

Eric JENN(1), Arnaud DIEUMEGARD(1), Bruno d’AUSBOURG(2), Vincent LECRUBIER(2), Yamine AÏT-AMEUR(3)

1. <prénom>.<nom>@onera.fr, (2) <prénom>.<nom>@onera.fr, (3)yamine@enseeiht.fr

Abstract

This document gives the specification and LIDL model of the RWS HMI

Rover Warning System

LIDL modeling

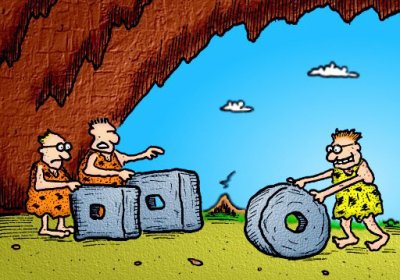


Table of Contents

[1 Definitions 5](#_Toc454180215)

[2 Specification 5](#_Toc454180216)

Document history

|  |  |  |
| --- | --- | --- |
| Version | Modification | Location |
| 0.0 | Creation | All |

# Definitions

[D] The **RWS** is the system in charge of the computation and presentation of alerts. It is composed of two mains part: a **RWS core** in charge of computing the state of all alerts, and a **RWS HMI** in charge of the presentation of the alerts to the **supervisor**.

[D] The supervision operator is referred to as **supervisor** in the specification.

[D] The terms “**event occurrence**” refers to something that takes place at a certain place in space and time. The term “**event**” refers to the set of all event occurrences that share certain common characteristics, in the same way as a class describes all the individual objects that share the same structure. An event is a class of event occurrences. "Activation of alert A" is an event. The actual activations of alert A at times , , are occurrences of the event "Activation of alert A".

[D] An **alert** refers to some specific condition on the monitored system. For instance, “left wheel is blocked” is an alert. Satisfaction (or “activation”) of the condition “left wheel is blocked” is an event. The actual blocking of the wheel at time is an occurrence of the event “left wheel is blocked”.

[D] An **alert signal** is the means by which the supervisor is informed of the occurrence of the alert activation. The **transmission** of the alert signal to the supervisor is also called “presentation”. It shall be noted that if the occurrence of the alert signal is conditioned by the satisfaction of some alert condition, the signal may continue to exist while the condition is negated. It shall also be noted that the signal may cease to be transmitted to the supervisor for some time or be transmitted to the supervisor on demand (see specification).

[D] Activation conditions are evaluated from data produced by the rovers, the supervision station, the in-door stations, and the activation state of other alerts.

[D] The **monitored system** is composed of: (i) a set of rovers, (ii) a supervision station, (iii) a set of in-door GPS stations (3 stations). It also covers all required communication means between these elements.

[D] The **global system** is composed of the **monitored system** and the **supervisor**.

[D] Alerts are categorized as "caution", "warning" or "advisory".

# Specification

**[R1] Signalling of alerts**

The RWS IHM shall signal alerts occurrences to the supervision operator. The reception of an alert signal shall provide the supervisor with sufficient information about the situation (e.g., which alert, at what time,…) during sufficient time. We consider that situation awareness is possible if the information is presented continuously to the supervisor for at least 3 seconds.

□

**[R2] Separation between alerts signals**

The signalling of an alert occurrence shall not alter / jeopardize the signalling of another alert occurrence.

□

*Rationale: Let the occurrence of alert A be presented to the supervisor when occurrence of alert B occurs. Then the message related to B shall not cover the message related to A up to the point where it makes message related to A unintelligible. Separation between messages related to alert A and alert B may be ensure in space and/or time.*

**[R3] Navigation through alert signals**

If all alert signals cannot be transmitted at once to the supervisor, s/he shall be able to “navigate” through the set of alert signals in order for the transmission to be done sequentially.

□

[D] The RWS is hosted on the supervision station. The rovers communicate directly with the supervision station. The in-door GPS stations communicate indirectly with the supervision station through the rovers.

**[PRE] Alerts are be predefined.**

□

**[R4] Uniqueness of alert signals**

There shall be a unique signal for a given alert. If the signal for alert A is active (presented or not to the supervisor), then no other occurrence of alert A can be signalled to the supervisor.



□

**[PRE]** An alert may occur at any time.

□

**[R5] Presentation latency**

An alert signal shall be transmitted to the supervisor within at most 100ms after the triggering of the activation condition.

□

**[R6] Presentation duration**

An alert signal shall be transmissible (not necessarily transmitted) to the supervisor until it is cleared.

□

**[R7] Acknowledgment**

The RWS IHM shall provide the supervisor with a means to confirm that s/he has actually received the alert signal. This is referred to as « acknowledgement ».

□

**[R8] Automatic acknowledgment**

An alert may be acknowledged automatically when the alert activation condition is negated.

□

**[R9] Concurrence between automatic and manual acknowledgment**

An alert shall always be acknowledgeable by the supervisor even if automatic acknowledgment is configured.

□

**[R10] Acknowledgment configuration**

The choice between automatic or supervisor-initiated acknowledgement shall be alert-specific and be defined by configuration.

□

**[R11] Acknowledgment state transmission**

The alert signal shall transmit the acknowledgement state of the alert.

□

**[R12] Indication of non-transmitted alert signals**

If the RWS IHM cannot transmit the alert signal to the supervisor (for instance due to lack of space), it shall at least transmit a signal indicating that there is a non-transmissible alert signal.

□

**[R13] Provision of means to transmit alert signals**

If the RWS IHM cannot transmit the alert signal to the supervisor (for instance due to lack of space), it shall provide some means to activate the transmission of those alert signals. Hints shall be provided to the supervisor to facilitate this operation.

□

**[R14] Number of non-transmitted alert signals**

If all active alerts cannot be presented simultaneously, an indicator shall be provided to the supervisor to let him know the total number of non-transmitted alert signals.

□

**[R15] Manual clearing of alert signals**

The RWS HMI shall provide a means for the supervisor to clear an alert signal.

□

**[R16] Clearing alert signals**

Once cleared, an alert signal shall cease to be transmitted to the supervisor. Note that a new occurrence of the same alert signal may be transmitted later to the supervisor if the associated alert condition becomes asserted again.

□

**[R17] Relation between acknowledging and clearing alert signals**

An alert may only be cleared after being acknowledged.

□

**[R18] Automatic clearing of alert signals**

An acknowledged alert signal may be cleared automatically when its activation condition is negated.

□

**[R19] Clearing configuration**

The choice between automatic or supervisor-initiated clearing shall be alert-specific and be defined by configuration.

□

**[R20] Priorities of alert signals**

Alert signals shall be transmitted to the supervisor in such a way that alerts with high priorities are received by the supervisor *preferably* before alerts with lower priorities. Priority is defined according to the following precedence relations (level is used to sort alerts when attributes at levels are equal):

1. Level 1: "warning" > "caution" > "advisory"
2. Level 2: priority within the category
3. Level 3: "not acked" > "acked"
4. Level 4: increasing time stamp. Timestamps are unique and monotonically increasing.

□

**[R21] Attention getter**

The attention of the supervisor shall be captured when an alert signal occurs.

□

**[R22] Procedures**

The supervisor shall be able to activate the presentation of the procedure associated with any signalled alert. Any alert may have an associated procedure. This is defined by configuration.

□

**[R23] Relation between procedures and alert signals**

The presentation of the alert / procedure shall clearly establish the relation between the alert signal and the procedure.

□

**[R24] Procedure contents**

A procedure describes a sequence of actions to be performed by the supervisor. Each actions is called a “step”. Each step is associated with a message to be presented to the supervisor. The message describes an action to be carried out by the supervisor to diagnose, correct, etc. the associated alert. At a given step in the procedure, the last 2 steps (if possible) and the next 2 steps (if possible) shall be presented to the user so that s/he can build a mental representation of what he is doing and anticipate the next actions.

□

**[R25] Presentation of the current step**

The current step shall be clearly indicated on the presented procedure.

□

**[R26] Cancelling a procedure**

The supervisor shall be able to cancel a procedure. Cancelling a procedure means « ceasing » to present the procedure. The procedure may be presented again. In that case, it shall start again at the first step of the procedure.

□

**[R27] Presentation of the procedure state**

The state of the procedure (“not yet started”, “completed”, or “at step <X>”) shall be transmitted by the alert signal.

□

**[R28] Stacking of procedures**

It shall be able to present procedure for alert B while procedure for alert A is being presented. The supervisor shall be able to come back to procedure A and continue the procedure from the step where it was interrupted.

□

**[R29] Initial step of the procedures**

All procedures are set in their initial state at system startup.

□

**[R30] Effect of alert signal clearing on procedures**

When an alert is manually cleared, the procedure shall be abandoned (even if it was interrupted by the opening of another alert). Note: the procedure shall not be abandoned if the alert is automatically cleared.

□

**[R31] Effect of alert signal clearing on procedure stacking**

When a procedure is cancelled, any active procedure that was interrupted by the one that is cancelled shall be presented again (in FIFO order).

□

**[R32] Procedure actions**

The next step of a procedure may be determined by a supervisor action. Actions are “YES/NO/ DONE”.

□