 2.1.3 | ADS | fails to | request post-incident management procedures | 5 |
| 2.2.1 | FOC | fails to | detect DDT fallback is required | 5 |
| 2.2.2 | FOC | fails to | send correct DDT fallback command | 5 |
| 2.2.3 | FOC | fails to | initiate post-incident procedures | 4 |
| 2.2.4 | FOC | fails to | communicate with passenger | 5 |

| ID # | Hazard Scenario | | | Highest Risk Level |
|---|---|---|---|---|
| 3.2.1 | FOC | fails to | not scheduled vehicle for inspection or corrective maintenance | 2 |
| 3.2.2 | FOC | fails to | not scheduled vehicle for preventive maintenance | 2 |
| 3.2.4 | FOC | fails to | follow procedure on vehicle status | 2 |
| 3.3.3 | MOC | fails to | perform inspection correctly | 2 |
| 3.3.11 | MOC | fails to | perform service inspection correctly | 2 |
| 4.1.1 | ADS | fails to | achieve SSC for pick-up/drop-off | 5 |
| 5.2.1 | FOC | fails to | confirm other road users are involved | 4 |
| 5.2.2 | FOC | fails to | contact first responders | 4 |
| 5.2.4 | FOC | fails to | communicate with passenger | 4 |
| 5.2.5 | FOC | fails to | dispatch secondary vehicle for passengers | 4 |
| 5.2.6 | FOC | fails to | send correct DDT fallback command | 4 |

*Table 4: Risk mitigation activity derivation example – risk mitigation activities derived to support the target agent (FOC safety operator).*

| **Risk Mitigation Activity Type** | **Activity Purpose** | **Scenarios** |
|---|---|---|
| Operator & Crew Training | Recognize ODD conditions and ADS failures | 1.1.3, 1.1.6, 1.2.1, 1.2.2, 2.1.2, 2.1.3, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 5.2.1, 5.2.2, 5.2.6 |
| | Select adequate DDT-fallback strategies | |
| | Use HSI to monitor and intervene in the vehicle's operation | |
| | Recognize HSI and connectivity failures | |
| Operational Procedures | Establish FOC operator intervention criteria | 1.2.2, 2.1.3, 2.2.2, 2.2.3, 3.2.1, 3.2.4, 5.2.5, 5.2.6 |
| | Establish responsibilities during post-incident procedures | 5.2.1, 5.2.2, 5.2.4, 5.2.5, 5.2.6 |
| | Establish information sharing procedures between fleet operator's agents | 2.2.1, 2.2.2, 2.2.3, 2.2.4, 3.2.1, 3.2.2, 3.2.4, 3.3.3, 3.3.11, 5.2.1, 5.2.4, 5.2.5, 5.2.6 |
| Hardware & Software Tools | Provide adequate HSI design to support agents' tasks | 1.1.3, 1.1.6, 1.2.1, 1.2.2, 2.1.2, 2.1.3, 2.2.1, 2.2.2, 2.2.3, 3.2.1, 3.2.2, 5.2.1, 5.2.2, 5.2.4, 5.2.5, 5.2.6 |
| Working Conditions | Follow adequate length of shifts | 1.1.6, 1.2.1, 1.2.2, 2.2.1, 2.2.2, 2.2.3, 3.2.1, 3.2.2, 3.2.4, 3.3.3, 3.3.11, 5.2.1, 5.2.2, 5.2.4, 5.2.5, 5.2.6, |
| | Have access to emergency procedure handbooks and other supporting documentation during operation. | 1.1.6, 2.1.3, 2.2.3, 5.2.1, 5.2.2, 5.2.4, 5.2.5, 5.2.6, 5.3.1 |

Note that the activity purpose provides information about the content of the risk mitigation activity. Table 4 can thus be read as "The fleet operator should provide:

- Training program for the FOC safety operators that includes how to:

    - Recognize ODD conditions and ADS failures,
    - Correctly select adequate DDT- fallback strategies,
    - Use HSI to monitor and intervene in the vehicle's operation when needed,
    - Recognize HSI and connectivity failures
- Operational procedures that:
    - Establish FOC operator intervention criteria,
    - Establish responsibilities during post-incident procedures,
    - Establish information-sharing procedures between fleet operator's agents
- Hardware and software tools for the FOC safety operators that:
    - Provide adequate HSI design to support operators' tasks
- Working conditions that:
    - Follow adequate length of shifts,
    - Follow emergency procedure handbooks / guidelines.

Note that the activities provide a "checklist" of minimum requirements for each activity type. They are not an exhaustive list, e.g., the training should cover aspects additional than the ones listed. Certain details are to be determined by the fleet operator, for instance, the frequency of training programs or the HSI design following human factors principles.

## Risk Mitigation Activities

The analysis resulted in 140 risk mitigation activities, each assessed through the potential safety impact and required implementation resources (cost, time, frequency). This list contains activities that impact the tasks and performance of multiple target agents, and thus can be aggregated into 81 unique activities spanning operator and crew training, operational procedure development, software and hardware tools, and workplace adequacy factors.

This methodology guarantees that all risk mitigation activities cover the identified safety responsibilities. Additionally, all safety hazard scenarios are cross-referenced through the safety responsibilities with the risk mitigation activities.

Table 5 provides the top safety priority activities. These activities target all system agents and include key activities such as those related to management of change, training remote supervisors to monitor and intervene vehicles' operation, providing adequate working conditions for operators, enforcing vehicle connectivity and dispatching requirements, and coordinating internal incident mitigation activities. Providing adequate working conditions refers to elements designed to support the operators and crew in performing their tasks based on principles of human factor studies. These may include factors related to environmental conditions (e.g., lighting, noise, ventilation, and ergonomic workstation design) and floor layouts (e.g., location and orientation of equipment) as well as compliance with workplace-specific safety regulations. Adequate HSI design is also a major factor of workplace adequacy. Adequate HSI implementation considers the particular tasks each operator or crew member is expected to perform (e.g., task complexity, time restrictions, interactions with other agents, etc.)

Note that this list contains some activities that had been ranked as a "Low" business priority. Indeed, these activities related to the FOC Safety and Service Operators mitigate high-risk hazard

scenarios and require a high level of resources to be implemented ("Provide adequate HSI design to support agent tasks", "Provide and maintain functioning HSI").

*Table 5: Top Safety Priority Risk Mitigation Activities.*

| Target Agent | Activity Type | Activity Purpose | Safety Impact | Business Impact |
|---|---|---|---|---|
| MOC Coordinators | Procedures | Record operational procedure updates | Moderate | Very High |
| FOC Safety Operator | Work conditions | Follow adequate length of shifts | Very High | Very High |
| FOC Safety Operator | Work conditions | Provide adequate working conditions | Very High | Very High |
| FOC Service Operator | Tools | Provide in-vehicle passenger communication devices | Very High | Very High |
| MOC External Operations | Procedures | Record operational procedure updates | High | Very High |
| ADS Vehicle | Tools | Provide communication devices between agents (FOC, MOC) | Very High | Very High |
| FOC Service Operator | Work conditions | Follow adequate length of shifts | High | Very High |
| FOC Safety Operator | Procedures | Establish information-sharing procedures between fleet operator's agents | High | Very High |
| FOC Service Operator | Procedures | Establish information-sharing procedures between fleet operator's agents | High | Very High |
| FOC Service Operator | Procedures | Establish passenger data privacy policies | High | Very High |
| FOC Safety Operator | Training | Enforce management of change policies | High | Very High |
| FOC Service Operator | Training | Enforce management of change policies | High | Very High |
| MOC Coordinators | Procedures | Provide shift take-over procedures | High | Very High |
| MOC Coordinators | Training | Enforce management of change policies | Very High | High |
| MOC Coordinators | Work conditions | Provide adequate working conditions | High | High |
| ADS Vehicle | Procedures | Enforce data transmission and storage policies | High | High |
| ADS Vehicle | Tools | Provide navigation and HD map support | High | High |
| FOC Service Operator | Procedures | Managing requests from other agents (FOC, MOC) | High | High |

| Target Agent | Activity Type | Activity Purpose | Safety Impact | Business Impact |
|---|---|---|---|---|
| ADS Vehicle | Procedures | Enforce vehicle connectivity requirements | Very High | High |
| MOC Maintenance Crew | Training | Enforce vehicle communication devices safety checklist | High | High |
| MOC Inspection Crew | Training | Enforce vehicle communication devices safety checklist | High | Medium |
| ADS Vehicle | Procedures | Follow specified DDT-fallback goals and strategies | High | Medium |
| ADS Vehicle | Procedures | Enforce ODD and local road restrictions | High | Medium |
| ADS Vehicle | Procedures | Ensure self-diagnostic capabilities are available (vehicle hardware, software) | High | Medium |
| ADS Vehicle | Procedures | Ensure DDT-fallback commands are received and implemented as specified | High | Medium |
| ADS Vehicle | Procedures | Interact with first responders/law enforcement | High | Medium |
| FOC Safety Operator | Training | Use HSI to monitor and intervene in the vehicle's operation | High | Medium |
| FOC Safety Operator | Tools | Provide adequate HSI design to support agent tasks | High | Low |
| FOC Service Operator | Tools | Provide adequate HSI design to support agent tasks | High | Low |
| FOC Safety Operator | Work conditions | Provide and maintain functioning HSI | High | Low |
| FOC Service Operator | Work conditions | Provide and maintain functioning HSI | High | Low |

### List of risk mitigation activities by activity type

The following Table 6-Table 9 provide the complete list of risk mitigation activities organized by the type of activity.

The safety priority rank, business priority rank and the relative risk level of the impacted hazard scenarios are provided for each activity and averaged by type. A lower value reflects a higher priority for both safety and business priority. In contrast, for the relative risk level, a higher value represents an activity that impacts scenarios with a higher risk. Risk mitigation activities with a top safety priority (Safety Priority Rank 1) are highlighted in blue.

*Table 6: List of risk mitigation activities by type: operational procedures.*

| Activity Type | Procedures | |
|---|---|---|
| | **Safety Priority Rank** | **Business Priority Rank** |
| **ADS Vehicle** | **Medium** | **Medium** |
| Enforce vehicle connectivity requirements | Top | High |
| Interact with first responders/law enforcement | Top | Medium |
| Enforce data transmission and storage policies | Top | High |
| Enforce ODD and local road restrictions | Top | Medium |
| Ensure self-diagnostic capabilities are available (vehicle hardware, software) | Top | Medium |
| Follow specified DDT-fallback goals and strategies | Top | Medium |
| Ensure DDT-fallback commands are received and implemented as specified | Top | Medium |
| Select routes within established ODD | Medium | Medium |
| Ensure dispatch commands are received and implemented as specified | Medium | Medium |
| Interact with passengers (pickup, start/end trip, drop-off) | Low | Low |
| **FOC Safety Operator** | **Medium** | **Medium** |
| Establish information sharing procedures between fleet operator's agents | Top | Very High |
| Record operation logs to support accident investigation | Very High | Very High |
| Record operation logs to support maintenance procedures | Very High | Very High |
| Record operational procedure updates | High | High |
| Provide shift take-over procedures | High | High |
| Enforce vehicle dispatching requirements | High | High |
| Enforce vehicle physical recovery requirements | High | High |
| Manage requests from other agents (FOC, MOC) | Medium | Medium |
| Locate and manage vehicles exhibiting abnormal behavior | Medium | Medium |
| Establish FOC operator intervention criteria | Medium | Medium |
| Determine DDT-fallback goals and strategies | Low | Low |
| Establish responsibilities during post-incident procedures | Low | Low |
| **FOC Service Operator** | **Medium** | **Medium** |
| Manage requests from other agents (FOC, MOC) | Top | High |
| Establish information sharing procedures between fleet operator's agents | Top | Very High |
| Establish passenger data privacy policies | Top | Very High |
| Record operation logs to support accident investigation | Very High | Very High |
| Request secondary vehicle dispatch for passengers | Very High | Very High |
| Provide shift take-over procedures | High | High |
| Request intervention from FOC Safety Operator | Medium | Medium |
| Establish responsibilities during post-incident procedures | Low | Low |
| **MOC Coordinators** | **Medium** | **Medium** |
| Record operational procedure updates | Top | Very High |
| Provide shift take-over procedures | Top | Very High |
| Record maintenance activity reports to support incident investigation | Very High | Very High |
| Develop maintenance activities safety checklist | Very High | Very High |
| Record fleet activities with ADS Developer to support incident management | Very High | Very High |
| Establish information sharing procedures between fleet operator's agents | High | High |
| Coordinate internal maintenance activities | High | High |
| Enforce vehicle recovery procedures | High | High |

| Activity Type | Procedures | |
|---|---|---|
| Implement specified maintenance activities content and frequency | Medium | Medium |
| Interact with first responders/law enforcement for incident management | Low | Low |
| Establish responsibilities during post-incident procedures | Low | Low |
| **MOC External Operations** | **Medium** | **Medium** |
| Record operational procedure updates | Top | Very High |
| Communicate operational procedure updates to FOC/MOC | Very High | Very High |
| Record fleet activities with ADS Developer to support incident management | Very High | Very High |
| Manage communications with ADS Developer | High | High |
| Establish passenger data privacy policies | High | High |
| Coordinate external maintenance activities with ADS Developer | High | High |
| Assist in performing accident investigation activities | Medium | Medium |
| Coordinate training activities with ADS Developer | Medium | Medium |
| Manage communications with first responders/law enforcement | Low | Low |
| **MOC Inspection Crew** | **Medium** | **Medium** |
| Record inspection reports to support maintenance activities | Very High | Very High |
| Enforce vehicle clearance requirements | Very High | Very High |
| Implement specified pre-shift inspection contents and performance metrics. | High | High |
| Provide shift take-over procedures | High | High |
| Implement specified service inspection contents and performance metrics | Medium | Medium |
| Establish emergency and safe operation procedures | Low | Low |
| **MOC Maintenance Crew** | **Medium** | **Medium** |
| Request external maintenance support | Very High | Very High |
| Record maintenance reports to support maintenance activities | Very High | Very High |
| Implement specified system update contents and performance metrics | High | High |
| Provide shift take-over procedures | High | High |
| Implement specified corrective maintenance contents and performance metrics | Medium | Medium |
| Implement specified service maintenance contents and performance metrics | Medium | Medium |
| Establish emergency and safe operation procedures | Low | Low |

**This table reads as: the fleet operator should provide operational procedures for the (*target agent*) that include how to (*activity)***

*Table 7: List of risk mitigation activities by type: software and hardware tools.*

| **Activity type** | Software and hardware tools | |
|---|---|---|
| | **Safety Priority Rank** | **Business Priority Rank** |
| **ADS Vehicle** | **High** | **Medium** |
| Provide navigation and HD map support | Top | High |
| Provide communication devices between agents (FOC, MOC) | Top | Very High |
| Provide passenger interaction cues (audio, video) | Medium | Medium |
| **FOC Safety Operator** | **Medium** | **Medium** |
| Provide adequate HSI design to support agent tasks | Top | Low |
| Provide communication devices between agents (FOC, MOC) | Medium | Medium |
| Provide vehicle operation intervention mechanisms | Medium | Medium |
| **FOC Service Operator** | **Top** | **Medium** |
| Provide adequate HSI design to support agent tasks | Top | Low |
| Provide in-vehicle passenger communication devices | Top | Very High |
| **MOC Coordinators** | **Low** | **Low** |
| Provide communication devices between agents (FOC, MOC) | Medium | Medium |
| Provide vehicle inventory and status | Medium | Medium |
| Provide adequate HSI design to support agent tasks | Low | Low |
| **MOC Inspection Crew** | **Low** | **Low** |
| Provide low-complexity inspection tools (software, hardware, vehicle) | Medium | Medium |
| Provide vehicle performance tests (at hardware, software, vehicle level) | Low | Low |
| Provide adequate HSI design to support agent tasks | Low | Low |
| **MOC Maintenance Crew** | **Low** | **Low** |
| Provide low-complexity repair tools and replacement parts onsite | Medium | Medium |
| Provide vehicle performance tests (at hardware, software, vehicle level) | Low | Low |
| Provide adequate HSI design to support agent tasks | Low | Low |
| **This table reads as: the fleet operator should (*activity)* for the (*target agent*) to have adequate software and hardware tools to perform their tasks** | | |

*Table 8: List of risk mitigation activities by type: operator and crew training.*

| Activity type | Operator and crew training | |
|---|---|---|
| | **Safety Priority Rank** | **Business Priority Rank** |
| **FOC Safety Operator** | **Medium** | **Medium** |
| Enforce management of change policies | Top | Very High |
| Use HSI to monitor and intervene the vehicle's operation | Top | Medium |
| Enforce vehicle clearance requirements | Medium | Medium |
| Recognize HSI and connectivity failures | Medium | Medium |
| Coordinate team responses with other agents (FOC, MOC) | Medium | Medium |
| Recognize DDT-fallback goals and evaluate outcomes | Medium | Medium |
| Recognize HSI information and alarms | Medium | Medium |
| Recognize ODD conditions and system failures | Low | Low |
| Transmit adequate DDT-fallback strategies | Low | Low |
| Select adequate DDT-fallback strategies | Low | Low |
| Follow incident management procedures and emergency response | Low | Low |
| **FOC Service Operator** | **Low** | **Low** |
| Enforce management of change policies | Top | Very High |
| Coordinate team responses with other agents (FOC, MOC) | Medium | Medium |
| Recognize HSI and connectivity failures | Medium | Medium |
| Manage passenger communication (requests, interactions) | Medium | Medium |
| Interact with first responders/law enforcement during incident management | Low | Low |
| Follow incident management procedures and emergency response | Low | Low |
| **MOC Coordinators** | **Low** | **Low** |
| Enforce management of change policies | Top | High |
| Coordinate team responses with other agents (FOC, MOC) | Low | Low |
| Recognize HSI and connectivity failures | Low | Low |
| Interact with first responders/law enforcement during vehicle recovery | Low | Low |
| Follow incident management procedures and emergency response | Low | Low |
| **MOC Inspection Crew** | **Medium** | **Medium** |
| Enforce vehicle communication devices safety checklist | Top | Medium |
| Enforce management of change policies | High | High |
| Enforce vehicle software safety checklist | Medium | Medium |
| Enforce vehicle sensor safety checklist | Medium | Medium |
| Enforce workplace safety culture and emergency procedures | Medium | Medium |
| Enforce vehicle hardware safety checklist | Medium | Medium |
| Enforce vehicle passenger interaction devices safety checklist | Medium | Medium |
| Recognize system errors in diagnostic logs | Medium | Medium |
| Coordinate team responses with other agents (FOC, MOC) | Low | Low |
| **MOC Maintenance Crew** | **Medium** | **Medium** |
| Enforce vehicle communication devices safety checklist | Top | High |

| | | |
|---|---|---|
| Enforce management of change policies | High | High |
| Enforce vehicle software safety checklist | Medium | Medium |
| Enforce vehicle sensor safety checklist | Medium | Medium |
| Enforce workplace safety culture and emergency procedures | Medium | Medium |
| Enforce vehicle passenger interaction devices safety checklist | Medium | Medium |
| Enforce vehicle hardware safety checklist | Medium | Medium |
| Coordinate team responses with other agents (FOC, MOC) | Low | Low |
| Recognize system errors in diagnostic logs | Low | Low |

**This table reads as: the fleet operator should provide a training program to the (*target agent*) that includes how to (*activity)*.**

*Table 9: List of risk mitigation activities by type: work conditions.*

| Activity Type | Work Conditions | |
|---|---|---|
| | **Safety Priority Rank** | **Business Priority Rank** |
| **FOC Safety Operator** | **High** | **Medium** |
| Provide adequate working conditions | Top | Very High |
| Provide and maintain functioning HSI | Top | Low |
| Determine adequate length of shifts | Top | Very High |
| Provide emergency procedure handbooks/guidelines | Medium | Medium |
| **FOC Service Operator** | **High** | **Medium** |
| Provide and maintain functioning HSI | Top | Low |
| Determine adequate length of shifts | Top | Very High |
| Provide adequate working conditions | High | High |
| Provide emergency procedure handbooks/guidelines | Medium | Medium |
| **MOC Coordinators** | **Medium** | **Medium** |
| Provide adequate working conditions | Top | High |
| Determine adequate length of shifts | High | High |
| Provide emergency procedure handbooks/guidelines | Medium | Medium |
| Provide and maintain functioning HSI | Low | Low |
| **MOC Inspection Crew** | **Medium** | **Medium** |
| Provide adequate working conditions | High | High |
| Determine adequate length of shifts | High | High |
| Provide emergency procedure handbooks/guidelines | Medium | Medium |
| Provide and maintain functioning HSI | Low | Low |
| **MOC Maintenance Crew** | **Medium** | **Medium** |
| Provide adequate working conditions | High | High |
| Determine adequate length of shifts | High | High |
| Provide emergency procedure handbooks/guidelines | Medium | Medium |
| Provide and maintain functioning HSI | Low | Low |

**This table reads as: the fleet operator should provide adequate work conditions to the (*target agent*), including (*activity)*.**

# Appendix

## Activity Assessment

Each risk mitigation activity is assigned a business impact category based on the potential safety impact, the estimated resources (cost, time) required for implementation, and how frequently the fleet operator should implement them, as described in the following sections.

### *Safety Impact*

The safety impact is represented by a relative risk level, calculated as a combination of the risk level of the hazards prevented or mitigated by these activities and the relative importance of the activity for each target agent. This is represented by the following expression:

$$f_{RR} = R_{ave} \times I_{rel},$$

where $R_{ave}$ is the average maximum risk of the hazard scenarios prevented or mitigated by these activities and $I_{rel}$ is a value between [0,1] representing the ratio of the number of hazard scenarios impacted by each activity normalized by the total number of scenarios where the target agent participates in. This allows the comparison of each activity independently of the hazard scenarios identified. Table 10 presents the safety impact levels and corresponding average risk threshold. Table 11 provides an example of the use of the safety impact scale with some identified risk mitigation activities.

*Table 10: Safety impact level descriptions.*

| Safety Impact Level | Safety Impact Value | Average Risk Level |
|---|---|---|
| Very Low | 5 | Level <1 |
| Low | 4 | Level 1<2 |
| Moderate | 3 | Level 2<3 |
| High | 2 | Level 3<4 |
| Very High | 1 | > Level 4 |

*Table 11: Example of Safety Impact Scale*

| Target Agent | Activity Type | Activity Purpose | # Hazards Involved | %Relative Importance | Average Risk Level | Relative Risk Level | Safety Impact |
|---|---|---|---|---|---|---|---|
| FOC Safety Operator | Procedures | Record operation logs to support accident investigation. | 15 | 0.50 | 4.33 | 2.17 | Moderate |

| Target Agent | Activity Type | Activity Purpose | # Hazards Involved | %Relative Importance | Average Risk Level | Relative Risk Level | Safety Impact |
|---|---|---|---|---|---|---|---|
| ADS Vehicle | Tools | Communication devices between agents (FOC, MOC) | 29 | 0.94 | 4.56 | 4.26 | Very High |
| FOC Service Operator | Tools | In-vehicle passenger communication devices | 11 | 1.00 | 4.33 | 4.33 | Very High |
| MOC Coordinators | Procedures | Maintenance activities safety checklist | 24 | 0.77 | 4.38 | 3.39 | High |

### *Resources: Cost, Time & Frequency*

Table 12 and Table 13 provide the qualitative measure of the cost and time required to implement the activities, respectively. Additionally, Table 14**Error! Reference source not found.** provides a qualitative measure of how frequent the activities need to be implemented.

*Table 12: Category-based risk mitigation activity assessment scale: implementation cost.*

| Cost Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| High (3) | Activities of high complexity or requiring highly specialized personnel to develop or maintain elements in the system. | Work conditions | Provide and maintain functioning HSI. |
| | | Tools | Provide adequate HSI design to support agent tasks. |
| | | Training | Follow incident management procedures and emergency response. |
| | | Procedures | Interact with first responders/law enforcement. |
| Moderate (2) | Activities requiring multiple parties' participation to be developed and implemented | Work conditions | Determine adequate length of shifts, provide adequate working conditions. |
| | | Tools | Provide vehicle operation intervention mechanisms, passenger interaction cues (audio, video), low-complexity inspection and maintenance tools. |
| | | Training | Coordinate team responses with other agents, select and transmit adequate DDT- |

| Cost Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| | (i.e., fleet operator, ADS developer, first responders, law enforcement). | | fallback strategies, recognize DDT-fallback goals, and evaluate outcomes. |
| | | Procedures | Establish responsibilities during post-incident procedures, implement specified inspection and maintenance contents and performance metrics, enforce ODD, connectivity and local restrictions, coordinate external maintenance activities with ADS Developer |
| Low (1) | Activities that can be developed internally by the fleet operator or can be directly implemented into the workflow. | Work conditions | Provide emergency procedure handbooks/guidelines. |
| | | Tools | Provide in-vehicle passenger and between agents (FOC, MOC) communication devices. |
| | | Procedures | Provide shift take-over procedures, coordinate internal maintenance activities, and record operation logs to support maintenance activities, accident investigation, and operational procedure updates. |
| | | Training | Enforce vehicle inspection and maintenance safety checklist, enforce management of change policies. |

*Table 13: Category-based risk mitigation activity assessment scale: implementation time.*

| Time Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| High (3) | Activities that require extensive time to be designed and validated by specialized personnel. | Tools | Provide adequate HSI design to support agent tasks. |
| | | Procedures | Establish responsibilities during post-incident procedures. |
| | | Training | Follow incident management procedures and emergency response, recognize ODD conditions and system failures, select and transmit adequate DDT-fallback strategies. |
| Moderate (2) | Activities that may require modifications or multiple iterations based on the fleet operator's | Procedures | Provide shift take-over procedures, coordinate internal maintenance activities, manage requests from other agents, interact with passengers and third parties. |
| | | Work conditions | Provide and maintain functioning HSI, provide emergency procedure handbooks/guidelines. |

| Time Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| | experience. This includes the coordination of multiple teams to perform their tasks. | Training | Enforce vehicle inspection and maintenance safety checklist, recognize DDT-fallback goals, and evaluate outcomes, coordinate team responses with other agents, recognize HSI and connectivity failures. |
| | | Tools | Provide vehicle operation intervention mechanisms and vehicle performance tests (at hardware, software, vehicle level). |
| Low (1) | Activities that may receive key input from external entities or directly obtained from external parties. These are implemented by the fleet operator. | Procedures | Record operation logs to support maintenance activities, accident investigation, and operational procedure updates, implement specified inspection and maintenance contents and performance metrics, and establish information-sharing procedures between fleet operator's agents. |
| | | Tools | Provide in-vehicle passenger and between agents (FOC, MOC) communication devices, and provide low-complexity inspection and maintenance tools. |
| | | Training | Enforce management of change policies. |
| | | Work conditions | Determine adequate length of shifts, provide adequate working conditions. |

*Table 14: Category-based risk mitigation activity assessment scale: implementation frequency.*

| Frequency Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| Constant (3) | Activities that must be constantly updated, available, or accessible to the fleet operator's agents. | Work conditions | Provide emergency procedure handbooks/guidelines and maintain functioning HSI. |
| | | Tools | Provide in-vehicle passenger and between agents (FOC, MOC) communication devices. |
| Periodic (2) | Activities expected to be revised on a periodic basis, based upon the input of the ADS developer, other third parties, and | Training | All training procedures are expected to be implemented periodically as defined by the fleet operator and ADS developer. |
| | | Procedures | Interact with first responders/law enforcement, establish responsibilities during post-incident procedures, implement specified inspection and maintenance contents and performance |

| Frequency Level | Level Description | Activity Type | Activity Example |
|---|---|---|---|
| | internal coordination experience. | | metrics, enforce ODD, connectivity and local restrictions. |
| | | Tools | Provide vehicle operation intervention mechanisms and performance tests (hardware, software, and vehicle level). |
| Once (1) | Activities expected not to require modifications after implementation. | Procedures | Record operation logs to support maintenance activities, accident investigation, and operational procedure updates, provide shift take-over procedures, establish information sharing procedures between fleet operator's agents, and coordinate external maintenance activities with ADS Developer. |
| | | Work conditions | Determine adequate length of shifts, provide adequate working conditions. |

### *Business Impact*

Each risk mitigation activity is characterized by the three category-based scales (cost, time, frequency) and the safety impact (derived from the risk scale). A combination of these scales is consolidated into a *business impact* four-dimensional matrix. This impact scale is presented in Table 15.

This table is read as a combination of multiple lower-dimension matrices according to the activities' safety impact, cost, frequency, and time dimension. A "high" business impact relates to low-effort activities with high safety impact i.e., activities that require a comparatively low implementation cost, time, and frequency that prevent or mitigate high-risk hazard scenarios.

*Table 15: Consolidated business impact matrix.*

| Safety Impact | Cost | Frequency | Time | | |
|---|---|---|---|---|---|
| | | | *High* | *Medium* | *Low* |
| Very High | High | Once | 9 | 6 | 3 |
| | | Periodic | 18 | 12 | 6 |
| | | Constant | 27 | 18 | 9 |
| | Medium | Once | 6 | 4 | 2 |
| | | Periodic | 12 | 8 | 4 |
| | | Constant | 18 | 12 | 6 |
| | Low | Once | 3 | 2 | 1 |
| | | Periodic | 6 | 4 | 2 |
| | | Constant | 9 | 6 | 3 |
| High | High | Once | 18 | 12 | 6 |
| | | Periodic | 36 | 24 | 12 |
| | | Constant | 54 | 36 | 18 |
| | Medium | Once | 12 | 8 | 4 |

| Safety Impact | Cost | Frequency | Time | | |
|---|---|---|---|---|---|
| | | | *High* | *Medium* | *Low* |
| | | Periodic | 24 | 16 | 8 |
| | | Constant | 36 | 24 | 12 |
| | Low | Once | 6 | 4 | 2 |
| | | Periodic | 12 | 8 | 4 |
| | | Constant | 18 | 12 | 6 |
| Moderate | High | Once | 27 | 18 | 9 |
| | | Periodic | 54 | 36 | 18 |
| | | Constant | 81 | 54 | 27 |
| | Medium | Once | 18 | 12 | 6 |
| | | Periodic | 36 | 24 | 12 |
| | | Constant | 54 | 36 | 18 |
| | Low | Once | 9 | 6 | 3 |
| | | Periodic | 18 | 12 | 6 |
| | | Constant | 27 | 18 | 9 |
| Low | High | Once | 27 | 18 | 9 |
| | | Periodic | 54 | 36 | 18 |
| | | Constant | 81 | 54 | 27 |
| | Medium | Once | 18 | 12 | 6 |
| | | Periodic | 36 | 24 | 12 |
| | | Constant | 54 | 36 | 18 |
| | Low | Once | 9 | 6 | 3 |
| | | Periodic | 18 | 12 | 6 |
| | | Constant | 27 | 18 | 9 |
| Very Low | High | Once | 27 | 18 | 9 |
| | | Periodic | 54 | 36 | 18 |
| | | Constant | 81 | 54 | 27 |
| | Medium | Once | 18 | 12 | 6 |
| | | Periodic | 36 | 24 | 12 |
| | | Constant | 54 | 36 | 18 |
| | Low | Once | 9 | 6 | 3 |
| | | Periodic | 18 | 12 | 6 |
| | | Constant | 27 | 18 | 9 |

This is represented by the following expression:

$$B_R = S_I \times R_C \times R_T \times R_F,$$

where $R_S$ is the safety impact rank (1-5 scale, see Table 10), $R_C$ is the implementation cost level (1-3 scale, see Table 12), $R_T$ is the implementation time level (1-3 scale, see Table 13) and $R_F$ is the frequency of implementation (1-3 scale, see Table 14). The values of $B_I$ are then organized into the categories presented in Table 16.

*Table 16: Business Impact Scale Levels.*

| Business Impact | Business Priority Rank Range |
|---|---|
| Very High | [1, 4] |
| High | [5, 8] |
| Moderate | [9, 24] |
| Low | >24 |

### *Safety Priority Rank*

Some activities with high safety impact may require a higher implementation cost or time or need to be implemented periodically or constantly. This business impact scale would then rank these activities with a low priority. Hence, a modification is introduced to counter this. Any risk mitigation activity with a "Very High" or "High" safety impact is prioritized with a Safety Priority Rank 1. This process overrides the business impact scale for those activities but retains the rank for lower safety impact activities. This is represented by the following expression, resulting in the categories presented in Table 17.

$$S_R = \begin{cases} 1 & if \ \leq 2 \\ B_R & if \ S_I > 2 \end{cases}$$

*Table 17: Safety Priority Scale Levels.*

| **Safety Priority** | **Safety Priority Rank Range** |
|---|---|
| Top | 1 |
| Very High | [2, 4] |
| High | [5, 8] |
| Moderate | [9, 24] |
| Low | >24 |