Modelling an Aircraft Landing System in Event-B*

Dominique Méry
Université de Lorraine, LORIA
BP 239, Nancy, France
Dominique.Mery@loria.fr

Neeraj Kumar Singh
McMaster Centre for Software Certification
Hamilton, ON, Canada
singhn10@mcmaster.ca

July 3, 2014

Abstract

The failure of hardware or software in a critical system can lead to loss of lives. The design errors can be main source of the failures that can be introduced during system development process. Formal techniques are an alternative approach to verify the correctness of critical systems, overcoming limitations of the traditional validation techniques such as simulation and testing. The increasing complexity and failure rate brings new challenges in the area of verification and validation of avionic systems. Since the reliability of the software cannot be quantified, the *correct by construction* approach can implement a reliable system. Refinement plays a major role to build a large system incrementally from an abstract specification to a concrete system. This paper contributes as a stepwise formal development of the landing system of an aircraft. The formal models include the complex behaviour, temporal behaviour and sequence of operations of the landing gear system. The models are formalized in Event-B modelling language, which supports stepwise refinement. This case study is considered as a benchmark for techniques and tools dedicated to the verification of behavioural properties of systems.

Keywords

Abstract model, Event-B, Event-driven approach, Proof-based development, Refinement, Landing Gear System

1 Introduction

In the cutting edge technology of aircraft, the requirements for avionic systems become increasingly complex. The failure of hardware or software in such a complex system

*The current report is the companion paper of the paper [17] accepted for publication in the volume 433 of the serie Communications in Computer Information Science. The Event-B models are available at the link http://eb2all.loria.fr. Processed on July 3, 2014.

can lead to loss of lives. The increasing complexity and failure rate brings new challenges in the area of verification and validation of avionic systems. The Federal Aviation Administration (FAA) ensures that aircraft meets highest safety standards. The FAA recommends the catastrophic failures of the aircraft and suggests probabilities of failure on the order of per flight hour [12].

Hardware component failures and design errors are two main reasonable factors to major the reliability of the avionics. There are several techniques like redundancy and voting are used to handle the hardware failures. However, the design errors can be introduced at the development phase, which may include errors in the system specification, and errors made during the implementation of the software or hardware [14].

The complexity of software has been tremendously increased. Our experience, intuition and developed methodologies is reliable for building the continuous system, but software exhibits discontinuous behaviour. To verify the correctness of the system, it is highly desirable to reason about millions of sequences of discrete state transitions. Traditional techniques like testing and simulations are infeasible to test the correctness of a system [7]. Since the reliability of the software cannot be quantified, the avionic software must be developed using *correct by construction* [15] approach that can produce the correct design and implementation of the final system [19].

This paper describes how rigorous analysis employing formal methods can be applied to the software development process. Formal methods is considered as an alternative approach for certification in the DO-178B standard for avionics software development. We propose the refinement based correct by construction approach to develop a critical system. The nature of the refinement that we verify using the RODIN [18] proof tools is a safety refinement. Thus, the behaviour of final resulting system is preserved by an abstract model as well as in the correctly refined models. Proof-based development methods [1] integrate formal proof techniques in the development of software systems. The main idea is to start with a very abstract model of the system under development. Details are gradually added to this first model by building a sequence of more concrete events. The relationship between two successive models in this sequence is *refinement* [1, 3]. Here we present stepwise development to model and verify such interdisciplinary requirements in Event-B [8, 1] modelling language. The correctness of each step is proved in order to achieve a reliable system.

In this paper, we present the stepwise formalization of the benchmark case study landing system of an aircraft. The current work intends to explore those problems related to modelling the sequence of operations of landing gears and doors associated with hydraulic cylinders under the real-time constraints and to evaluate the refinement process.

The outline of the remaining paper is as follows. Section 2 presents selection of the case study related to the landing system of an aircraft for formalization. In Section 3, we explore the incremental proof-based formal development of the landing system. Finally, in Section 4, we conclude the paper.

2 Basic Overview of Landing Gear System

The landing gear is an essential system that allows an aircraft to land safely, and supports the entire weight of an aircraft during landing and ground operations. The basic engineering and operational behaviors behind a landing gear system are very complex. There are several types of gears, which depend on the aircraft design and its intended use. Most landing gears have wheels to facilitate operation to and form hard surfaces,

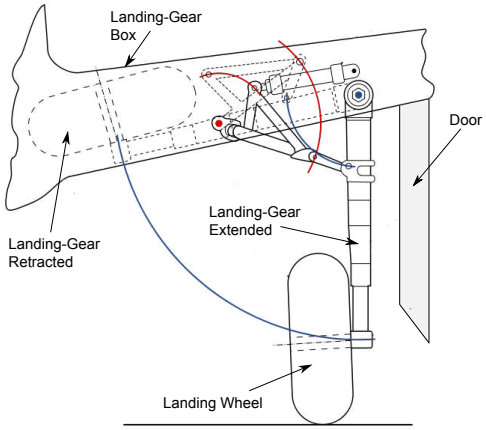

Figure 1: Landing Gear System

such as airport runways [11].

Three basic arrangements of landing gear are used: tail wheel type landing gear, tandem landing gear, and tricycle-type landing gear. The most commonly used landing gear arrangement is the tricycle-type landing gear. All these aircraft landing gears are further classified into fixed and retractable categories. Single engine and light weight aircrafts use fixed landing gear while the retractable gear is used in heavy aircrafts [11].

The landing system controls the maneuvering landing gears and associated doors. Fig. 1 depicts basic components of a landing system. The landing system is made of three different landing sets, which corresponds to front, left and right. The main components of a landing system are doors, landing gears and hydraulic cylinders.

The landing gear system is controlled by the software in nominal operating mode, and an emergency mode is handled analogically. Generally, landing system always use nominal mode. In case of system failure, the pilot can activate the emergency mode. However, the landing system can be activated in emergency mode only when any anomaly is detected in the system.

There are sequential operations of the landing gear system. The sequential operations for extending gears are: open the doors of gear boxes, extend the landing gears, and close the doors. Similarly the sequential operations for retraction gears are: open the door, retract the landing gears, and close the doors. During these sequential operations there are several parameters and conditions, which can be used to assess the health of a landing system [6].

There are three main components of the landing gear system: 1) mechanical system, 2) digital system, and 3) pilot interface. The mechanical system is composed of three landing sets, where each set contains landing gear box, and a door with latching boxes. The landing gears and doors motions are performed with the help of cylinders. The cylinder position is used to identify the various states of the door or landing gear positions. Hydraulic power is used to control the cylinders with the help of electro-valves. These electro-valves are activated by a digital system. The digital system is composed of two identical computing modules, which execute parallel. The digital system is only the responsible for controlling mechanical parts like gears and doors, and for detecting anomalies. The pilot interface has an Up/Down handle and a set of indicators. The handle is used by pilot for extending or retracting the landing gear

sequence, and a set of indicators is the different type of lights for giving the actual position of gears and doors, and the system state. A detailed description of the landing gear system is given in [11, 6].

The landing gear system is a critical embedded system, where all the operations are based on the state of a physical device, and required temporal behaviour. The main challenge is to model the system behaviour of the landing gear system, and to prove the safety requirements under the consideration of physical behaviour of hydraulic devices.

3 Formal Development of the Landing System

The development is progressively designing the landing system by integrating observations and elements of the document. The first model is specific as abstract as possible and it captures the different possible *big* steps of the system by defining the synchronous atomic events. For example, the sequence of door opening, door closing, gear extension and gear retraction etc.

3.1 M1: Moving Up and Down

When the system is moving up (resp. *down*) till retraction (resp. extension), it will be in a position *halt* and *up* (resp. *down*), namely *haltup* (resp. *haltdown)*. The first model observes the positions of the global state which considers that the landing system is either moving *down* from a *haltup* position, or moving *up* from a *haltdown* position. The global state expresses the state of handle at an initialization in a *down* state ($button := DOWN$) and the gear system is halted in a *haltdown* position ($phase := haltdown$). It means that initially the gear system is extended and locked. Two state variables record these informations namely $button$ and $phase$. Events model the possible observable actions and modifications over the global system:

- PressDOWN is enabled, when the gear system is halted up and retracted; the system is in a new state corresponding to the *movingup* action. The intention is to extend the gear system.
- PressUP is enabled, when the gear system is halted down and extended; the system is in a new state corresponding to the *movingdown* action. The intention if to retract the gear system.

Moreover, when one of events PressDOWN or PressUP (solid labelled transitions in Fig. 2) is observed, the system should provide a *service* corresponding to an effective action (dashed labelled transitions in Fig. 2) of the landing system and physically moving gears. The landing system *reacts* (dashed labelled transitions in Fig. 2) to the orders of the pilot (solid labelled transitions in Fig. 2).

- movingup is an action supported by engine which helps to move the landing system into the state *haltup* and to the retracted state.
- movingdopwn is an action supported by engine which helps to move the landing system into the state *haltdown* and to the extended state.

Events express that, when the button remains UP (resp. DOWN), the reaction of the system is to reach the state *retracted* (resp. *extended*). The current diagram assumes that the system is operating in normal mode. The detection of anomalies is left for the

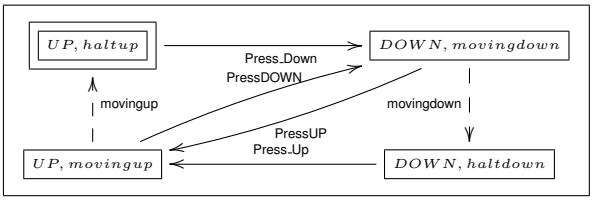

Figure 2: State-based automaton for the model M1

next refinements. The diagram contains the main goals of the system which is operating in a cyclic mode. The requirements R11bis and R12bis are clearly satisfied, as well as R12 and R11. Other requirements are not considered since they are related to features that are not yet defined.

3.2 M2: Opening and Closing Doors

The model M2 is considering different possible steps in the moving up or in the moving down phases. However, the different steps are possibly victims of counters orders. The pilot decides to press UP and then to press DOWN or reciprocally. These movements affect the classical cycle of the system starting from a locked closed position to another one without interrupt. First observation leads to consider that we identify that doors are alternatively *opening* and *closing*. We add a detail on the fact that the doors are opened when they are unlocked and when they are closed, they are locked. A new state is enriching the previous one by a state variable for doors states ($dstate$) and a variable for expressing when doors are locked ($lstate$). Three variables are used to control the possible change of decisions and expressing the sequentialisation of *extension* scenario or *retraction* scenario: p, l, i.

The next invariant states that when the doors are opened, the doors are unlocked ($M2\_inv5$); when one door is opened, all the doors are opened ($M2\_inv3$) and when a door is closed, all the doors are closed ($M2\_inv4$).

$M2\_inv1 : dstate \in DOORS \rightarrow SDOORS$
$M2\_inv2 : lstate \in DOORS \rightarrow SLOCKS$
$M2\_inv3 : dstate^{-1}[\{OPEN\}] \neq \varnothing \Rightarrow dstate^{-1}[\{OPEN\}] = DOORS$
$M2\_inv4 : dstate^{-1}[\{CLOSED\}] \neq \varnothing \Rightarrow dstate^{-1}[\{CLOSED\}] = DOORS$
$M2\_inv5 : dstate[DOORS] = \{OPEN\} \Rightarrow lstate[DOORS] = \{UNLOCKED\}$
$M2\_inv6 : l = E \wedge p = R \Rightarrow lstate[DOORS] = \{UNLOCKED\}$
$M2\_inv7 : l = R \wedge p = E \Rightarrow lstate[DOORS] = \{UNLOCKED\}$

Events are now capturing the observation of opening and closing with possible counter orders by the pilot. We have not yet considered the state of *flying* or *grounding*. Initially, doors are closed and the state is *haltdown*. It means that the landing system is corresponding to a state on ground and should be obviously extended. The three auxiliary variables (p,l,i) are set to R to mean that the system is ready to retract whenever the pilot wants. We do not consider the case when a *crazy* pilot would try to retract when the aircraft is on the ground but we may consider that we observe a safe situation. Further refinements will forbid these kinds of possible behaviours. Events are refining the previous four events and we refine the two events PressDown and PressUp by events that can interrupt the initial scenario and switch to the other scenario. Fig. 3 describes the state-based automaton for the model M2 and we use the following notations UP for $button = UP$, DN for $button = DOWN$, C for $dstate[DOORSQ] =$

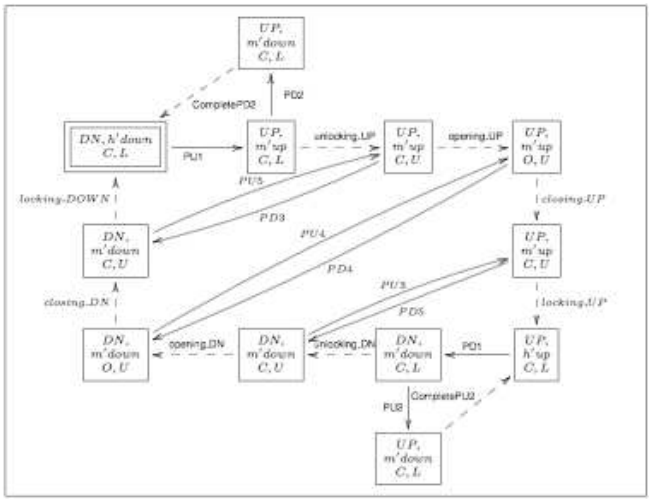

Figure 3: State-based Automaton for Events in model M2

$\{CLOSED\}$, O for $dstate[DOORSQ] = \{OPEN\}$, L for $lstate[DOORSQ] = \{LOCKED\}$, U for $lstate[DOORSQ] = \{UNLOCKED\}$, $m'down$ for $phase = movingdown$",m'upforphase=movingup,h'downforphase=haltdown", $h'up$ for $phase = haltup$. The dashed and plain arrows present the distinction between two different types of actions. Dashed arrows show that it is an action of the system, and plain arrows show that it is an action of the pilot.

The diagram Fig. 3 confirms the requirements. The model is validated using ProB and the sequences of retraction and extension are observed according to the requirements.

3.3 M3: Observing the gears

The next observation leads us to consider the full mechanical system. In fact, doors are opened and closed but we have the time to see that gears are either moving out (extension scenario) or moving in (retraction scenario). The next model is refining the previous one by adding gears and observing different states of the gears ($gstate \in GEARS \rightarrow SGEARS$). $SGEARS$ is defined as enumerated set $partition(SGEARS, \{RETRACTED\}, \{EXTENDED\}, \{RETRACTING\}, \{EXTENDING\})$ to capture the multiple states of gears. There are obvious invariant properties that express that the doors are opened when the gears are moving. The invariants are listed as follow:

$$
\begin{array}{l}
M3\_inv1 : gstate \in GEARS \rightarrow SGEARS \\
M3\_inv2 : \forall door \cdot \left(\begin{array}{l} door \in DOORS \wedge dstate(door) = CLOSED \\ \wedge ran(gstate) \neq \{RETRACTED\} \\ \Rightarrow \\ ran(gstate) = \{EXTENDED\} \end{array} \right) \\
M3\_inv3 : \forall door \cdot \left(\begin{array}{l} door \in DOORS \wedge dstate(door) = CLOSED \\ \wedge ran(gstate) \neq \{EXTENDED\} \\ \Rightarrow \\ ran(gstate) = \{RETRACTED\} \end{array} \right)
\end{array}
$$

$$M3\_inv4 : \left(\begin{array}{l} ran(gstate) \neq \{RETRACTED\} \wedge ran(gstate) \neq \{EXTENDED\} \\ \Rightarrow \\ ran(dstate) = \{OPEN\} \end{array} \right)$$

$$M3\_inv5 : \left(\begin{array}{l} ran(dstate) = \{CLOSED\} \\ \Rightarrow \\ ran(gstate) \cap \{RETRACTING, EXTENDING\} = \varnothing \end{array} \right)$$

$M3\_inv2$ and $M3\_inv3$ express that when doors are opened, either the gears are extended or the gears are retracted. When the doors are closed, the gears are not in moving state ($M3\_inv4$ and $M3\_inv5$). When the gears are moving, the doors are opened. The expression of the simultaneaous state of the doors either closed or opened, as well as the gears either extended or retracted, prepare the conditions of the synchronisation over the doors and the gears. Fig. 3 is now detailed by splitting the two states $(DN, m'down, O, U)$ and $(UP, m'up, O, U)$ and by considering that the new variable $gstate$ is modified at this stage. We are introducing four new events corresponding to the retraction of gears and to the extension of gears.

The *retraction* phase is decomposed into two events retracting_gears and retraction and the gears are transiting from a state *EXTENDED* into the state *RETRACTING* and finally the state *RETRACTED*.

EVENT retracting_gears
  WHEN
    $grd1 : dstate[DOORS] = \{OPEN\}$
    $grd2 : gstate[GEARS] = \{EXTENDED\}$
    $grd3 : p = R$
  THEN
    $act1 : gstate := \{a \mapsto b | a \in GEARS \wedge b = RETRACTING\}$
  END
EVENT retraction
  WHEN
    $grd1 : dstate[DOORS] = \{OPEN\}$
    $grd2 : gstate[GEARS] = \{RETRACTING\}$
  THEN
    $act1 : gstate := \{a \mapsto b | a \in GEARS \wedge b = RETRACTED\}$
  END

The *extension* phase is decomposed into two events extending_gears and extension and the gears are transiting from a state *RETRACTED* into the state *EXTENDING* and finally the state *EXTENDED*.

EVENT extending_gears
  WHEN
    $grd1 : dstate[DOORS] = \{OPEN\}$
    $grd2 : gstate[GEARS] = \{RETRACTED\}$
    $grd3 : p = E$
  THEN
    $act1 : gstate := \{a \mapsto b | a \in GEARS \wedge b = EXTENDING\}$
  END
EVENT extension
  WHEN
    $grd1 : dstate[DOORS] = \{OPEN\}$
    $grd2 : gstate[GEARS] = \{EXTENDING\}$
  THEN
    $act1 : gstate := \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\}$
  END

The events PU4 and PD4 are both refined into three events which are controlling or switching from the retraction to the extension and vice-versa. The two possible scenarios (extension and retraction) have a meaning and we can address the requirements R21 and R22.

The model M3 is refined into a new model called M30 which is *forbidden* the use of buttons. The model is clearly satisfying the requirement over the successive actions. ProB is also used to validate the behaviour of system.

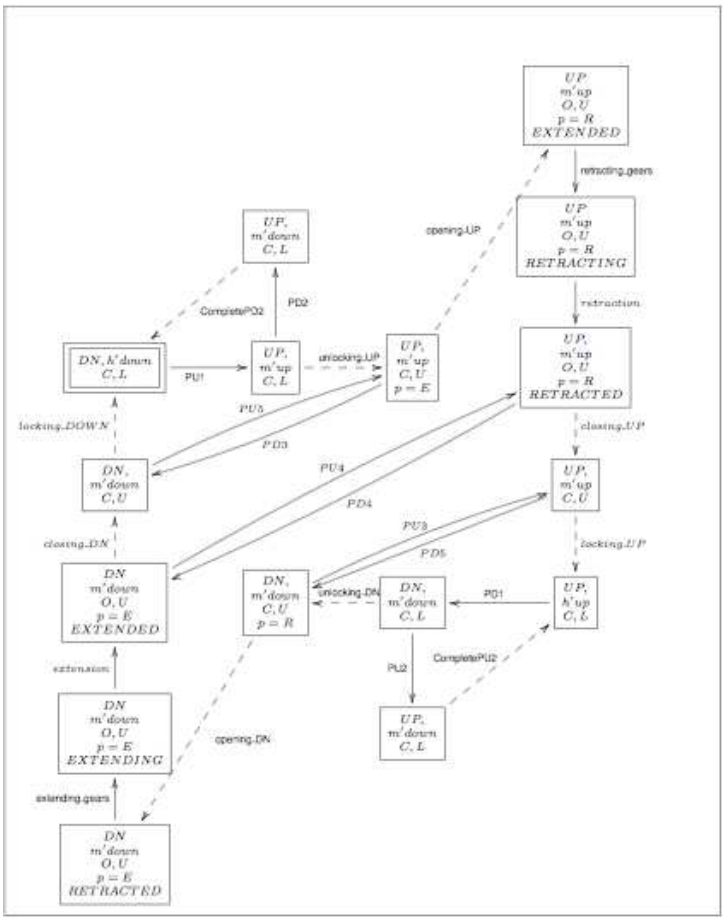

Figure 4: State-based Automaton for Events in model M3

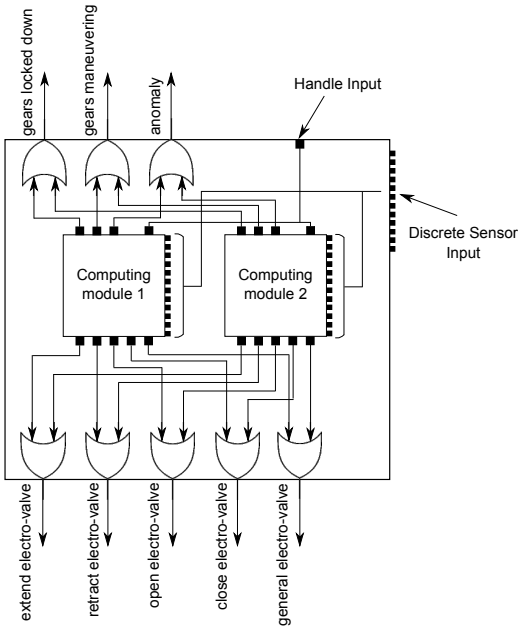

Figure 5: Architecture of the computing modules

3.4 M4: Sensors and Actuators

In this refinement, we address the problem of sensors and actuators. We introduce the management of sensors and actuators by considering the collection of values of sensors and an abstract expression of computing modules for analysing the sensed values. We introduce a list of new variables according to the Fig. 5:

- Variables for expressing the sensors states: *handle* (for the pilot interface), *analogical_switch*, *gear_extended* (sensor for detecting an extension activity), *gear_retracted* (sensor for detecting a retraction activity), *gear_shock_absorber* (sensor for detecting the flight or ground mode), *door_closed* (sensor for stating when the doors are closed), *door_open* (sensor for stating when the doors are opened), *circuit_pressurized* (sensor for the pressure control).
- Variables for getting the evaluation of the sensed states of the system by the computing modules: *general_EV*, *close_EV*, *retract_EV*, *extend_EV*, *open_EV*.
- Variables for modelling the computation of the sensed state from the collected sensed values: *general_EV_func*, *close_EV_func*, *retract_EV_func*, *extend_EV_func*, *open_EV_func*.
- Variables for collecting output of computing modules: *gears_locked_down*, *gears_man*, *anomaly*.

New variables are used for adding some constraints over guards of previous events:

- HPD1 and HPU1 are two events corresponding to the order by the pilot interface to extend (HPD1) or to retract (HPU1) the gears. For instance, the guard $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$ senses that the handle is UP and then it moves to

DOWN ($handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$. The sensors are triplicated and we define each sensor value by a function from 1..3 into the sensors values.

- Analogical_switch_closed and Analogical_switch_open are two events for updating the general switch for protecting the system agiants abnormal behaviour of the digital part.
- Circuit_pressurized manages the sensor of the pressure control.
- Computing_Module_1_2 models in a very abstract way for computing and updating of EV variables using sensors values.
- Failure_Detection detects any failure in the system.

The model introduces sensors and values synthesized from sensors values. We have used a very abstract way to state the values of sensors. The model M4 is not analyse-able with ProB. The previous requirements R11, R11bis, R12, R12bis, R22, R21 are remaining satisfied by the model M4 by refinement. We need to strengthening the guards of events ($\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$). The reader will notice that the two events HPU1 and HPD1 are the external interfaces for controlling the events to associate the functionality of handle with old variable $button$. The guard $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b = ground\}$ indicates that now we know that either we are on the ground or not: it means that we assume that sensors are trusted and this assumption is valid. The state of $gear\_shock\_absorber$ is modified according to the figure 11, page 12 of [6] and it is the reason for updating in two events extension and retraction.

In this refinement, the number of proof obligations is very high (247) but it is possible to add intermediate models for progressive development.

- The two events HPU1 and HPD1 are adding a small amount of new proof obligations.
- The unproved proof obligations appearing in the summary are mainly typing properties and they are discharged either using the SMT solver or a procedure. We consider that they are pseudo-automatic proof obligations.

3.5 M5: Managing electro-valves

The model M5 takes into account the management of electro-valves used for moving the gears from a position to another one. Four new variables are modelling pressure states (page 10, subsection 3.2, Electro-valves) and they model the hydraulical features of the system: $general\_EV\_Hout$, $close\_EV\_Hout$, $retract\_EV\_Hout$, $extend\_EV\_Hout$, $open\_EV\_Hout$, A_Switch_Out. The invariant is stating that either the pressure is on or off by the two possible values: 0 or Hin:

$$
\begin{array}{l}
inv1 : general\_EV\_Hout \in \{0, Hin\} \\
inv2 : close\_EV\_Hout \in \{0, Hin\} \\
inv3 : retract\_EV\_Hout \in \{0, Hin\} \\
inv4 : extend\_EV\_Hout \in \{0, Hin\} \\
inv5 : open\_EV\_Hout \in \{0, Hin\}
\end{array}
$$

The summary of new proof obligations is simply that 19 new proof obligations are generated and automatically discharged. In the previous development, the values were

less precise and we got a problem in the next refinements with some proof obligations to discharge. A new event Update_Hout is introduced to update the values of sensors for the hyraulic part:

EVENT Update_Hout
BEGIN

$$act1 : general\_EV\_Hout :| \left(\begin{array}{l} (general\_EV = TRUE \wedge general\_EV\_Hout' = Hin) \\ \vee (general\_EV = FALSE \wedge general\_EV\_Hout' = 0) \\ \vee (A\_Switch\_Out = TRUE \wedge general\_EV\_Hout' = Hin) \\ \vee (A\_Switch\_Out = FALSE \wedge general\_EV\_Hout' = 0) \end{array} \right)$$

$$act2 : close\_EV\_Hout :| \left(\begin{array}{l} (close\_EV = TRUE \wedge close\_EV\_Hout' = Hin) \\ \vee (close\_EV = FALSE \wedge close\_EV\_Hout' = 0) \end{array} \right)$$

$$act3 : open\_EV\_Hout :| \left(\begin{array}{l} (open\_EV = TRUE \wedge open\_EV\_Hout' = Hin) \\ \vee (open\_EV = FALSE \wedge open\_EV\_Hout' = 0) \end{array} \right)$$

$$act4 : extend\_EV\_Hout :| \left(\begin{array}{l} (extend\_EV = TRUE \wedge extend\_EV\_Hout' = Hin) \\ \vee (extend\_EV = FALSE \wedge extend\_EV\_Hout' = 0) \end{array} \right)$$

$$act5 : retract\_EV\_Hout :| \left(\begin{array}{l} (retract\_EV = TRUE \wedge retract\_EV\_Hout' = Hin) \\ \vee (retract\_EV = FALSE \wedge retract\_EV\_Hout' = 0) \end{array} \right)$$

END

The event Circuit_pressurized is refined by two events considering that the sensing is OK or not; it assigns the value of $Hout$.

EVENT Circuit_pressurized
REFINES Circuit_pressurized
WHEN
$grd1 : general\_EV\_Hout = Hin$
THEN
$act9 : circuit\_pressurized :\in 1 \,..\, 3 \rightarrow \{TRUE\}$
END

EVENT Circuit_pressurized_notOK
REFINES Circuit_pressurized
WHEN
$grd1 : general\_EV\_Hout = 0$
THEN
$act9 : circuit\_pressurized :\in 1 \,..\, 3 \rightarrow \{FALSE\}$
END

3.6 M6: Integrating Cylinders Behaviours

The next step is to integrate the cylinders behaviour according to the electro-valves circuit and to control the process, which is computing from sensors values the global state of the system. It leads to strengthen guards of events opening and closing doors and gears using cyliders sensors and hydraulic pressure (opening_doors_DOWN, opening_doors_UP, closing_doors_UP, closing_doors_DOWN, unlocking_UP, locking_UP, unlocking_DOWN, locking_DOWN, retracting_gears, retraction, extending_gears, extension). The event CylinderMovingOrStop models the change of the cylinders according to the pressure, when the value of $state$ is $cylinder$. It leads to a next state which *activates* the computing modules.

EVENT CylinderMovingOrStop

Cylinder Moving or Stop according to the output of hydraulic circuit

WHEN

$grd1 : state = cylinder$

THEN

$act1 : SGCylinder : |$

$$\left(\begin{array}{l} \left(\begin{array}{l} SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \\ \wedge\ extend\_EV\_Hout = Hin \end{array} \right) \\ \vee \left(\begin{array}{l} SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \\ \wedge\ extend\_EV\_Hout = 0 \end{array} \right) \\ \vee \left(\begin{array}{l} SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \\ \wedge\ retract\_EV\_Hout = Hin \end{array} \right) \\ \vee \left(\begin{array}{l} SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \\ \wedge\ retract\_EV\_Hout = 0 \end{array} \right) \end{array} \right)$$

$act2 : SDCylinder : |$

$$\left(\begin{array}{l} \left(\begin{array}{l} SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \\ \wedge\ open\_EV\_Hout = Hin \end{array} \right) \\ \vee \left(\begin{array}{l} SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \\ \wedge\ open\_EV\_Hout = 0 \end{array} \right) \\ \vee \left(\begin{array}{l} SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \\ \wedge\ close\_EV\_Hout = Hin \end{array} \right) \\ \vee \left(\begin{array}{l} SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \\ \wedge\ close\_EV\_Hout = 0 \end{array} \right) \end{array} \right)$$

$act3 : state := computing$

END

More than 50 % of the proof obligations are manually discharged. However, it appears that the disjunction of actions allows us to have a unique view of the cylinders behaviours. The proofs to discharge are not complex and are mainly discharged by several clicks on procedures buttons.

3.7 M7: Failure Detection

The model M7 is modelling the detection of different possible failures. Page 16 and page 17 of the case study have given a list of conditions for detecting anomalies: *Analogical switch monitoring, Pressure sensor monitoring, Doors motion monitoring, Gears motion monitoring, Expected behavior in case of anomaly.* The decision is to refine the event Failure_Detection into six events which are modelling the different cases for failure detection: Failure_Detection_Generic_Monitoring, Failure_Detection_Ana-logical_Switch, Failure_Detection_Pressure_Sensor, Failure_Detection_Doors, Failure_Detection_Gears, Failure_Detection_Generic_Monitoring. The decision is to postpone the introduction of timing constraints in the last model. However, we have to strengthen the guards of events opening_doors_DOWN, opening_doors_UP, closing_doors_UP, closing_doors_DOWN, unlocking_UP, locking_UP, unlocking_DOWN, locking_DOWN by adding a condition $anomaly = FALSE$.

3.8 M8: Timing Requirements

The time pattern [9] provides a way to add timing properties. The pattern adds an event tic_tock simulating the progression of time. Timing properties are derived from the document. We agree with possible discussions on the modelling of time but it appears that further works are required to get a better integration of a *more real time* approach. However, we think that the current model M8 is an abstraction of another automaton with real time features [2].

EVENT tic_tock
ANY
tm
WHERE
$grd1 : tm \in \mathbb{N}$
$grd2 : tm > time$
$grd3 : ran(at) \neq \varnothing \Rightarrow tm \leq min(ran(at))$
THEN
$act1 : time := tm$
END

The pilot uses the handle and the handle is taking some time to change the value of the sensors.

EVENT HPD1
REFINES HPD1
WHEN
$grd3 : \forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$
THEN
$act2 : handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$
$act3 : at := at \cup \{(index + 1) \mapsto (time + 160)\}$
$act4 : handleDown\_interval := time + 40000$
$act5 : handleUp\_interval := 0$
$act6 : index := index + 1$
END
EVENT HPU1
REFINES HPU1
WHEN
$grd3 : \forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$ THEN
$act2 : handle :\in 1 \mathinner{..} 3 \rightarrow \{UP\}$
$act3 : at := at \cup \{(index + 1) \mapsto (time + 160)\}$
$act4 : handleUp\_interval := time + 40000$
$act5 : handleDown\_interval := 0$
$act6 : index := index + 1$
END

The proof assistant is not efficient on this new refinement. However, now we can cover requirements with timing aspects.

3.9 M9: Adding Lights

The last refinement of our development introduces the interface of the pilot: *the lights*. These lights are modelled by a variable as $pilot\_interface\_light \in colorSet \rightarrow lightState$. Initially, p$ilot_interface_light$ is set to $\{Green \mapsto Off, Orange \mapsto Off, Red \mapsto Off\}$. The following events are informing the pilot by interpreting the results of the computing modules and they are extracted from the document:

- pilot_interface_Green_light_On: green light is on; when gears locked down is true.
- pilot_interface_Orange_light_On: orange light is on, when gears maneuvering is true.
- pilot_interface_Red_light_On: red light is on, when anomaly is detected (true).
- pilot_interface_Green_light_Off: green light is off, when gears locked down is false.
- pilot_interface_Orange_light_Off: orange light is off, when gears maneuvering is false.
- pilot_interface_Red_light_Off: red light is off, when anomaly is detected (false).

Model	Requirements	Total PO	Auto	Man
M1	R11, R11bis,R12, R12bis	10	10	0
M2	R11, R11bis,R12, R12bis	33	33	0
M3	R11, R11bis,R12, R12bis, R22, R21	44	44	0
M4	R11, R11bis,R12, R12bis, R22, R21	264	252	12
M5	R11, R11bis,R12, R12bis, R22, R21	19	19	0
M6	R11, R11bis,R12, R12bis, R22, R21	49	20	29
M7	R11, R11bis,R12, R12bis, R22, R21	1	0	1
M8	R11, R11bis,R12, R12bis, R22, R21	56	23	33
M9	R11, R11bis,R12, R12bis, R22, R21	9	3	6
Total	R11, R11bis,R12, R12bis, R22, R21	529	448	81

Figure 6: Table of requirements satisfied by models and proof statistics

4 Conclusion

Validation and verification are processed by using the ProB tool [16] and Proof Statistics. *Validation* refers to gaining confidence that the developed formal models are consistent with the requirements, which are expressed in the requirements document [6]. The landing system specification is developed and formally proved by the Event-B tool support prover. The developed formal models are also validated by the ProB tool through animation and model checker tool support of the abstract and successive refined models under some constraints of the tool. These constraints are the selection of parameters for testing the given model, and avoiding the failure of the tool during animation or model checking. However, we use this tool on abstract and all the refined models to check that the developed specification is deadlock free from an initial model to the concrete model. Due to features of ProB, we have used ProB for the models M1, M2 and M3.

The Table-Fig6 is expressing the proof statistics of the development in the RODIN tool. These statistics measure the size of the model, the proof obligations are generated and discharged by the Rodin platform, and those are interactively proved. The complete development of landing system results in 529(100%) proof obligations, in which 448(84,68%) are proved completely automatically by the RODIN tool. The remaining 81(15,31%) proof obligations are proved interactively using RODIN tool. In the models, many proof obligations are generated due to introduction of new functional and temporal behaviors. In order to guarantee the correctness of these functional and temporal behaviors, we have established various invariants in stepwise refinement. Most of the proofs are automatically discharged and the interactively discharged proof obligations are discharged by simple sequence of using automatic procedures of Rodin.

The current version of the development is the n^{th} version. The document describes a concrete system with sensors, mechanical parts and digital part. A first attempt by one of the authors was to propose a sequence of refined models too much close of this description. Then we try to have a global view of the system and to provide a very abstract initial model. In a second round of derivation of models, we got a wrong model, since we did not take into account the counter orders. Finally, the diagram of the Fig. 4 summarizes main steps of the system. From this model, we decide to make elements more concrete and we introduce sensors, computing modules. Timing requirements are added in the pre-last model M8 which is then equipped by lights in

the model M9. Our models are still too abstract and we have to get comments and feedbacks from the domain experts.

References

[1] J.-R. Abrial. *Modeling in Event-B: System and Software Engineering*. 2010.

[2] Rajeev Alur and David L. Dill. A theory of timed automata. *Theor. Comput. Sci.*, 126(2):183–235, 1994.

[3] R.J.R. Back. On correct refinement of programs. *Journal of Computer and System Sciences*, 23(1):49 – 68, 1981.

[4] Dines Bjorner. *Software Engineering: Vol 1 Abstraction and Modelling - Vol 2 Specification of Systems and Languages - Vol 3 Domains, Requirements, and Software Design*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2006. ISBN: 978-3-540-21149-5.

[5] Dines Bjørner and Martin C. Henson, editors. *Logics of Specification Languages*. EATCS Textbook in Computer Science. Springer, 2007.

[6] Frédéric Boniol and Virginie Wiels. Landing Gear System. http://www.irit.fr, 2013.

[7] R.W. Butler and George B. Finelli. The infeasibility of quantifying the reliability of life-critical real-time software. *Software Engineering, IEEE Transactions on*, 19(1):3–12, 1993.

[8] Dominique Cansell and Dominique Méry. *The event-B Modelling Method: Concepts and Case Studies*, pages 33–140. Springer, 2007. See [5].

[9] Dominique Cansell, Dominique Méry, and Joris Rehm. Time constraint patterns for event b development. In Jacques Julliand and Olga Kouchnarenko, editors, *B 2007: Formal Specification and Development in B*, volume 4355 of *Lecture Notes in Computer Science*, pages 140–154. Springer Berlin Heidelberg, 2006.

[10] ClearSy. Atelier B. http://www.clearsy.com.

[11] Federal Aviation Administration (FAA). *Aircraft Landing Gear System, Chapter 13 in Aviation Maintenance Technician Handbook - Airframe Vol-1*. U.S. Department of Transportation, Washington, D.C., 2012.

[12] Federal Aviation Administration (FAA). System Design and Analysis, Advisory Circular AC 25.1309-1A. http://www.faa.gov, June 1988.

[13] E. Gamma, R. Helm, R. Johnson, R. Vlissides, and P. Gamma. *Design Patterns : Elements of Reusable Object-Oriented Software design Patterns*. Addison-Wesley Professional Computing, 1994.

[14] Sally C. Johnson and Ricky W. Butler. *Formal Methods, Chapter 21 in The Avionics Handbook*. CRC Press, 2001. edited by Cary R. Spitzer.

[15] Gary T. Leavens, Jean-Raymond Abrial, Don Batory, Michael Butler, Alessandro Coglio, Kathi Fisler, Eric Hehner, Cliff Jones, Dale Miller, Simon Peyton-Jones, Murali Sitaraman, Douglas R. Smith, and Aaron Stump. Roadmap for enhanced languages and methods to aid verification. In *Fifth Intl. Conf. Generative Programming and Component Engineering (GPCE 2006)*, pages 221–235. ACM, October 2006.

[16] Michael Leuschel and Michael Butler. *ProB: A Model Checker for B*, pages 855–874. Lecture Notes in Computer Science. Springer, 2003.

[17] Dominique Méry and Neeraj Kumar Singh. Modelling an aircraft landing system in event-b. In *ABZ Case Study*, volume 433 of *Communications in Computer Information Science*. Springer, 2014.

[18] RODIN. Rigorous open development environment for complex systems. http://rodin-b-sharp.sourceforge.net, 2004. 2004-2013.

[19] Neeraj Kumar Singh. *Using Event-B for Critical Device Software Systems*. Springer-Verlag GmbH, 2013.

A Requirements

R11:*When the command line is working (normal mode), if the landing gear command button has been pushed DOWN and stays DOWN, then the gears will be locked down and the doors will be seen closed less than 15 seconds after the button has been pushed.*

R12: *When the command line is working (normal mode), if the landing gear command button has been pushed UP and stays UP, then the gears will be locked retracted and the doors will be seen closed less than 15 seconds after the button has been pushed. Note that a weaker version of these two requirements could be considered as well. This weaker version does not take into account quantitative time.*

(R11bis): *When the command line is working (normal mode), if the landing gear command button has been pushed DOWN and stays DOWN, then eventually the gears will be locked down and the doors will be seen closed.*

(R12bis): *When the command line is working (normal mode), if the landing gear command button has been pushed UP and stays UP, then eventually the gears will be locked retracted and the doors will be seen closed.*

(R21): *When the command line is working (normal mode), if the landing gear command button remains in the DOWN position, then retraction sequence is not observed.*

(R22): *When the command line is working (normal mode), if the landing gear command button remains in the UP position, then outgoing sequence is not observed.*

(R31): *When the command line is working (normal mode), the stimulation of the gears outgoing or the retraction electro-valves can only happen when the three doors are locked open.*

(R32): *When the command line is working (normal mode), the stimulation of the doors opening or closure electro-valves can only happen when the three gears are locked down or up.*

(R41): *When the command line is working (normal mode), opening and closure doors electro-valves are not stimulated simultaneously ; outgoing and retraction gears electro-valves are not stimulated simultaneously.*

(R42): *When the command line is working (normal mode), opening doors electro-valve and closure doors electro-valve are not stimulated simultaneously outgoing gears electro-valve and retraction gears electro-valve are not stimulated simultaneously*

(R51):
When the command line is working (normal mode), it is not possible to stimulate the maneuvering electro-valve (opening, closure, outgoing or retraction) without stimulating the general electro-valve.

(R61): *If one of the three doors is still seen locked in the closed position more than 0.5 second after stimulating the opening electro-valve, then the boolean output normal mode is set to false.*

(R62): *If one of the three doors is still seen locked in the open position more than 0.5 second after stimulating the closure electro-valve, then the boolean output normal mode is set to false.*

(R63): *If one of the three gears is still seen locked in the down position more than 0.5 second after stimulating the retraction electro-valve, then the boolean output normal mode is set to false.*

(R64): *If one of the three gears is still seen locked in the up position more than 0.5 second after stimulating the outgoing electro-valve, then the boolean output normal mode is set to false.*

(R71): *If one of the three doors is not seen locked in the open position more than 2 seconds after stimulating the opening electro-valve, then the boolean output normal mode is set to false.*

(R72): *If one of the three doors is not seen locked in the closed position more than 2 seconds after stimulating the closure electro-valve, then the boolean output normal mode is set to false.*

(R73): *If one of the three gears is not seen locked in the up position more than 10 seconds after stimulating the retraction electro-valve, then the boolean output normal mode is set to false.*

(R74): *If one of the three gears is not seen locked in the down position more than 10 seconds after stimulating the outgoing electro-valve, then the !boolean output normal mode is set to false.*

(R81): *When at least one computing module is working, if the landing gear command button has been DOWN for 15 seconds, and if the gears are not locked down after 15 seconds, then the red light landing gear system failure is on.*

(R82): *When at least one computing module is working, if the landing gear command button has been UP for 15 seconds, and if the gears are not locked retracted after 15 seconds, then the red light landing gear system failure is on.*

B Introduction of the Modeling Framework

We summarize the concepts of the EVENT B modeling language developed by Abrial [1] and indicate the links with the tool called RODIN [18]. The modeling process deals with various languages, as seen by considering the *triptych*[1] of Bjoerner [4]: $\mathcal{D}, \mathcal{S} \longrightarrow \mathcal{R}$. Here, the domain $\mathcal{D}$ deals with properties, axioms, sets, constants, functions, relations, and theories. The system model $\mathcal{S}$ expresses a model or a refinement-based chain of models of the system. Finally, $\mathcal{R}$ expresses requirements for the system to be designed. Considering the EVENT B modeling language, we notice that the language can express *safety* properties, which are either *invariants* or *theorems* in a machine corresponding to the system. Recall that two main structures are available in EVENT B:

- Contexts express static informations about the model.
- Machines express dynamic informations about the model, invariants, safety properties, and events.

A EVENT B model is defined either as a context or as a machine. The triptych of Bjoerner [4, 5] $\mathcal{D}, \mathcal{S} \longrightarrow \mathcal{R}$ is translated as follows: $\mathcal{C}, \mathcal{M} \longrightarrow \mathcal{R}$, where $\mathcal{C}$ is

[1] The term 'triptych' covers the three phases of software development: domain description, requirements prescription and software design.

a context, $\mathcal{M}$ is a machine and $\mathcal{R}$ are the requirements. The relation $\longrightarrow$ is defined to be a logical satisfaction relation with respect to an underlying logico-mathematical theory. The satisfaction relation is supported by the RODIN platform. A machine is organizing events modifying state variables and it uses static informations defined in a context. These basic structure mechanisms are extended by the refinement mechanism which provides a mechanism for relating an abstract model and a concrete model by adding new events or by adding new variables. This mechanism allows us to develop gradually EVENT B models and to validate each decision step using the proof tool. The refinement relationship should be expressed as follows: a model M is refined by a model P, when P is simulating M. The final concrete model is close to the behavior of real system that is executing events using real source code. We give details now on the definition of events, refinement and guidelines for developing complex system models.

B.1 Modeling Actions Over States

EVENT B [1] is based on the B notation. It extends the methodological scope of basic concepts to take into account the idea of *formal reactive models*. Briefly, a formal reactive model is characterized by a (finite) list x of *state variables* possibly modified by a (finite) list of *events*, where an invariant $I(x)$ states properties that must always be satisfied by the variables x and *maintained* by the activation of the events. In the following, we summarize the definitions and principles of formal models and explain how they can be managed by tools [18].

Generalized substitutions are borrowed from the B notation, which express changes in the value of state variables. An event has three main parts, namely a list of local parameters, a guard and a relation over values denotes *pre* values of variables and *post* values of variables. The most common event representation is (ANY t WHERE $G(t,x)$ THEN $x :|(R(x,x',t))$ END). The *before-after* predicate $BA(e)(x,x')$, associated with each event, describes the event as a logical predicate for expressing the relationship linking values of the state variables just before (x) and just after (x') the *execution* of event *e*. The form is semantically equivalent to $\exists\, t \cdot (G(t,x) \ \wedge \ R(x,x',t))$.

PROOF OBLIGATIONS

- (INV1) $Init(x) \ \Rightarrow \ I(x)$
- (INV2) $I(x) \ \wedge \ BA(e)(x,x') \ \Rightarrow \ I(x')$
- (FIS) $I(x) \ \wedge \ \mathsf{grd}(e)(x) \ \Rightarrow \exists y.BA(e)(x,y)$

Table-1 EVENT B proof obligations

Proof obligations (INV 1 and INV 2) are produced by the RODIN tool [18] from events to state that an invariant condition $I(x)$ is preserved. Their general form follows immediately from the definition of the before–after predicate $BA(e)(x,x')$ of each event e (see Table-1). Note that it follows from the two guarded forms of the events that this obligation is trivially discharged when the guard of the event is false. Whenever this is the case, the event is said to be *disabled*. The proof obligation FIS expresses the feasibility of the event e with respect to the invariant I. By proving feasibility, we achieve that $BA(e)(x,y)$ provides an after state whenever $grd(e)(x)$ holds. This means that the guard indeed represents the enabling condition of the event.

The intention of specifying a guard of an event is that the event may always occur when a given guard is true. There is, however, some interaction between guards and nondeterministic assignments, namely $x :|BA(e)(x,x')$. The predicate $BA(e)(x,x')$

of an action $x : |BA(e)(x, x')$ is not satisfiable or a set (S) is empty in an action predicate ($v :\in S$). Both cases show violations of the event feasibility proof obligation. We say that an assignment is feasible if there is an after-state satisfying the corresponding before-after predicate. For each event, its feasibility must be proved. Note, that for deterministic assignments the proof of feasibility is trivial. Also note, that feasibility of the initialization of a machine yields the existence of an initial state of the machine. It is not necessary to require an extra initialization.

B.2 Model Refinement

The refinement of a formal model allows us to enrich the model via a *step-by-step* approach and is the foundation of our correct-by-construction approach [15]. Refinement provides a way to strengthen invariants and to add details to a model. It is also used to transform an abstract model to a more concrete version by modifying the state description. This is done by extending the list of state variables (possibly suppressing some of them), by refining each abstract event to a set of possible concrete version, and by adding new events. The abstract (x) and concrete (y) state variables are linked by means of a *gluing invariant* $J(x, y)$. A number of proof obligations ensure that (1) each abstract event is correctly refined by its corresponding concrete version, (2) each new event refines $skip$, (3) no new event takes control for ever, and (4) relative deadlock freedom is preserved. Details of the formulation of these proofs follows.

We suppose that an abstract model AM with variables x and invariant $I(x)$ is refined by a concrete model CM with variables y and gluing invariant $J(x, y)$. Event e is in abstract model AM and event f is in concrete model CM. Event f refines event e. $BA(e)(x, x')$ and $BA(f)(y, y')$ are predicates of events e and f respectively, we have to prove the following statement, corresponding to proof obligation (1):

$$I(x) \ \wedge \ J(x, y) \ \wedge \ BA(f)(y, y') \ \Rightarrow \ \exists x' \cdot (BA(e)(x, x') \ \wedge \ J(x', y'))$$

The new events introduced in a refinement step can be viewed as hidden events not visible to the environment of a system and are thus outside the control of the environment. In EVENT B, requiring a new event to refine $skip$ means that the effect of the new event is not observable in the abstract model. Any number of executions of an internal action may occur in between each execution of a visible action. Now, proof obligation (2) states that $BA(f)(y, y')$ must refine $skip$ ($x' = x$), generating the following simple statement to prove (2):

$$I(x) \ \wedge \ J(x, y) \ \wedge \ BA(f)(y, y') \ \Rightarrow \ J(x, y')$$

In refining a model, an existing event can be refined by strengthening the guard and/or the before–after predicate (effectively reducing the degree of nondeterminism), or a new event can be added to refine the skip event. The feasibility condition is crucial to avoiding possible states that have no successor, such as division by zero. Furthermore, this refinement guarantees that the set of traces of the refined model contains (up to stuttering) the traces of the resulting model. The refinement of an event e by an event f means that the event f simulates the event e.

The EVENT B modeling language is supported by the RODIN platform [18] and has been introduced in publications [1], where the many case studies and discussions about the language itself and the foundations of the EVENT B approach. The language

of *generalized substitutions* is very rich, enabling the expression of any relation between states in a set-theoretical context. The expressive power of the language leads to a requirement for help in writing relational specifications, which is why we should provide guidelines for assisting the development of EVENT B models.

B.3 Time-Based Pattern in Event-B

The purpose of a design pattern [13] is to capture structures and to make decisions within a design that are common to similar modeling and analysis tasks. They can be re-applied when undertaking similar tasks in order to reduce the duplication of effort. The design pattern approach is the possibility to reuse solutions from earlier developments in the current project. This will lead to a correct refinement in the chain of models, without arising proof obligations. Since the correctness (i.e proof obligations are proved) of the pattern has been proved during its development, nothing is to be proved again when using this pattern.

The landing gear system is characterized by their functions, which can be expressed by analyzing the real-time patterns. Sequence of operations related to doors and gears, are performed under the real-time constraints. D. Cansell et. all [9] have introduced the time constraint pattern. In this case study, we use the same time pattern to solve the timing requirements of the landing system. This time pattern is fully based on timed automaton. The timed automaton is a finite state machine that is useful to model the components of real-time systems. In a model, the timed automata interacts with each other and defines a timed transition system. Besides ordinary action transitions that can represent input, output and internal actions. A timed transition system has time progress transitions. Such time progress transitions result in synchronous progress of all clock variables in the model. Here we apply the time pattern to model the sequential operations of doors and gears of the landing system in continuous progressive time constraint. In the model every events are controlled under time constraints, which means action of any event activates only when time constraint satisfies on specific time. The time progress is also an event, so there is no modification of the underlying B language. It is only a modeling technique instead of a specialized formal system. The timed variable is in $\mathbb{N}$ $(natural\ numbers)$ but the time constraint can be written in terms involving unknown constants or expressions between different times. Finally, the timed event observations can be constrained by other events which determine future activations.

B.4 Tools Environments for EVENT B

The EVENT B modeling language is supported by the Atelier B [10] environment and by the RODIN platform [18]. Both environments provide facilities for editing machines, refinements, contexts and projects, for generating proof obligations corresponding to a given property, for proving proof obligations in an automatic or/and interactive process and for animating models. The internal prover is shared by the two environments and there are hints generated by the prover interface for helping the interactive proofs. However, the refinement process of machines should be progressive when adding new elements to a given current model and the goal is to distribute the complexity of proofs through the proof-based refinement. These tools are based on logical and semantical concepts of EVENT B models (machines, contexts,refinement) and our methodology for modeling medical protocol or guidelines can be built from them.

C M1

An Event-B Specification of M1
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M1
SEES C0
VARIABLES

$button$
$phase$

INVARIANTS

inv1 : $button \in POSITIONS$
inv2 : $phase \in PHASES$
inv3 : $phase = movingup \Rightarrow button = UP$
inv4 : $phase = movingdown \Rightarrow button = DOWN$
inv5 : $button = UP \Rightarrow phase \notin \{movingdown, haltdown\}$
inv6 : $button = DOWN \Rightarrow phase \notin \{movingup, haltup\}$

EVENTS
Initialisation
begin

act1 : $button := DOWN$
act2 : $phase := haltdown$

end
Event *PressDOWN* $\widehat{=}$
when

grd1 : $button = UP$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$

end
Event *PressUP* $\widehat{=}$
when

grd1 : $button = DOWN$

then

act1 : $phase := movingup$
act2 : $button := UP$

end
Event *movingup* $\widehat{=}$
when

grd1 : $phase = movingup$

then

act1 : $phase := haltup$

end

Event *movingdown* $\widehat{=}$

when

grd1 : $phase = movingdown$

then

act1 : $phase := haltdown$

end

END

D M2

An Event-B Specification of M2
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M2
REFINES M1
SEES C0
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i

INVARIANTS

inv1 : $dstate \in DOORS \rightarrow SDOORS$
inv2 : $dstate^{-1}[\{OPEN\}] \neq \varnothing \Rightarrow dstate^{-1}[\{OPEN\}] = DOORS$
when one door is open, each door is open.
inv3 : $dstate^{-1}[\{CLOSED\}] \neq \varnothing \Rightarrow dstate^{-1}[\{CLOSED\}] = DOORS$
when a door is closed, t each door is closed
inv6 : $lstate \in DOORS \rightarrow SLOCKS$
inv7 : $dstate[DOORS] = \{OPEN\} \Rightarrow lstate[DOORS] = \{UNLOCKED\}$
inv12 : $p \in P$
inv13 : $l \in P$
inv14 : $i \in P$
inv15 : $l = E \wedge p = R \Rightarrow lstate[DOORS] = \{UNLOCKED\}$
inv16 : $l = R \wedge p = E \Rightarrow lstate[DOORS] = \{UNLOCKED\}$

EVENTS
Initialisation

extended

begin

act1 : $button := DOWN$
act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \rightarrow SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

end

Event *opening_doors_DOWN* $\widehat{=}$

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd5 : $lstate[DOORS] = \{UNLOCKED\}$

grd7 : $phase = movingdown$

grd8 : $p = R$

grd9 : $l = R$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \wedge b = OPEN\}$

act2 : $p := E$

end

Event *opening_doors_UP* $\widehat{=}$

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd4 : $lstate[DOORS] = \{UNLOCKED\}$

grd5 : $phase = movingup$

grd6 : $p = E$

grd7 : $l = E$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \wedge b = OPEN\}$

act2 : $p := R$

end

Event *closing_doors_UP* $\widehat{=}$

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$

grd3 : $f \in DOORS \rightarrow SDOORS$

grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$

grd5 : $phase = movingup$

grd6 : $p = R$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$

end

Event *locking_UP* $\widehat{=}$

refines *movingup*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery

end

Event *unlocking_DOWN* $\widehat{=}$

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$

end

Event *locking_DOWN* $\widehat{=}$

refines *movingdown*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$

end

Event *PD1* $\widehat{=}$
refines *PressDOWN*

when

grd1 : $button = UP$
grd2 : $phase = haltup$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
refines *PressUP*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
refines *PressUP*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$

then

act1 : $phase := movingup$

act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$

refines *movingup*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$

refines *PressUP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$

refines *PressUP*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$

refines *PressUP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$

refines *PressDOWN*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$

refines *movingdown*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$

refines *PressDOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$

grd5 : $l = E$
grd6 : $button = UP$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
refines *PressDOWN*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
refines *PressDOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

END

E M3

An Event-B Specification of M3
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M3
REFINES M2

SEES C0

VARIABLES

$dstate$

$lstate$

$phase$

$button$

p

l

i

$gstate$

INVARIANTS

M3_inv1 : $gstate \in GEARS \rightarrow SGEARS$

M3_inv3 : $\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED \wedge ran(gstate) \neq \{RETRACTED\} \Rightarrow ran(gstate) = \{EXTENDED\}$

gears can not be out or moving in this case.

M3_inv6 : $\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED \wedge ran(gstate) \neq \{EXTENDED\} \Rightarrow ran(gstate) = \{RETRACTED\}$

M3_inv7 : $ran(gstate) \neq \{RETRACTED\} \wedge ran(gstate) \neq \{EXTENDED\} \Rightarrow ran(dstate) = \{OPEN\}$

M3_inv11 : $ran(dstate) = \{CLOSED\} \Rightarrow ran(gstate) \cap \{RETRACTING, EXTENDING\} = \varnothing$

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate :\mid (dstate' \in DOORS \rightarrow SDOORS \wedge dstate' = \{a \mapsto b \mid a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b \mid a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate :\mid (gstate' \in GEARS \rightarrow SGEARS \wedge gstate' = \{a \mapsto b \mid a \in GEARS \wedge b = EXTENDED\})$

end

Event *opening_doors_DOWN* $\widehat{=}$

extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd5 : $lstate[DOORS] = \{UNLOCKED\}$

grd7 : $phase = movingdown$

grd8 : $p = R$

grd9 : $l = R$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := E$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $lstate[DOORS] = \{UNLOCKED\}$
grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$

end

Event *closing_doors_UP* $\widehat{=}$
refines *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
refines *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$

extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$

end

Event *locking_UP* $\widehat{=}$

extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$

added by D Mery

end

Event *unlocking_DOWN* $\widehat{=}$

extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$

end

Event *locking_DOWN* $\widehat{=}$

extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act3 : $phase := haltdown$
act4 : $l := E$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$

extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$

extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$

extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*
when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end
Event *PD5* $\widehat{=}$
extends *PD5*
when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end
Event *retracting_gears* $\widehat{=}$
when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$

end
Event *retraction* $\widehat{=}$
when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$

end
Event *extending_gears* $\widehat{=}$
when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \wedge b = EXTENDING\}$

end

Event *extension* $\widehat{=}$

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\}$

end

END

F M4

An Event-B Specification of M4
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M4
Reading Sensor
Computing Module
REFINES M3
SEES C1
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$

$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$
$anomaly\_func$
A_Switch_Out

INVARIANTS

inv3 : $handle \in 1 \mathinner{..} 3 \to POSITIONS$

inv4 : $analogical\_switch \in 1 \mathinner{..} 3 \to A\_Switch$

inv5 : $gear\_extended \in 1 \mathinner{..} 3 \to (GEARS \to BOOL)$

inv6 : $gear\_retracted \in 1 \mathinner{..} 3 \to (GEARS \to BOOL)$

inv7 : $gear\_shock\_absorber \in 1 \mathinner{..} 3 \to GEAR\_ABSORBER$

inv8 : $door\_closed \in 1 \mathinner{..} 3 \to (DOORS \to BOOL)$

inv9 : $door\_open \in 1 \mathinner{..} 3 \to (DOORS \to BOOL)$

inv10 : $circuit\_pressurized \in 1 \mathinner{..} 3 \to BOOL$

inv13 : $general\_EV \in BOOL$

inv14 : $close\_EV \in BOOL$

inv15 : $retract\_EV \in BOOL$

inv16 : $extend\_EV \in BOOL$

inv18 : $open\_EV \in BOOL$

inv19 : $gears\_locked\_down \in BOOL$

inv20 : $gears\_man \in BOOL$

inv21 : $anomaly \in BOOL$

inv22 : $general\_EV\_func \in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

inv23 : $close\_EV\_func \in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

inv24 : $retract\_EV\_func \in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

inv25 : $extend\_EV\_func \in (1 \mathinner{..} 3 \rightarrow POSITIONS) \times (1 \mathinner{..} 3 \rightarrow A\_Switch) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow BOOL) \rightarrow BOOL$

inv26 : $open\_EV\_func \in (1 \mathinner{..} 3 \rightarrow POSITIONS) \times (1 \mathinner{..} 3 \rightarrow A\_Switch) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow BOOL) \rightarrow BOOL$

inv27 : $gears\_locked\_down\_func \in (1 \mathinner{..} 3 \rightarrow POSITIONS) \times (1 \mathinner{..} 3 \rightarrow A\_Switch) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow BOOL) \rightarrow BOOL$

inv28 : $gears\_man\_func \in (1 \mathinner{..} 3 \rightarrow POSITIONS) \times (1 \mathinner{..} 3 \rightarrow A\_Switch) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow BOOL) \rightarrow BOOL$

inv29 : $anomaly\_func \in (1 \mathinner{..} 3 \rightarrow POSITIONS) \times (1 \mathinner{..} 3 \rightarrow A\_Switch) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow BOOL)) \times (1 \mathinner{..} 3 \rightarrow BOOL) \rightarrow BOOL$

inv30 : $A\_Switch\_Out \in BOOL$

M1_inv1 : $button \in POSITIONS$

M1_inv2 : $phase \in PHASES$

M1_inv3 : $phase = movingup \Rightarrow button = UP$

M1_inv4 : $phase = movingdown \Rightarrow button = DOWN$

M1_inv5 : $button = UP \Rightarrow phase \notin \{movingdown, haltdown\}$

M1_inv6 : $button = DOWN \Rightarrow phase \notin \{movingup, haltup\}$

M2_inv1 : $dstate \in DOORS \rightarrow SDOORS$

M2_inv2 : $dstate^{-1}[\{OPEN\}] \neq \varnothing \Rightarrow dstate^{-1}[\{OPEN\}] = DOORS$

when one door is open, each door is open.

M2_inv3 : $dstate^{-1}[\{CLOSED\}] \neq \varnothing \Rightarrow dstate^{-1}[\{CLOSED\}] = DOORS$

when a door is closed, t each door is closed

M2_inv6 : $lstate \in DOORS \rightarrow SLOCKS$

M2_inv7 : $dstate[DOORS] = \{OPEN\} \Rightarrow lstate[DOORS] = \{UNLOCKED\}$

M2_inv12 : $p \in P$

M2_inv13 : $l \in P$

M2_inv14 : $i \in P$

M2_inv15 : $l = E \wedge p = R \Rightarrow lstate[DOORS] = \{UNLOCKED\}$

M2_inv16 : $l = R \wedge p = E \Rightarrow lstate[DOORS] = \{UNLOCKED\}$

M3_inv1 : $gstate \in GEARS \rightarrow SGEARS$

M3_inv3 : $\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED \wedge ran(gstate) \neq \{RETRACTED\} \Rightarrow ran(gstate) = \{EXTENDED\}$

gears can not be out or moving in this case.

M3_inv6 : $\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED \wedge ran(gstate) \neq \{EXTENDED\} \Rightarrow ran(gstate) = \{RETRACTED\}$

M3_inv7 : $ran(gstate) \neq \{RETRACTED\} \land ran(gstate) \neq \{EXTENDED\} \Rightarrow ran(dstate) = \{OPEN\}$

M3_inv11 : $ran(dstate) = \{CLOSED\} \Rightarrow ran(gstate) \cap \{RETRACTING, EXTENDING\} = \varnothing$

EVENTS

Initialisation

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \to SDOORS \land dstate' = \{a \mapsto b | a \in DOORS \land b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate : |(gstate' \in GEARS \to SGEARS \land gstate' = \{a \mapsto b | a \in GEARS \land b = EXTENDED\})$

act14 : $handle :\in 1 \,..\, 3 \to \{DOWN\}$

act15 : $analogical\_switch :\in 1 \,..\, 3 \to \{open\}$

act16 : $gear\_extended :\in 1 \,..\, 3 \to (GEARS \to \{TRUE\})$

act17 : $gear\_retracted :\in 1 \,..\, 3 \to (GEARS \to \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \,..\, 3 \to \{ground\}$

act19 : $door\_closed :\in 1 \,..\, 3 \to (DOORS \to \{TRUE\})$

act20 : $door\_open :\in 1 \,..\, 3 \to (DOORS \to \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \,..\, 3 \to \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1 \,..\, 3 \to POSITIONS) \times (1 \,..\, 3 \to A\_Switch) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to GEAR\_ABSORBER) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1 \,..\, 3 \to POSITIONS) \times (1 \,..\, 3 \to A\_Switch) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to GEAR\_ABSORBER) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1 \,..\, 3 \to POSITIONS) \times (1 \,..\, 3 \to A\_Switch) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to (GEARS \to BOOL)) \times (1 \,..\, 3 \to GEAR\_ABSORBER) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to (DOORS \to BOOL)) \times (1 \,..\, 3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

end

Event *opening_doors_DOWN* $\widehat{=}$
refines *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd7 : $phase = movingdown$
grd8 : $p = R$
grd9 : $l = R$
grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \to \{FALSE\}\}$
grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \to \{FALSE\}\}$
grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \wedge b = OPEN\}$
act2 : $p := E$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *opening_doors_UP* $\widehat{=}$
refines *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $lstate[DOORS] = \{UNLOCKED\}$
grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \to \{FALSE\}\}$

grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

end

Event *closing_doors_UP* $\widehat{=}$
refines *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
refines *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
refines *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{TRUE\}\}$

grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$
refines *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery
act44 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

end

Event *unlocking_DOWN* $\widehat{=}$
refines *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
refines *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$

grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *PD1* $\widehat{=}$
refines *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
refines *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
refines *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
refines *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
refines *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
refines *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$

act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
refines *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
refines *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
refines *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
refines *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
refines *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
refines *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$

act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
refines *retracting_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$

end

Event *retraction* $\widehat{=}$
refines *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
refines *extending_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

end

Event *extension* $\widehat{=}$
refines *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$

end

Event *HPU1* $\widehat{=}$

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{UP\}$

end

Event *Analogical_switch_closed* $\widehat{=}$

any

in in port

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{closed\}$
act4 : $A\_Switch\_Out := TRUE$

end

Event *Analogical_switch_open* $\widehat{=}$

any

in in port

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act4 : $A\_Switch\_Out := FALSE$

end

Event *Circuit_pressurized* $\widehat{=}$

begin

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow BOOL$

end

Event *Computing_Module_1_2* $\widehat{=}$

begin

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

end

Event *Failure_Detection* $\widehat{=}$

begin

act1 : $anomaly := TRUE$

end

END

G M5

An Event-B Specification of M5
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M5

Hydraulic circuit output for Electro-valves.

REFINES M4

SEES C1
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$
$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$
$anomaly\_func$
$general\_EV\_Hout$
$close\_EV\_Hout$
$retract\_EV\_Hout$
$extend\_EV\_Hout$
$open\_EV\_Hout$
A_Switch_Out

INVARIANTS

inv1 : $general\_EV\_Hout \in \{0, Hin\}$
inv2 : $close\_EV\_Hout \in \{0, Hin\}$

inv3 : $retract\_EV\_Hout \in \{0, Hin\}$

inv4 : $extend\_EV\_Hout \in \{0, Hin\}$

inv5 : $open\_EV\_Hout \in \{0, Hin\}$

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \to SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate : |(gstate' \in GEARS \to SGEARS \wedge gstate' = \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\})$

act14 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$

act15 : $analogical\_switch :\in 1 \mathinner{..} 3 \to \{open\}$

act16 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

act17 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \mathinner{..} 3 \to \{ground\}$

act19 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

act20 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \to \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

act40 : $close\_EV\_Hout := 0$

act41 : $retract\_EV\_Hout := 0$

act42 : $extend\_EV\_Hout := 0$

act43 : $open\_EV\_Hout := 0$

act44 : $general\_EV\_Hout := 0$

end

Event *opening_doors_DOWN* $\widehat{=}$
extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd5 : $lstate[DOORS] = \{UNLOCKED\}$

grd7 : $phase = movingdown$

grd8 : $p = R$

grd9 : $l = R$

grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$

act2 : $p := E$

act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd4 : $lstate[DOORS] = \{UNLOCKED\}$

grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *closing_doors_UP* $\widehat{=}$
extends *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
extends *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$

grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$
extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery
act44 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *unlocking_DOWN* $\widehat{=}$
extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$

grd6 : $lstate[DOORS] = \{LOCKED\}$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$

grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$

grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
extends *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
extends *retracting_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$

end

Event *retraction* $\widehat{=}$
extends *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
extends *extending_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

end

Event *extension* $\widehat{=}$
extends *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$
extends *HPD1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$

end

Event *HPU1* $\widehat{=}$
extends *HPU1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{UP\}$

end

Event *Analogical_switch_closed* $\widehat{=}$
extends *Analogical_switch_closed*

any

in in port

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \to \{closed\}$
act4 : $A\_Switch\_Out := TRUE$

end

Event *Analogical_switch_open* $\widehat{=}$
extends *Analogical_switch_open*

any

in in port

where

grd1 : $in = general\_EV$

grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act4 : $A\_Switch\_Out := FALSE$

end

Event *Circuit_pressurized_OK* $\widehat{=}$
refines *Circuit_pressurized*

when

grd1 : $general\_EV\_Hout = Hin$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{TRUE\}$

end

Event *Circuit_pressurized_notOK* $\widehat{=}$
refines *Circuit_pressurized*

when

grd1 : $general\_EV\_Hout = 0$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

end

Event *Computing_Module_1_2* $\widehat{=}$
extends *Computing_Module_1_2*

begin

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

end

Event *Update_Hout* $\widehat{=}$

Assign the value of Hout

begin

act1 : $general\_EV\_Hout :\mid ((general\_EV = TRUE \wedge general\_EV\_Hout' = Hin) \vee (general\_EV = FALSE \wedge general\_EV\_Hout' = 0) \vee (A\_Switch\_Out = TRUE \wedge general\_EV\_Hout' = Hin) \vee (A\_Switch\_Out = FALSE \wedge general\_EV\_Hout' = 0))$

pass the current value of hydraulic input port (Hin) to hydraulic output port (Hout)

act2 : $close\_EV\_Hout :\mid ((close\_EV = TRUE \wedge close\_EV\_Hout' = Hin) \vee (close\_EV = FALSE \wedge close\_EV\_Hout' = 0))$

act3 : $open\_EV\_Hout :\mid ((open\_EV = TRUE \wedge open\_EV\_Hout' = Hin) \vee (open\_EV = FALSE \wedge open\_EV\_Hout' = 0))$

act4 : $extend\_EV\_Hout :\mid ((extend\_EV = TRUE \wedge extend\_EV\_Hout' = Hin) \vee (extend\_EV = FALSE \wedge extend\_EV\_Hout' = 0))$

act5 : $retract\_EV\_Hout :\mid ((retract\_EV = TRUE \wedge retract\_EV\_Hout' = Hin) \vee (retract\_EV = FALSE \wedge retract\_EV\_Hout' = 0))$

end

Event *Failure_Detection* $\widehat{=}$
extends *Failure_Detection*

begin

act1 : $anomaly := TRUE$

end

END

H M6

An Event-B Specification of M6
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M6

Integration of Cylinder bhavior according to the Electro-valves circuit
Strengthing guards of opening and closing doors and gears using cyliders sensors, and haudrlic pressure.

REFINES M5
SEES C1
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l

i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$
$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$
$anomaly\_func$
$general\_EV\_Hout$
$close\_EV\_Hout$
$retract\_EV\_Hout$
$extend\_EV\_Hout$
$open\_EV\_Hout$
$state$
$SDCylinder$ State of Door Cylinder
$SGCylinder$ State of Gear Cylinder
A_Switch_Out

INVARIANTS

inv1 : $SDCylinder \in DOORS \times \{DCYF, DCYR, DCYL\} \rightarrow S\_CYLINDER$
inv2 : $SGCylinder \in GEARS \times \{GCYF, GCYR, GCYL\} \rightarrow S\_CYLINDER$
inv17 : $state \in SPHASES$
inv4 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \wedge b = STOP\} \wedge dstate^{-1}[\{CLOSED\}] \neq \varnothing \Rightarrow dstate^{-1}[\{CLOSED\}] = DOORS$

inv5 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = STOP\} \wedge$
$(\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED) \wedge ran(gstate) \neq \{RETRACTED\} \wedge ran(gstate) \neq \{RETRACTING\} \wedge ran(gstate) \neq \{EXTENDING\} \Rightarrow ran(gstate) = \{EXTENDED\}$

inv6 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = STOP\} \wedge$
$(\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED) \wedge ran(gstate) \neq \{EXTENDED\} \wedge ran(gstate) \neq \{RETRACTING\} \wedge ran(gstate) \neq \{EXTENDING\} \Rightarrow ran(gstate) = \{RETRACTED\}$

inv7 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = MOVING\} \wedge$
$(\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED) \wedge ran(gstate) \neq \{RETRACTED\} \wedge ran(gstate) \neq \{EXTENDED\} \wedge ran(gstate) \neq \{EXTENDING\} \Rightarrow ran(gstate) = \{RETRACTING\}$

inv8 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = MOVING\} \wedge$
$(\forall door \cdot door \in DOORS \wedge dstate(door) = CLOSED) \wedge ran(gstate) \neq \{RETRACTED\} \wedge ran(gstate) \neq \{EXTENDED\} \wedge ran(gstate) \neq \{RETRACTING\} \Rightarrow ran(gstate) = \{EXTENDING\}$

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate :| (dstate' \in DOORS \rightarrow SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate :| (gstate' \in GEARS \rightarrow SGEARS \wedge gstate' = \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\})$

act14 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$

act15 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act16 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$

act17 : $gear\_retracted :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \mathinner{..} 3 \rightarrow \{ground\}$

act19 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

act20 : $door\_open :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1\,..\,3 \to POSITIONS) \times (1\,..\,3 \to A\_Switch) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to (GEARS \to BOOL)) \times (1\,..\,3 \to GEAR\_ABSORBER) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to (DOORS \to BOOL)) \times (1\,..\,3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

act40 : $close\_EV\_Hout := 0$

act41 : $retract\_EV\_Hout := 0$

act42 : $extend\_EV\_Hout := 0$

act43 : $open\_EV\_Hout := 0$

act44 : $general\_EV\_Hout := 0$

act45 : $SDCylinder :\in DOORS \times \{DCYF, DCYR, DCYL\} \to \{STOP\}$

act46 : $SGCylinder :\in GEARS \times \{GCYF, GCYR, GCYL\} \to \{STOP\}$

act26 : $state := computing$

end

Event *opening_doors_DOWN* $\widehat{=}$
extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd5 : $lstate[DOORS] = \{UNLOCKED\}$

grd7 : $phase = movingdown$

grd8 : $p = R$

grd9 : $l = R$

grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := E$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $lstate[DOORS] = \{UNLOCKED\}$
grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *closing_doors_UP* $\widehat{=}$
extends *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
extends *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$
extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd8 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \wedge b = STOP\}$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$

added by D Mery

act44 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

end

Event *unlocking_DOWN* $\widehat{=}$
extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd6 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$

grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$

grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$

grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$

grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
extends *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
extends *retracting_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd5 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$

end

Event *retraction* $\widehat{=}$
extends *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$

grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
extends *extending_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd4 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

end

Event *extension* $\widehat{=}$
extends *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$
extends *HPD1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$

end

Event *HPU1* $\widehat{=}$

extends *HPU1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{UP\}$

end

Event *Analogical_switch_closed* $\widehat{=}$
extends *Analogical_switch_closed*

any

in in port

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{closed\}$
act4 : $A\_Switch\_Out := TRUE$

end

Event *Analogical_switch_open* $\widehat{=}$
extends *Analogical_switch_open*

any

in in port

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$
act4 : $A\_Switch\_Out := FALSE$

end

Event *Circuit_pressurized_OK* $\widehat{=}$
extends *Circuit_pressurized_OK*

when

grd1 : $general\_EV\_Hout = Hin$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{TRUE\}$

end

Event *Circuit_pressurized_notOK* $\widehat{=}$
extends *Circuit_pressurized_notOK*

when

grd1 : $general\_EV\_Hout = 0$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

end

Event *Computing_Module_1_2* $\widehat{=}$
extends *Computing_Module_1_2*

when

grd1 : $state = computing$

then

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act9 : $state := electroValve$

end

Event *Update_Hout* $\widehat{=}$

Assign the value of Hout

extends *Update_Hout*

when

grd1 : $state = electroValve$

then

act1 : $general\_EV\_Hout :| ((general\_EV = TRUE \land general\_EV\_Hout' = Hin) \lor (general\_EV = FALSE \land general\_EV\_Hout' = 0) \lor (A\_Switch\_Out = TRUE \land general\_EV\_Hout' = Hin) \lor (A\_Switch\_Out = FALSE \land general\_EV\_Hout' = 0))$

pass the current value of hydraulic input port (Hin) to hydraulic output port (Hout)

act2 : $close\_EV\_Hout :| ((close\_EV = TRUE \land close\_EV\_Hout' = Hin) \lor (close\_EV = FALSE \land close\_EV\_Hout' = 0))$

act3 : $open\_EV\_Hout :| ((open\_EV = TRUE \land open\_EV\_Hout' = Hin) \lor (open\_EV = FALSE \land open\_EV\_Hout' = 0))$

act4 : $extend\_EV\_Hout :| ((extend\_EV = TRUE \land extend\_EV\_Hout' = Hin) \lor (extend\_EV = FALSE \land extend\_EV\_Hout' = 0))$

act5 : $retract\_EV\_Hout :| ((retract\_EV = TRUE \land retract\_EV\_Hout' = Hin) \lor (retract\_EV = FALSE \land retract\_EV\_Hout' = 0))$

act6 : $state := cylinder$

end

Event *CylinderMovingOrStop* $\widehat{=}$

Cylinder Moving or Stop according to the output of hydraulic circuit

when

grd1 : $state = cylinder$

then

act1 : $SGCylinder : |((SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge extend\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge extend\_EV\_Hout = 0) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge retract\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge retract\_EV\_Hout = 0))$

act2 : $SDCylinder : |((SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge open\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge open\_EV\_Hout = 0) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge close\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge close\_EV\_Hout = 0))$

act3 : $state := computing$

end

Event *Failure_Detection* $\widehat{=}$

extends *Failure_Detection*

begin

act1 : $anomaly := TRUE$

end

END

I M7

An Event-B Specification of M7
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M7

Failure Modelling
Generic Monitoring failure
Failure detection is added for doors and gears motion monitioring (Page 17)
Analogical Switch Monitioring failure (Page 16)
Pressure Sensor Monitioring faliure (Page 16)
But timing requirements can be added only in last.

REFINES M6
SEES C1
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$
$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$
$anomaly\_func$
$general\_EV\_Hout$
$close\_EV\_Hout$
$retract\_EV\_Hout$
$extend\_EV\_Hout$
$open\_EV\_Hout$
A_Switch_Out
$SDCylinder$ State of Door Cylinder
$SGCylinder$ State of Gear Cylinder
$state$

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \to SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate : |(gstate' \in GEARS \to SGEARS \wedge gstate' = \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\})$

act14 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$

act15 : $analogical\_switch :\in 1 \mathinner{..} 3 \to \{open\}$

act16 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

act17 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \mathinner{..} 3 \to \{ground\}$

act19 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

act20 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \to \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

act40 : $close\_EV\_Hout := 0$

act41 : $retract\_EV\_Hout := 0$

act42 : $extend\_EV\_Hout := 0$

act43 : $open\_EV\_Hout := 0$

act44 : $general\_EV\_Hout := 0$

act45 : $SDCylinder :\in DOORS \times \{DCYF, DCYR, DCYL\} \to \{STOP\}$

act46 : $SGCylinder :\in GEARS \times \{GCYF, GCYR, GCYL\} \to \{STOP\}$

act26 : $state := computing$

end

Event *opening_doors_DOWN* $\widehat{=}$
extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd5 : $lstate[DOORS] = \{UNLOCKED\}$

grd7 : $phase = movingdown$

grd8 : $p = R$

grd9 : $l = R$

grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$

grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$

grd13 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$

act2 : $p := E$

act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$

grd4 : $lstate[DOORS] = \{UNLOCKED\}$

grd5 : $phase = movingup$

grd6 : $p = E$

grd7 : $l = E$

grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$
grd11 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *closing_doors_UP* $\widehat{=}$
extends *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
extends *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$

grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$
extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd8 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$
grd12 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery
act44 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *unlocking_DOWN* $\widehat{=}$
extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd6 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$
grd10 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$

extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
extends *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
extends *retracting_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd5 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$

end

Event *retraction* $\widehat{=}$
extends *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
extends *extending_gears*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd4 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$

end

Event *extension* $\widehat{=}$
extends *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$
extends *HPD1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$

end

Event *HPU1* $\widehat{=}$
extends *HPU1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{UP\}$

end

Event *Analogical_switch_closed* $\widehat{=}$
extends *Analogical_switch_closed*

any

in in port

where

grd1 : $in = general\_EV$

grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{closed\}$

act4 : $A\_Switch\_Out := TRUE$

end

Event *Analogical_switch_open* $\widehat{=}$
extends *Analogical_switch_open*

any

in in port

where

grd1 : $in = general\_EV$

grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act4 : $A\_Switch\_Out := FALSE$

end

Event *Circuit_pressurized_OK* $\widehat{=}$
extends *Circuit_pressurized_OK*

when

grd1 : $general\_EV\_Hout = Hin$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{TRUE\}$

end

Event *Circuit_pressurized_notOK* $\widehat{=}$
extends *Circuit_pressurized_notOK*

when

grd1 : $general\_EV\_Hout = 0$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

end

Event *Computing_Module_1_2* $\widehat{=}$
extends *Computing_Module_1_2*

when

grd1 : $state = computing$

then

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$

act9 : $state := electroValve$

end

Event *Update_Hout* $\widehat{=}$

Assign the value of Hout

extends *Update_Hout*

when

grd1 : $state = electroValve$

then

act1 : $general\_EV\_Hout :\mid ((general\_EV = TRUE \land general\_EV\_Hout' = Hin) \lor (general\_EV = FALSE \land general\_EV\_Hout' = 0) \lor (A\_Switch\_Out = TRUE \land general\_EV\_Hout' = Hin) \lor (A\_Switch\_Out = FALSE \land general\_EV\_Hout' = 0))$

pass the current value of hydraulic input port (Hin) to hydraulic output port (Hout)

act2 : $close\_EV\_Hout :\mid ((close\_EV = TRUE \land close\_EV\_Hout' = Hin) \lor (close\_EV = FALSE \land close\_EV\_Hout' = 0))$

act3 : $open\_EV\_Hout :\mid ((open\_EV = TRUE \land open\_EV\_Hout' = Hin) \lor (open\_EV = FALSE \land open\_EV\_Hout' = 0))$

act4 : $extend\_EV\_Hout :\mid ((extend\_EV = TRUE \land extend\_EV\_Hout' = Hin) \lor (extend\_EV = FALSE \land extend\_EV\_Hout' = 0))$

act5 : $retract\_EV\_Hout :\mid ((retract\_EV = TRUE \land retract\_EV\_Hout' = Hin) \lor (retract\_EV = FALSE \land retract\_EV\_Hout' = 0))$

act6 : $state := cylinder$

end

Event *CylinderMovingOrStop* $\widehat{=}$

Cylinder Moving or Stop according to the output of hydraulic circuit

extends *CylinderMovingOrStop*

when

grd1 : $state = cylinder$

then

act1 : $SGCylinder : |((SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \land b = MOVING\} \land extend\_EV\_Hout = Hin) \lor$
$(SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \land b = STOP\} \land extend\_EV\_Hout = 0) \lor$
$(SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \land b = MOVING\} \land retract\_EV\_Hout = Hin) \lor$
$(SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \land b = STOP\} \land retract\_EV\_Hout = 0))$

act2 : $SDCylinder : |((SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \land b = MOVING\} \land open\_EV\_Hout = Hin) \lor$
$(SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \land b = STOP\} \land open\_EV\_Hout = 0) \lor$
$(SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \land b = MOVING\} \land close\_EV\_Hout = Hin) \lor$
$(SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \land b = STOP\} \land close\_EV\_Hout = 0))$

act3 : $state := computing$

end

Event *Failure_Detection_Generic_Monitoring* $\widehat{=}$
extends *Failure_Detection*

when

grd1 : $(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(handle(x) \neq handle(y) \land handle(y) \neq handle(z) \land handle(x) \neq handle(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(analogical\_switch(x) \neq analogical\_switch(y) \land analogical\_switch(y) \neq analogical\_switch(z) \land analogical\_switch(x) \neq analogical\_switch(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(gear\_extended(x) \neq gear\_extended(y) \land gear\_extended(y) \neq gear\_extended(z) \land gear\_extended(x) \neq gear\_extended(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(gear\_retracted(x) \neq gear\_retracted(y) \land gear\_retracted(y) \neq gear\_retracted(z) \land gear\_retracted(x) \neq gear\_retracted(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(gear\_shock\_absorber(x) \neq gear\_shock\_absorber(y) \land gear\_shock\_absorber(y) \neq gear\_shock\_absorber(z) \land gear\_shock\_absorber(x) \neq gear\_shock\_absorber(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(door\_open(x) \neq door\_open(y) \land door\_open(y) \neq door\_open(z) \land door\_open(x) \neq door\_open(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(door\_closed(x) \neq door\_closed(y) \land door\_closed(y) \neq door\_closed(z) \land door\_closed(x) \neq door\_closed(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow$
$(circuit\_pressurized(x) \neq circuit\_pressurized(y) \land circuit\_pressurized(y) \neq circuit\_pressurized(z) \land circuit\_pressurized(x) \neq circuit\_pressurized(z)))$

Generic Monitoring uisng all sensors

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Analogical_Switch* $\widehat{=}$
extends *Failure_Detection*

when

grd1 : $analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = open\}$
$\lor$
$analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = closed\}$

Gears motion monitoring without considering time

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Pressure_Sensor* $\widehat{=}$

extends *Failure_Detection*

when

grd1 : $circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = TRUE\}$
$\lor$
$circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = FALSE\}$
Circuit pressurized motion monitoring without considering time

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Doors* $\widehat{=}$
extends *Failure_Detection*

when

grd1 : $door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{TRUE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{FALSE\}\}$
$\lor$
$door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \rightarrow \{TRUE\}\}$
Doors motion monitoring without considering time

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Gears* $\widehat{=}$
extends *Failure_Detection*

when

grd1 : $gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
$\lor$
$gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{TRUE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{TRUE\}\}$
Gears motion monitoring without considering time

then

act1 : $anomaly := TRUE$

end

END

J M8

An Event-B Specification of M8
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M8
Timing Requirements.

REFINES M7
SEES C1
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$
$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$
$anomaly\_func$
$general\_EV\_Hout$
$close\_EV\_Hout$
$retract\_EV\_Hout$
$extend\_EV\_Hout$
$open\_EV\_Hout$
$SDCylinder$ State of Door Cylinder
$SGCylinder$ State of Gear Cylinder
A_Switch_Out State of Gear Cylinder

$state$

$time$ current time

at a future event activation set.

$index$ To take a function to index different sets for event activation set

$handleUp\_interval$ To keep an update time duration after handle up

$handleDown\_interval$ To keep an update time duration after handle down

INVARIANTS

inv1 : $time \in \mathbb{N}$
current updating time

inv2 : $at \subseteq \mathbb{N} \times \mathbb{N}$
a set of times for activating event

inv3 : $ran(at) \neq \varnothing \Rightarrow time \leq min(ran(at))$
if activation is a non empty set then the current time will be less than or equal to the minimum of activation set.

inv4 : $index \in \mathbb{N}$
an index for event activation set to store multiple identical values

inv5 : $handleUp\_interval \in \mathbb{N}$
time interval after handle up

inv6 : $handleDown\_interval \in \mathbb{N}$
time interval after handle down

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \rightarrow SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$
missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate : |(gstate' \in GEARS \rightarrow SGEARS \wedge gstate' = \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\})$

act14 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$

act15 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act16 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$

act17 : $gear\_retracted :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \mathinner{..} 3 \rightarrow \{ground\}$

act19 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

act20 : $door\_open :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

act40 : $close\_EV\_Hout := 0$

act41 : $retract\_EV\_Hout := 0$

act42 : $extend\_EV\_Hout := 0$

act43 : $open\_EV\_Hout := 0$

act44 : $general\_EV\_Hout := 0$

act45 : $SDCylinder :\in DOORS \times \{DCYF, DCYR, DCYL\} \to \{STOP\}$

act46 : $SGCylinder :\in GEARS \times \{GCYF, GCYR, GCYL\} \to \{STOP\}$

act26 : $state := computing$

act47 : $at := \varnothing$

act48 : $time := 0$

act49 : $index := 0$

act50 : $handleUp\_interval := 0$

act51 : $handleDown\_interval := 0$

end

Event *opening_doors_DOWN* $\widehat{=}$
extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd7 : $phase = movingdown$
grd8 : $p = R$
grd9 : $l = R$
grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$
grd13 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := E$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act4 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door open to gear extension
act5 : $index := index + 1$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $lstate[DOORS] = \{UNLOCKED\}$
grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$
grd11 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act4 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door open to gear retraction
act5 : $index := index + 1$

end

Event *closing_doors_UP* $\widehat{=}$
extends *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$

grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
extends *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \to SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$
extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$

grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd8 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$
grd12 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery
act44 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act5 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door closed to gear extension/retraction
act6 : $index := index + 1$

end

Event *unlocking_DOWN* $\widehat{=}$
extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd6 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$
grd10 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act6 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door closed to extension/retraction
act7 : $index := index + 1$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$

act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
extends *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$

act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
extends *retracting_gears*

any

ind

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in GEARS \rightarrow \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in GEARS \rightarrow \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd5 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = MOVING\}$
grd10 : $at \neq \varnothing$
grd11 : $time \in ran(at)$
grd12 : $ind \in dom(at) \wedge ind \mapsto time \in at$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \wedge b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b = flight\}$
act4 : $at := at \setminus \{ind \mapsto time\}$

end

Event *retraction* $\widehat{=}$
extends *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in GEARS \rightarrow \{FALSE\}\}$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in GEARS \rightarrow \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \wedge b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \wedge b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
extends *extending_gears*

any

ind

where

grd1 : $dstate[DOORS] = \{OPEN\}$

grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd4 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$
grd9 : $at \neq \varnothing$
grd10 : $time \in ran(at)$
grd11 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$
act3 : $at := at \setminus \{ind \mapsto time\}$

end

Event *extension* $\widehat{=}$
extends *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$
extends *HPD1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$
act3 : $at := at \cup \{(index + 1) \mapsto (time + 160)\}$
analogical switch is seen open 160ms after handle position has changed
act4 : $handleDown\_interval := time + 40000$
add a new time interval (current time + handle not changed interval) in the event activation set
act5 : $handleUp\_interval := 0$
update the handle up interval as 0
act6 : $index := index + 1$
update the current index value

end

Event *HPU1* $\widehat{=}$

extends *HPU1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{UP\}$

act3 : $at := at \cup \{(index + 1) \mapsto (time + 160)\}$

analogical switch is seen open 160ms after handle position has changed

act4 : $handleUp\_interval := time + 40000$

add a new time interval (current time + handle not changed interval) in the event activation set

act5 : $handleDown\_interval := 0$

update the handle down interval as 0

act6 : $index := index + 1$

update the current index value

end

Event *Analogical_switch_closed* $\widehat{=}$
extends *Analogical_switch_closed*

any

in in port
ind

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$
grd3 : $at \neq \varnothing$
grd4 : $time \in ran(at)$
grd5 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{closed\}$
act4 : $A\_Switch\_Out := TRUE$
act5 : $at := (at \cup \{(index + 1) \mapsto (time + 1200)\}) \setminus \{ind \mapsto time\}$

from closed to open 1.2 sec.

act6 : $index := index + 1$

end

Event *Analogical_switch_open* $\widehat{=}$
extends *Analogical_switch_open*

any

in in port
ind

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$
grd3 : $at \neq \varnothing$
grd4 : $time \in ran(at)$
grd5 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$
act4 : $A\_Switch\_Out := FALSE$

act5 : $at := (at \cup \{(index + 1) \mapsto (time + 800)\}) \setminus \{ind \mapsto time\}$
from open to closed .8 sec.
act6 : $index := index + 1$

end

Event *Circuit_pressurized_OK* $\widehat{=}$
extends *Circuit_pressurized_OK*

when

grd1 : $general\_EV\_Hout = Hin$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{TRUE\}$

end

Event *Circuit_pressurized_notOK* $\widehat{=}$
extends *Circuit_pressurized_notOK*

when

grd1 : $general\_EV\_Hout = 0$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

end

Event *Computing_Module_1_2* $\widehat{=}$
extends *Computing_Module_1_2*

when

grd1 : $state = computing$

then

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act9 : $state := electroValve$

end

Event *Update_Hout* $\widehat{=}$

Assign the value of Hout

extends *Update_Hout*

when

grd1 : $state = electroValve$

then

act1 : $general\_EV\_Hout :\mid ((general\_EV = TRUE \land general\_EV\_Hout' = Hin) \lor (general\_EV = FALSE \land general\_EV\_Hout' = 0) \lor (A\_Switch\_Out = TRUE \land general\_EV\_Hout' = Hin) \lor (A\_Switch\_Out = FALSE \land general\_EV\_Hout' = 0))$

pass the current value of hydraulic input port (Hin) to hydraulic output port (Hout)

act2 : $close\_EV\_Hout :\mid ((close\_EV = TRUE \land close\_EV\_Hout' = Hin) \lor (close\_EV = FALSE \land close\_EV\_Hout' = 0))$

act3 : $open\_EV\_Hout :\mid ((open\_EV = TRUE \land open\_EV\_Hout' = Hin) \lor (open\_EV = FALSE \land open\_EV\_Hout' = 0))$

act4 : $extend\_EV\_Hout :\mid ((extend\_EV = TRUE \land extend\_EV\_Hout' = Hin) \lor (extend\_EV = FALSE \land extend\_EV\_Hout' = 0))$

act5 : $retract\_EV\_Hout :\mid ((retract\_EV = TRUE \land retract\_EV\_Hout' = Hin) \lor (retract\_EV = FALSE \land retract\_EV\_Hout' = 0))$

act6 : $state := cylinder$

act7 : $at := at \cup$
$\{(index + 1) \mapsto (time + 2000)\} \cup$
$\{(index + 2) \mapsto (time + 10000)\} \cup$
$\{(index + 3) \mapsto (time + 500)\} \cup$
$\{(index + 4) \mapsto (time + 2000)\} \cup$
$\{(index + 5) \mapsto (time + 500)\} \cup$
$\{(index + 6) \mapsto (time + 2000)\} \cup$
$\{(index + 7) \mapsto (time + 500)\} \cup$
$\{(index + 8) \mapsto (time + 10000)\} \cup$
$\{(index + 9) \mapsto (time + 500)\} \cup$
$\{(index + 10) \mapsto (time + 10000)\}$

general EV 2 (time is given in comments in sec. while in model these are in ms.)

general EV 10
openning EV 0.5
openning EV 2
closure EV 0.5
closure EV 2
retraction EV 0.5
retraction EV 10
extension 0.5
extension 10

act8 : $index := index + 10$

end

Event *CylinderMovingOrStop* $\widehat{=}$

Cylinder Moving or Stop according to the output of hydraulic circuit

extends *CylinderMovingOrStop*

when

grd1 : $state = cylinder$

then

act1 : $SGCylinder : |((SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge extend\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge extend\_EV\_Hout = 0) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge retract\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge retract\_EV\_Hout = 0))$

act2 : $SDCylinder : |((SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge open\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge open\_EV\_Hout = 0) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge close\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge close\_EV\_Hout = 0))$

act3 : $state := computing$

end

Event *Failure_Detection_Generic_Monitoring* $\widehat{=}$
extends *Failure_Detection_Generic_Monitoring*

when

grd1 : $(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (handle(x) \neq handle(y) \land handle(y) \neq handle(z) \land handle(x) \neq handle(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (analogical\_switch(x) \neq analogical\_switch(y) \land analogical\_switch(y) \neq analogical\_switch(z) \land analogical\_switch(x) \neq analogical\_switch(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_extended(x) \neq gear\_extended(y) \land gear\_extended(y) \neq gear\_extended(z) \land gear\_extended(x) \neq gear\_extended(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_retracted(x) \neq gear\_retracted(y) \land gear\_retracted(y) \neq gear\_retracted(z) \land gear\_retracted(x) \neq gear\_retracted(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_shock\_absorber(x) \neq gear\_shock\_absorber(y) \land gear\_shock\_absorber(y) \neq gear\_shock\_absorber(z) \land gear\_shock\_absorber(x) \neq gear\_shock\_absorber(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (door\_open(x) \neq door\_open(y) \land door\_open(y) \neq door\_open(z) \land door\_open(x) \neq door\_open(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (door\_closed(x) \neq door\_closed(y) \land door\_closed(y) \neq door\_closed(z) \land door\_closed(x) \neq door\_closed(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (circuit\_pressurized(x) \neq circuit\_pressurized(y) \land circuit\_pressurized(y) \neq circuit\_pressurized(z) \land circuit\_pressurized(x) \neq circuit\_pressurized(z)))$

Generic Monitoring uisng all sensors

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Analogical_Switch* $\widehat{=}$
extends *Failure_Detection_Analogical_Switch*

any

ind

where

grd1 : $analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = open\}$
$\lor$
$analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = closed\}$

Gears motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *check_handle_delay* $\widehat{=}$

This event is used to set 280ms in the set "at" for event activation to detect anomaly and detect that hanlde is not change from last 40 sec.

when

grd1 : $time = handleUp\_interval \lor time = handleDown\_interval$

current time is either equal to handle up interval or equal to the handle down interval

then

act1 : $at := at \cup \{(index + 1) \mapsto (time + 280)\}$

To add a new interval to the event activation set

act3 : $index := index + 1$

update the current index value

end

Event *Failure_Detection_Pressure_Sensor* $\widehat{=}$
extends *Failure_Detection_Pressure_Sensor*

any

ind

where

grd1 : $circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = TRUE\} \lor circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = FALSE\}$

Circuit pressurized motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *Failure_Detection_Doors* $\widehat{=}$
extends *Failure_Detection_Doors*

any

ind

where

grd1 : $door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
$\lor$
$door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
Doors motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *Failure_Detection_Gears* $\widehat{=}$
extends *Failure_Detection_Gears*

any

ind

where

grd1 : $gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
$\lor$
$gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
Gears motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *tic_tock* $\widehat{=}$
time progression

any

tm

where

grd1 : $tm \in \mathbb{N}$

grd2 : $tm > time$
to take a new value of time in the future

grd3 : $ran(at) \neq \varnothing \Rightarrow tm \leq min(ran(at))$

then

act1 : $time := tm$
assign a new value of time to the current time

end
END

K M9

An Event-B Specification of M9
Creation Date: 27Jan2014 @ 10:44:59 AM

MACHINE M9
Pilot interface light implementation
REFINES M8
SEES C1, C2
VARIABLES

$dstate$
$lstate$
$phase$
$button$
p
l
i
$gstate$
$handle$
$analogical\_switch$
$gear\_extended$
$gear\_retracted$
$gear\_shock\_absorber$
$door\_closed$
$door\_open$
$circuit\_pressurized$
$general\_EV$
$close\_EV$
$retract\_EV$
$extend\_EV$
$open\_EV$
$gears\_locked\_down$
$gears\_man$
$anomaly$
$general\_EV\_func$
$close\_EV\_func$
$retract\_EV\_func$
$extend\_EV\_func$
$open\_EV\_func$
$gears\_locked\_down\_func$
$gears\_man\_func$

$anomaly\_func$

$general\_EV\_Hout$

$close\_EV\_Hout$

$retract\_EV\_Hout$

$extend\_EV\_Hout$

$open\_EV\_Hout$

$SDCylinder$ State of Door Cylinder

$SGCylinder$ State of Gear Cylinder

A_Switch_Out State of Gear Cylinder

$state$

$time$ current time

at a future event activation set.

$index$ To take a function to index different sets for event activation set

$handleUp\_interval$ To keep an update time duration after handle up

$handleDown\_interval$ To keep an update time duration after handle down

$pilot\_interface\_light$ current pilot interface light

INVARIANTS

inv1 : $pilot\_interface\_light \in colorSet \rightarrow lightState$

a function to map from colorset to light state

EVENTS

Initialisation

extended

begin

act1 : $button := DOWN$

act2 : $phase := haltdown$

act3 : $dstate : |(dstate' \in DOORS \rightarrow SDOORS \wedge dstate' = \{a \mapsto b | a \in DOORS \wedge b = CLOSED\})$

missing elements of the invariant

act4 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$

act5 : $p := R$

act6 : $l := R$

act7 : $i := R$

act8 : $gstate : |(gstate' \in GEARS \rightarrow SGEARS \wedge gstate' = \{a \mapsto b | a \in GEARS \wedge b = EXTENDED\})$

act14 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{DOWN\}$

act15 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$

act16 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$

act17 : $gear\_retracted :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$

act18 : $gear\_shock\_absorber :\in 1 \mathinner{..} 3 \rightarrow \{ground\}$

act19 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$

act20 : $door\_open :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

act21 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

act22 : $general\_EV := FALSE$

act23 : $close\_EV := TRUE$

act24 : $retract\_EV := FALSE$

act25 : $extend\_EV := TRUE$

act27 : $open\_EV := FALSE$

act28 : $gears\_locked\_down := TRUE$

act29 : $gears\_man := FALSE$

act30 : $anomaly := FALSE$

act31 : $general\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act32 : $close\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act33 : $retract\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act34 : $extend\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act35 : $open\_EV\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act36 : $gears\_locked\_down\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act37 : $gears\_man\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act38 : $anomaly\_func :\in (1 \mathinner{..} 3 \to POSITIONS) \times (1 \mathinner{..} 3 \to A\_Switch) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to (GEARS \to BOOL)) \times (1 \mathinner{..} 3 \to GEAR\_ABSORBER) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to (DOORS \to BOOL)) \times (1 \mathinner{..} 3 \to BOOL) \to BOOL$

act39 : $A\_Switch\_Out := FALSE$

act40 : $close\_EV\_Hout := 0$

act41 : $retract\_EV\_Hout := 0$

act42 : $extend\_EV\_Hout := 0$

act43 : $open\_EV\_Hout := 0$

act44 : $general\_EV\_Hout := 0$

act45 : $SDCylinder :\in DOORS \times \{DCYF, DCYR, DCYL\} \to \{STOP\}$

act46 : $SGCylinder :\in GEARS \times \{GCYF, GCYR, GCYL\} \to \{STOP\}$

act26 : $state := computing$

act47 : $at := \varnothing$

act48 : $time := 0$

act49 : $index := 0$

act50 : $handleUp\_interval := 0$

act51 : $handleDown\_interval := 0$

act52 : $pilot\_interface\_light := \{Green \mapsto Off, Orange \mapsto Off, Red \mapsto Off\}$

end

Event *opening_doors_DOWN* $\widehat{=}$
extends *opening_doors_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd7 : $phase = movingdown$
grd8 : $p = R$
grd9 : $l = R$
grd10 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd12 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$
grd13 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := E$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act4 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door open to gear extension
act5 : $index := index + 1$

end

Event *opening_doors_UP* $\widehat{=}$
extends *opening_doors_UP*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $lstate[DOORS] = \{UNLOCKED\}$
grd5 : $phase = movingup$
grd6 : $p = E$
grd7 : $l = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = MOVING\}$
grd11 : $anomaly = FALSE$

then

act1 : $dstate := \{a \mapsto b | a \in DOORS \land b = OPEN\}$
act2 : $p := R$
act3 : $door\_open :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act4 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door open to gear retraction
act5 : $index := index + 1$

end

Event *closing_doors_UP* $\widehat{=}$
extends *closing_doors_UP*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingup$
grd6 : $p = R$
grd7 : $gstate[GEARS] = \{RETRACTED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *closing_doors_DOWN* $\widehat{=}$
extends *closing_doors_DOWN*

any

f

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd3 : $f \in DOORS \rightarrow SDOORS$
grd4 : $\forall e \cdot e \in DOORS \Rightarrow f(e) = CLOSED$
grd5 : $phase = movingdown$
grd6 : $p = E$
grd7 : $gstate[GEARS] = \{EXTENDED\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd9 : $anomaly = FALSE$

then

act1 : $dstate := f$

end

Event *unlocking_UP* $\widehat{=}$
extends *unlocking_UP*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingup$
grd5 : $l = E$
grd6 : $p = E$
grd7 : $i = E$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \wedge b \in DOORS \rightarrow \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{FALSE\})$

end

Event *locking_UP* $\widehat{=}$

extends *locking_UP*

when

grd3 : $dstate[DOORS] = \{CLOSED\}$
grd4 : $phase = movingup$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $p = R$
grd7 : $l = E$
grd9 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd10 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd11 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd8 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \land b = STOP\}$
grd12 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = LOCKED\}$
act3 : $phase := haltup$
act4 : $l := R$
added by D Mery
act44 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{TRUE\})$
act5 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door closed to gear extension/retraction
act6 : $index := index + 1$

end

Event *unlocking_DOWN* $\widehat{=}$
extends *unlocking_DOWN*

when

grd3 : $lstate[DOORS] = \{LOCKED\}$
grd4 : $phase = movingdown$
grd5 : $l = R$
grd6 : $p = R$
grd7 : $i = R$
grd8 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd10 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd11 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \land b = UNLOCKED\}$
act2 : $door\_closed :\in 1 \mathinner{..} 3 \to (DOORS \to \{FALSE\})$

end

Event *locking_DOWN* $\widehat{=}$
extends *locking_DOWN*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $lstate[DOORS] = \{UNLOCKED\}$
grd4 : $p = E$
grd5 : $l = R$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$

grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd6 : $SDCylinder = \{a \mapsto b | a \in DOORS \times CYLINDER \wedge b = STOP\}$
grd10 : $anomaly = FALSE$

then

act1 : $lstate := \{a \mapsto b | a \in DOORS \wedge b = LOCKED\}$
act3 : $phase := haltdown$
act4 : $l := E$
act5 : $door\_closed :\in 1 \mathinner{..} 3 \rightarrow (DOORS \rightarrow \{TRUE\})$
act6 : $at := at \cup \{(index + 1) \mapsto (time + 100)\}$
minimal interval for door closed to extension/retraction
act7 : $index := index + 1$

end

Event *PD1* $\widehat{=}$
extends *PD1*

when

grd1 : $button = UP$
grd2 : $phase = haltup$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := R$

end

Event *PU1* $\widehat{=}$
extends *PU1*

when

grd1 : $button = DOWN$
grd2 : $phase = haltdown$
grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $button := UP$
act3 : $l := E$
act4 : $p := E$
act5 : $i := E$

end

Event *PU2* $\widehat{=}$
extends *PU2*

when

grd1 : $l = R$
grd2 : $p = R$
grd3 : $phase = movingdown$
grd4 : $button = DOWN$
grd5 : $i = R$
grd6 : $lstate[DOORS] = \{LOCKED\}$

grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act4 : $button := UP$
act5 : $l := E$
act6 : $p := E$
act7 : $i := R$

end

Event *CompletePU2* $\widehat{=}$
extends *CompletePU2*

when

grd1 : $phase = movingup$
grd2 : $button = UP$
grd3 : $l = E$
grd4 : $p = E$
grd5 : $i = R$

then

act1 : $phase := haltup$

end

Event *PU3* $\widehat{=}$
extends *PU3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingdown$
grd4 : $p = R$
grd5 : $l = R$
grd6 : $button = DOWN$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $l := E$
act4 : $button := UP$

end

Event *PU4* $\widehat{=}$
extends *PU4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act2 : $p := R$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PU5* $\widehat{=}$
extends *PU5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingdown$
grd3 : $p = E$
grd4 : $button = DOWN$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act1 : $phase := movingup$
act3 : $button := UP$
act4 : $i := E$
act5 : $l := E$

end

Event *PD2* $\widehat{=}$
extends *PD2*

when

grd1 : $l = E$
grd2 : $p = E$
grd3 : $phase = movingup$
grd4 : $i = E$
grd5 : $lstate[DOORS] = \{LOCKED\}$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $l := R$
act4 : $p := R$
act5 : $i := E$

end

Event *CompletePD2* $\widehat{=}$
extends *CompletePD2*

when

grd1 : $phase = movingdown$
grd2 : $button = DOWN$
grd3 : $l = R$
grd4 : $p = R$
grd5 : $i = E$

then

act1 : $phase := haltdown$

end

Event *PD3* $\widehat{=}$
extends *PD3*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $lstate[DOORS] = \{UNLOCKED\}$
grd3 : $phase = movingup$
grd4 : $p = E$
grd5 : $l = E$
grd6 : $button = UP$
grd7 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $l := R$
act4 : $button := DOWN$

end

Event *PD4* $\widehat{=}$
extends *PD4*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd6 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $p := E$
act3 : $button := DOWN$
act4 : $i := R$
act5 : $l := R$

end

Event *PD5* $\widehat{=}$
extends *PD5*

when

grd1 : $dstate[DOORS] = \{CLOSED\}$
grd2 : $phase = movingup$
grd3 : $p = R$
grd4 : $button = UP$
grd5 : $lstate[DOORS] = \{UNLOCKED\}$
grd6 : $door\_open = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd7 : $door\_closed = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act1 : $phase := movingdown$
act2 : $button := DOWN$
act3 : $i := R$
act4 : $l := R$

end

Event *retracting_gears* $\widehat{=}$
extends *retracting_gears*

any

ind

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDED\}$
grd3 : $p = R$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{TRUE\}\}$
grd7 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd8 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$
grd9 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd5 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$
grd10 : $at \neq \varnothing$
grd11 : $time \in ran(at)$
grd12 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTING\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{FALSE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
act4 : $at := at \setminus \{ind \mapsto time\}$

end

Event *retraction* $\widehat{=}$
extends *retraction*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTING\}$
grd4 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \rightarrow \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = RETRACTED\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \rightarrow (GEARS \rightarrow \{TRUE\})$

end

Event *extending_gears* $\widehat{=}$
extends *extending_gears*

any

ind

where

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{RETRACTED\}$
grd3 : $p = E$
grd5 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
grd6 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd7 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd8 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd4 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = MOVING\}$
grd9 : $at \neq \varnothing$
grd10 : $time \in ran(at)$
grd11 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDING\}$
act2 : $gear\_retracted :\in 1 \mathinner{..} 3 \to (GEARS \to \{FALSE\})$
act3 : $at := at \setminus \{ind \mapsto time\}$

end

Event *extension* $\widehat{=}$
extends *extension*

when

grd1 : $dstate[DOORS] = \{OPEN\}$
grd2 : $gstate[GEARS] = \{EXTENDING\}$
grd4 : $gear\_retracted = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd5 : $gear\_extended = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
grd6 : $gear\_shock\_absorber = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = flight\}$
grd7 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = button$
grd3 : $SGCylinder = \{a \mapsto b | a \in GEARS \times CYLINDER \land b = STOP\}$

then

act1 : $gstate := \{a \mapsto b | a \in GEARS \land b = EXTENDED\}$
act2 : $gear\_extended :\in 1 \mathinner{..} 3 \to (GEARS \to \{TRUE\})$
act3 : $gear\_shock\_absorber := \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = ground\}$

end

Event *HPD1* $\widehat{=}$
extends *HPD1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = UP$

then

act2 : $handle :\in 1 \mathinner{..} 3 \to \{DOWN\}$
act3 : $at := at \cup \{(index + 1) \mapsto (time + 160)\}$
analogical switch is seen open 160ms after handle position has changed
act4 : $handleDown\_interval := time + 40000$
add a new time interval (current time + handle not changed interval) in the event activation set
act5 : $handleUp\_interval := 0$
update the handle up interval as 0
act6 : $index := index + 1$
update the current index value

end

Event *HPU1* $\widehat{=}$
extends *HPU1*

when

grd3 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow handle(x) = DOWN$

then

act2 : $handle :\in 1 \mathinner{..} 3 \rightarrow \{UP\}$
act3 : $at := at \cup \{(index + 1) \mapsto (time + 160)\}$
analogical switch is seen open 160ms after handle position has changed
act4 : $handleUp\_interval := time + 40000$
add a new time interval (current time + handle not changed interval) in the event activation set
act5 : $handleDown\_interval := 0$
update the handle down interval as 0
act6 : $index := index + 1$
update the current index value

end

Event *Analogical_switch_closed* $\widehat{=}$
extends *Analogical_switch_closed*

any

in in port
ind

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$
grd3 : $at \neq \varnothing$
grd4 : $time \in ran(at)$
grd5 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{closed\}$
act4 : $A\_Switch\_Out := TRUE$
act5 : $at := (at \cup \{(index + 1) \mapsto (time + 1200)\}) \setminus \{ind \mapsto time\}$
from closed to open 1.2 sec.
act6 : $index := index + 1$

end

Event *Analogical_switch_open* $\widehat{=}$
extends *Analogical_switch_open*

any

in in port
ind

where

grd1 : $in = general\_EV$
grd2 : $\forall x \cdot x \in 1 \mathinner{..} 3 \Rightarrow (handle(x) = UP \lor handle(x) = DOWN)$
grd3 : $at \neq \varnothing$
grd4 : $time \in ran(at)$
grd5 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act3 : $analogical\_switch :\in 1 \mathinner{..} 3 \rightarrow \{open\}$
act4 : $A\_Switch\_Out := FALSE$

act5 : $at := (at \cup \{(index + 1) \mapsto (time + 800)\}) \setminus \{ind \mapsto time\}$
from open to closed .8 sec.
act6 : $index := index + 1$

end

Event *Circuit_pressurized_OK* $\widehat{=}$
extends *Circuit_pressurized_OK*

when

grd1 : $general\_EV\_Hout = Hin$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{TRUE\}$

end

Event *Circuit_pressurized_notOK* $\widehat{=}$
extends *Circuit_pressurized_notOK*

when

grd1 : $general\_EV\_Hout = 0$

then

act9 : $circuit\_pressurized :\in 1 \mathinner{..} 3 \rightarrow \{FALSE\}$

end

Event *Computing_Module_1_2* $\widehat{=}$
extends *Computing_Module_1_2*

when

grd1 : $state = computing$

then

act1 : $general\_EV := general\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act2 : $close\_EV := close\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act3 : $retract\_EV := retract\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act4 : $extend\_EV := extend\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act5 : $open\_EV := open\_EV\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act6 : $gears\_locked\_down := gears\_locked\_down\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act7 : $gears\_man := gears\_man\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act8 : $anomaly := anomaly\_func(handle \mapsto analogical\_switch \mapsto gear\_extended \mapsto gear\_retracted \mapsto gear\_shock\_absorber \mapsto door\_open \mapsto door\_closed \mapsto circuit\_pressurized)$
act9 : $state := electroValve$

end

Event *Update_Hout* $\widehat{=}$

Assign the value of Hout

extends *Update_Hout*

when

grd1 : $state = electroValve$

then

act1 : $general\_EV\_Hout :\mid ((general\_EV = TRUE \land general\_EV\_Hout' = Hin) \lor (general\_EV = FALSE \land general\_EV\_Hout' = 0) \lor (A\_Switch\_Out = TRUE \land general\_EV\_Hout' = Hin) \lor (A\_Switch\_Out = FALSE \land general\_EV\_Hout' = 0))$

pass the current value of hydraulic input port (Hin) to hydraulic output port (Hout)

act2 : $close\_EV\_Hout :\mid ((close\_EV = TRUE \land close\_EV\_Hout' = Hin) \lor (close\_EV = FALSE \land close\_EV\_Hout' = 0))$

act3 : $open\_EV\_Hout :\mid ((open\_EV = TRUE \land open\_EV\_Hout' = Hin) \lor (open\_EV = FALSE \land open\_EV\_Hout' = 0))$

act4 : $extend\_EV\_Hout :\mid ((extend\_EV = TRUE \land extend\_EV\_Hout' = Hin) \lor (extend\_EV = FALSE \land extend\_EV\_Hout' = 0))$

act5 : $retract\_EV\_Hout :\mid ((retract\_EV = TRUE \land retract\_EV\_Hout' = Hin) \lor (retract\_EV = FALSE \land retract\_EV\_Hout' = 0))$

act6 : $state := cylinder$

act7 : $at := at \cup$
$\{(index + 1) \mapsto (time + 2000)\} \cup$
$\{(index + 2) \mapsto (time + 10000)\} \cup$
$\{(index + 3) \mapsto (time + 500)\} \cup$
$\{(index + 4) \mapsto (time + 2000)\} \cup$
$\{(index + 5) \mapsto (time + 500)\} \cup$
$\{(index + 6) \mapsto (time + 2000)\} \cup$
$\{(index + 7) \mapsto (time + 500)\} \cup$
$\{(index + 8) \mapsto (time + 10000)\} \cup$
$\{(index + 9) \mapsto (time + 500)\} \cup$
$\{(index + 10) \mapsto (time + 10000)\}$

general EV 2 (time is given in comments in sec. while in model these are in ms.)

general EV 10
openning EV 0.5
openning EV 2
closure EV 0.5
closure EV 2
retraction EV 0.5
retraction EV 10
extension 0.5
extension 10

act8 : $index := index + 10$

end

Event *CylinderMovingOrStop* $\widehat{=}$

Cylinder Moving or Stop according to the output of hydraulic circuit

extends *CylinderMovingOrStop*

when

grd1 : $state = cylinder$

then

act1 : $SGCylinder : |((SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge extend\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge extend\_EV\_Hout = 0) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = MOVING\} \wedge retract\_EV\_Hout = Hin) \vee (SGCylinder' = \{a \mapsto b | a \in GEARS \times \{GCYF, GCYR, GCYL\} \wedge b = STOP\} \wedge retract\_EV\_Hout = 0))$

act2 : $SDCylinder : |((SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge open\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge open\_EV\_Hout = 0) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = MOVING\} \wedge close\_EV\_Hout = Hin) \vee (SDCylinder' = \{a \mapsto b | a \in DOORS \times \{DCYF, DCYR, DCYL\} \wedge b = STOP\} \wedge close\_EV\_Hout = 0))$

act3 : $state := computing$

end

Event *Failure_Detection_Generic_Monitoring* $\widehat{=}$
extends *Failure_Detection_Generic_Monitoring*

when

grd1 : $(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (handle(x) \neq handle(y) \land handle(y) \neq handle(z) \land handle(x) \neq handle(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (analogical\_switch(x) \neq analogical\_switch(y) \land analogical\_switch(y) \neq analogical\_switch(z) \land analogical\_switch(x) \neq analogical\_switch(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_extended(x) \neq gear\_extended(y) \land gear\_extended(y) \neq gear\_extended(z) \land gear\_extended(x) \neq gear\_extended(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_retracted(x) \neq gear\_retracted(y) \land gear\_retracted(y) \neq gear\_retracted(z) \land gear\_retracted(x) \neq gear\_retracted(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (gear\_shock\_absorber(x) \neq gear\_shock\_absorber(y) \land gear\_shock\_absorber(y) \neq gear\_shock\_absorber(z) \land gear\_shock\_absorber(x) \neq gear\_shock\_absorber(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (door\_open(x) \neq door\_open(y) \land door\_open(y) \neq door\_open(z) \land door\_open(x) \neq door\_open(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (door\_closed(x) \neq door\_closed(y) \land door\_closed(y) \neq door\_closed(z) \land door\_closed(x) \neq door\_closed(z)))$
$\lor$
$(\forall x, y, z \cdot x \in 1 \mathinner{..} 3 \land y \in 1 \mathinner{..} 3 \land z \in 1 \mathinner{..} 3 \land x \neq y \land y \neq z \land x \neq z \Rightarrow (circuit\_pressurized(x) \neq circuit\_pressurized(y) \land circuit\_pressurized(y) \neq circuit\_pressurized(z) \land circuit\_pressurized(x) \neq circuit\_pressurized(z)))$

Generic Monitoring uisng all sensors

then

act1 : $anomaly := TRUE$

end

Event *Failure_Detection_Analogical_Switch* $\widehat{=}$
extends *Failure_Detection_Analogical_Switch*

any

ind

where

grd1 : $analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = open\}$
$\lor$
$analogical\_switch = \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = closed\}$

Gears motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *check_handle_delay* $\widehat{=}$

This event is used to set 280ms in the set "at" for event activation to detect anomaly and detect that hanlde is not change from last 40 sec.

extends *check_handle_delay*

when

grd1 : $time = handleUp\_interval \lor time = handleDown\_interval$

current time is either equal to handle up interval or equal to the handle down interval

then

act1 : $at := at \cup \{(index + 1) \mapsto (time + 280)\}$

To add a new interval to the event activation set

act3 : $index := index + 1$

update the current index value

end

Event *Failure_Detection_Pressure_Sensor* $\widehat{=}$
extends *Failure_Detection_Pressure_Sensor*

any

ind

where

grd1 : $circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = TRUE\} \lor circuit\_pressurized \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b = FALSE\}$

Circuit pressurized motion monitoring without considering time

grd2 : $at \neq \varnothing$

grd3 : $time \in ran(at)$

grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$

act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *Failure_Detection_Doors* $\widehat{=}$
extends *Failure_Detection_Doors*

any

ind

where

grd1 : $door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
$\lor$
$door\_open \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{FALSE\}\}$
$\lor$
$door\_closed \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in DOORS \to \{TRUE\}\}$
Doors motion monitoring without considering time
grd2 : $at \neq \varnothing$
grd3 : $time \in ran(at)$
grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$
act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *Failure_Detection_Gears* $\widehat{=}$
extends *Failure_Detection_Gears*

any

ind

where

grd1 : $gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
$\lor$
$gear\_retracted \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{FALSE\}\}$
$\lor$
$gear\_extended \neq \{a \mapsto b | a \in 1 \mathinner{..} 3 \land b \in GEARS \to \{TRUE\}\}$
Gears motion monitoring without considering time
grd2 : $at \neq \varnothing$
grd3 : $time \in ran(at)$
grd4 : $ind \in dom(at) \land ind \mapsto time \in at$

then

act1 : $anomaly := TRUE$
act2 : $at := at \setminus \{ind \mapsto time\}$

end

Event *tic_tock* $\widehat{=}$
time progression
extends *tic_tock*

any

tm

where

grd1 : $tm \in \mathbb{N}$
grd2 : $tm > time$
to take a new value of time in the future
grd3 : $ran(at) \neq \varnothing \Rightarrow tm \leq min(ran(at))$

then

act1 : $time := tm$
assign a new value of time to the current time

end

Event *pilot_interface_Green_light_On* $\widehat{=}$ green light is on when gears locked down is true

when

grd1 : $gears\_locked\_down = TRUE$
gears locked down must be true

then

act1 : $pilot\_interface\_light(Green) := On$
To set on of Green light of pilot interface light

end

Event *pilot_interface_Orange_light_On* $\widehat{=}$ orange light is on when gears maneuvering is true

when

grd1 : $gears\_man = TRUE$
gears maneuvering must be true

then

act1 : $pilot\_interface\_light(Orange) := On$
To set on of Orange light of pilot interface light

end

Event *pilot_interface_Red_light_On* $\widehat{=}$ red light is on when anomaly is detected (true)

when

grd1 : $anomaly = TRUE$
anomaly must be true
grd2 : $pilot\_interface\_light(Red) = Off$

then

act1 : $pilot\_interface\_light(Red) := On$
To set on of Red light of pilot interface light

end

Event *pilot_interface_Green_light_Off* $\widehat{=}$ green light is off when gears locked down is false

when

grd1 : $gears\_locked\_down = FALSE$
gears locked down must be false

then

act1 : $pilot\_interface\_light(Green) := Off$
To set off of Green light of pilot interface light

end

Event *pilot_interface_Orange_light_Off* $\widehat{=}$ orange light is off when gears maneuvering is false

when

grd1 : $gears\_man = FALSE$
gears maneuvering must be false

then

act1 : $pilot\_interface\_light(Orange) := Off$
To set off of Orange light of pilot interface light

end

Event *pilot_interface_Red_light_Off* $\widehat{=}$ red light is off when anomaly is detected (false)

when

grd1 : $anomaly = FALSE$
anomaly must be false

grd2 : $pilot\_interface\_light(Red) = On$

then

act1 : $pilot\_interface\_light(Red) := Off$
To set off of Red light of pilot interface light

end

END