Landing gear system

Frédéric Boniol and Virginie Wiels

ONERA-Toulouse, 2 av. E. Belin, BP 4025, 31055 Toulouse France
{firstname.name}@onera.fr

Abstract. This document presents the landing system of an aircraft. It describes the system and provides some of its requirements. We propose this case study as a benchmark for techniques and tools dedicated to the verification of behavioral properties of systems.

1 Introduction

This document presents a landing system. It describes the system and provides some of its requirements. We propose this case study as a benchmark for techniques and tools dedicated to the verification of behavioral properties of systems.

The landing system is in charge of maneuvering landing gears and associated doors. The landing system is composed of 3 landing sets: front, left and right. Each landing set contains a door, a landing-gear and associated hydraulic cylinders. A simplified schema of a landing set is presented in Figure 1.

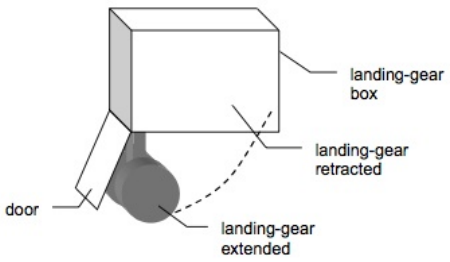


Fig. 1. Landing set

The system is controlled digitally in nominal mode and analogically in emergency mode. In this case study, we do not consider the emergency mode. However, in order to allow the pilot to activate the emergency command, the system has to elaborate health parameters for all the equipments involved in the landing gear function. This health monitoring part is in the scope of the case study.

In nominal mode, the landing sequence is: open the doors of the landing gear boxes, extend the landing gears and close the doors. This sequence is illustrated

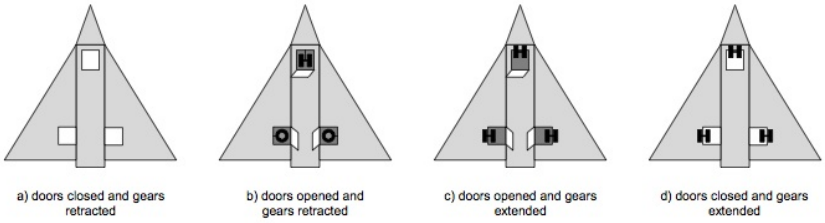


Fig. 2. The landing sequence

in Figure 2. After taking off, the retraction sequence to be performed is: open the doors, retract the landing gears and close the doors.

This system is representative of critical embedded systems. The action to be done at each time depends on the state of all the physical devices and on their temporal behavior. When considering such systems, the challenge is firstly to model and to program the software part controlling the landing and the retraction sequence, and secondly to prove safety requirements taking into account the physical behavior of hydraulic devices.

The document is organized as follows:

- Section 2 describes the architecture of the system;
- Section 3 describes the behavior of the hydraulic equipment;
- Section 4 specifies the expected behavior of the system, i.e. the behavior to be implemented by the control software;
- Section 5 presents the requirements of the system, that is the set of properties to be satisfied by the computing units of the system.

2 Architecture of the system

As shown in Figure 3, the landing gear system is composed of three parts:

- a mechanical part which contains all the mechanical devices and the three landing sets,
- a digital part including the control software,
- and a pilot interface.

2.1 The pilot interface

To command the retraction and outgoing of gears, an Up/Down handle is provided to the pilot. When the handle is switched to "Up" the retracting landing gear sequence is executed, when the handle is switched to "Down" the extending landing gear sequence is executed.

The pilot has a set of lights giving the current position of gears and doors, and the current health state of the system and its equipments. These lights are:

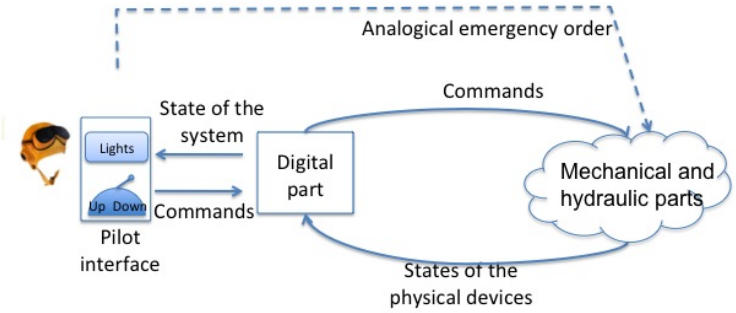


Fig. 3. Global architecture

– one green light: “gears are locked down”,
– one orange light: “gears maneuvering” ,
– one red light: “landing gear system failure”,

No light is on when the gears are locked up. In case of failure, the pilot can manually activate the emergency hydraulic circuit. The expected consequence of this action is to lock the gears in the down position. In case of success and if the corresponding sensors are still working, the green light “gears are locked down” must be on.

2.2 The mechanical and hydraulic parts

The architecture of the hydraulic part is described in Figure 4. As stated previously, the system is composed of three landing sets: front, left and right sets. Each set has got:

– a landing gear uplock box,
– and a door with two latching boxes in the closed position.

The landing gears and doors motion is performed by a set of actuating cylinders. The cylinder position corresponds to the door or landing gear position (when a door is open, the corresponding cylinder is extended). The landing system has the following actuating cylinders:

– For each door, a cylinder opens and closes the door.
– For each landing gear, a cylinder retracts and extends the landing gear.

Hydraulic power is provided to the cylinders by a set of electro-valves:

– One general electro-valve which supplies the specific electro-valves with hydraulic power from the aircraft hydraulic circuit.
– One electro-valve that sets pressure on the portion of the hydraulic circuit related to door opening.

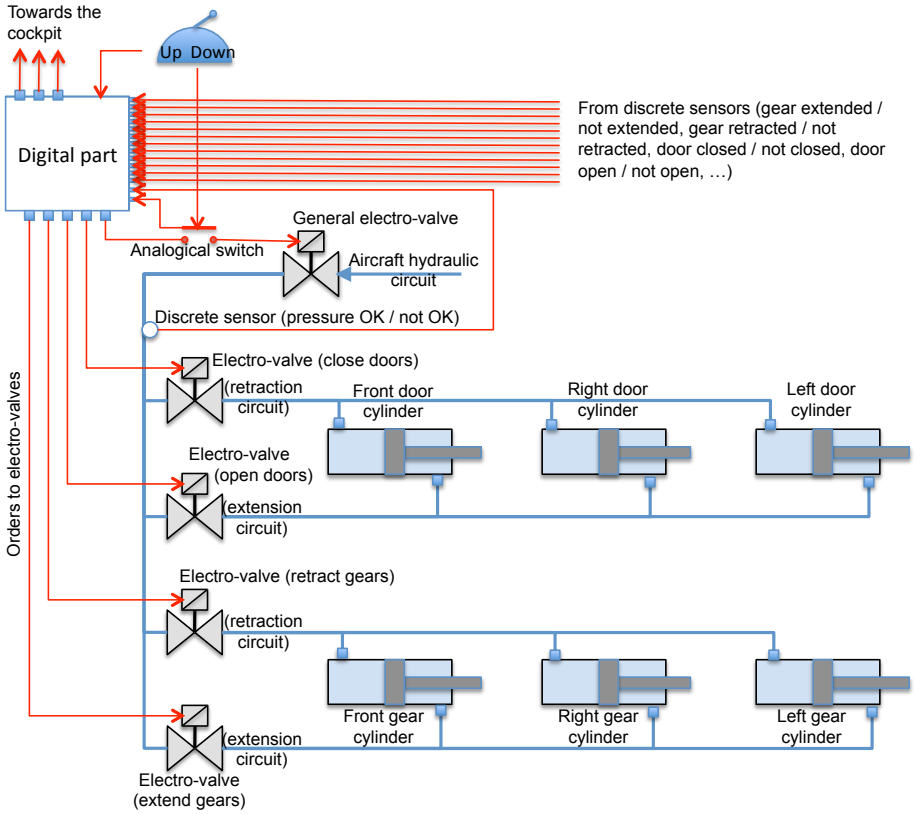


Fig. 4. Architecture of the hydraulic part

– One electro-valve that sets pressure on the portion of the hydraulic circuit related to door closing.
– One electro-valve that sets pressure on the portion of the hydraulic circuit related to landing gear extending.
– One electro-valve that sets pressure on the portion of the hydraulic circuit related to the landing gear retracting.

Each electro-valve is activated by an electrical order coming from the digital part. In the specific case of the general electro-valve, this electrical order goes through an analogical switch in order to prevent abnormal behavior of the digital part (e.g. abnormal activation of the general electro-valve).

Note that the three doors (resp. gears) are controlled simultaneously by the same electro-valve. Put differently, it is not possible to control the doors (resp. gears) separately.

A set of discrete sensors inform the digital part about the state of the equipments:

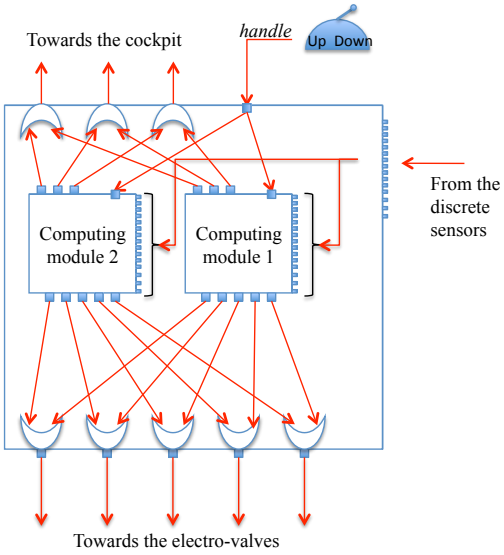


Fig. 5. Digital architecture

- Front / right / left gear is locked / not locked in the extended position.
- Front / right / left gear is locked / not locked in the retracted position.
- Front / right / left gear shock absorber is on ground / in flight.
- Front / right / left door is in open / not open position.
- Front / right / left door is locked / not locked in the closed position.
- The hydraulic circuit (after the general electro-valve) is pressurized / not pressurized.
- The analogical switch between the digital part and the general electro-valve is closed / open.

In order to prevent sensor failures, each sensor is triplicated (i.e. each sensor is divided into three independent micro-sensors). It delivers simultaneously three discrete values describing the same situation (for instance "the left gear is locked in retracted position").

The behavior of the physical equipment involved in the hydraulic architecture is described in Section 3.

2.3 The digital part

The digital part is composed of two identical computing modules (see Figure 5). Each one executes in parallel the same control software. This software is in charge of controlling gears and doors, of detecting anomalies, and of informing the pilot about the global state of the system and anomalies (if any). It is part of a retroaction loop with the physical system, and produces commands for the

distribution elements of the hydraulic system with respect to the sensors values and the pilot orders. The two computing modules receive the same inputs. These inputs are (remember that all the inputs are triplicated):

- $handle_i \in \{up, down\}$ $i = 1, 2, 3$
  $handle_i$ characterizes the position of the handle. If the handle is UP (resp. DOWN), then $handle_i = up$ (resp. $handle_i = down$).

- $analogical\_switch_i \in \{open, closed\}$ $i = 1, 2, 3$
  $analogical\_switch_i$ characterizes the position of the analogical switch: open or closed. See section 3.1.

- $gear\_extended_i[x] \in \{true, false\}$ $i = 1, 2, 3$, x in $\{front, right, left\}$
- $gear\_retracted_i[x] \in \{true, false\}$ $i = 1, 2, 3$, x in $\{front, right, left\}$
  $gear\_extended_i[x]$ is true if the corresponding gear is locked in the extended position and false in the other case.
  $gear\_retracted_i[x]$ is true if the corresponding gear is locked in the retracted position and false in the other case.
  See section 3.3 and Figure 11.

- $gear\_shock\_absorber_i[x] \in \{ground, flight\}$ $i = 1, 2, 3$, x in $\{front, right, left\}$
  $gear\_shock\_absorber_i[x]$ is returned by a sensor implemented directly on the corresponding gear (see Figure 11). It is true if and only if the aircraft is on ground.

- $door\_closed_i[x] \in \{true, false\}$ $i = 1, 2, 3$, x in $\{front, right, left\}$
- $door\_open_i[x] \in \{true, false\}$ $i = 1, 2, 3$, x in $\{front, right, left\}$
  $door\_closed_i[x]$ is true if and only if the corresponding door is locked closed.
  $door\_open_i[x]$ is true if and only if the corresponding door is locked open.
  See section 3.3 and Figure 12.

- $circuit\_pressurized_i \in \{true, false\}$ $i = 1, 2, 3$
  $circuit\_pressurized_i$ is returned by a pressure sensor on the hydraulic circuit between the general electro-valve and the maneuvering electro-valve (see Figure 4). $circuit\_pressurized_i$ is true if and only if the pressure is high in this part of the hydraulic circuit.

The total amount of input discrete values received by each computing module is 54 (3 *handle*, 3 *analogical_switch*, 9 *gear_extended*, 9 *gear_retracted*, 9 *gear_shock_absorber*, 9 *door_closed*, 9 *door_open* and 3 *circuit_pressurized*).

From these inputs, each module computes 5 electrical orders for the electro-valves:

- $general\_EV_k \in \{true, false\}$ $k = 1, 2$
- $close\_EV_k \in \{true, false\}$ $k = 1, 2$
- $open\_EV_k \in \{true, false\}$ $k = 1, 2$

- $retract\_EV_k \in \{true, false\}\ k = 1, 2$
- $extend\_EV_k \in \{true, false\}\ k = 1, 2$

where "EV" stands for "Electro-Valve" and k stands for the number of the considered computing module. These corresponding electrical orders outgoing from the two modules are physically produced on the same electrical line. The implicit composition of two outputs is an electrical "OR" as shown in Figure 5. For instance, let us consider the *general_EV* parameter. If the two modules produce the same value on $general\_EV_1$ and $general\_EV_2$, then this value is produced to the general electro-valve. Otherwise, if only one of them is *true* (because of a failure somewhere in the digital part), then the value *true* is produced to the electro-valve, even if it is not the correct value. The problem will anyway be detected at the next cycle when the module that produced the *false* value will detect an unexpected behavior with respect to its own orders. Then it will inform the pilot of a potential anomaly in the system.

Similarly the two modules produce global boolean state variables to the cockpit:

- $gears\_locked\_down_k \in \{true, false\}\ k = 1, 2$
- $gears\_maneuvering_k \in \{true, false\}\ k = 1, 2$
- $anomaly_k \in \{true, false\}\ k = 1, 2$

These outputs are synthesized by each module from sensors data and from the situation awareness. Similarly to electrical orders provided to the electro-valves, the boolean state variables from the two modules are composed following a logical "OR" operation. If $gears\_locked\_down_k$ (for some k) is sent to the pilot interface with the value *true*, then the green light "gears are locked down" is on. If $gears\_maneuvering_k$ (for some k) is sent to the pilot interface with the value *true*, then the orange light "gears maneuvering" is on. If $anomaly_k$ (for some k) is sent to the pilot interface with the value *true*, then the red light "landing gear system failure" is on. The specification of the digital part is described in Section 4.

The output interface of each module is synthesized on Figure 6.

3 Behavior of the hydraulic equipment

3.1 The analogical switch (between the digital part and the general electro-valve)

The aim of this switch is to protect the system against abnormal behavior of the digital part. In order to prevent inadvertent order to the electro-valves, the general electro-valve can be stimulated only if this switch is closed. The switch is closed each time the "Up/Down" handle is moved by the pilot, and it remains closed 20 seconds. After this duration, the switch automatically becomes open. In the closed position, the switch transmits the electrical order from the digital part to the general electro-valve. In the open position, no electrical order is sent

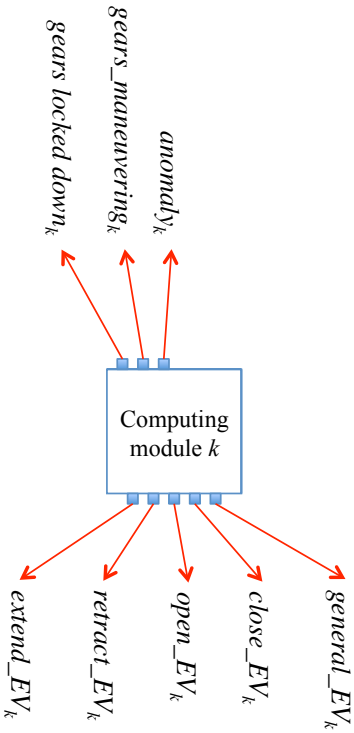


Fig. 6. Electrical outputs of the computing module k ($k = 1, 2$)

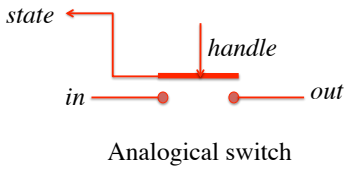


Fig. 7. Interface of the analogical switch

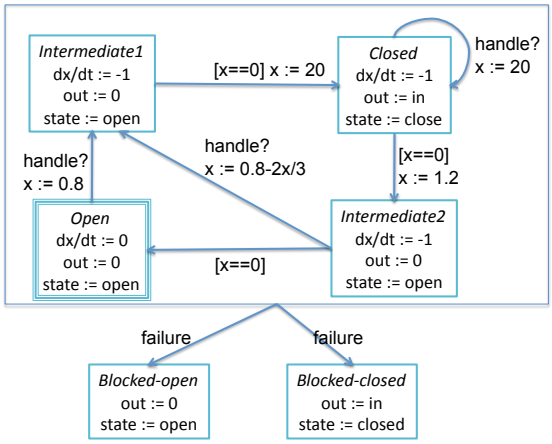


Fig. 8. Physical behavior of the analogical switch

to the electro-valve. In that case, the oil pressure in the hydraulic circuit becomes down.

Because of inertial reasons, the transition from the two states closed and open takes a given amount of time:

- from open to closed: 0.8 second,
- from closed to open 1.2 seconds,

In addition to this normal behavior, the analogical switch can fail. We consider only permanent failures: the switch remains blocked in the closed or in the open position. A failure can occur at any time.

The global behavior of the switch, including failures, is specified by the model of Figure 7 and the hierarchical hybrid automaton of Figure 8. In this specification, *in* stands for the input value of the switch. In the global architecture of Figure 4, the *in* port of the analogical switch is connected to the *general_EV* output of the digital part (i.e., $in = general\_EV$). The variable *out* stands for the electrical output of the switch. It is connected to the electrical port of the general electro-valve. The variable *state* is the logical output of the switch. It belongs to the set $\{open, closed\}$. It is connected to the input port *analogical_switch* of the

digital part. Note that this output value is triplicated as explained in section 2.3. The event *handle?* stands for the detection of a movement of the pilot handle. This event is received each time the pilot moves the handle. And finally x is an internal continuous variable that evolves according to the differential equation in each state. The aim of this variable is to count the time in each state. For instance, in the state Open, x does not evolve, *state* is set to *open*, and *out* is set to 0 whatever the value of *in*. When *handle* is received, x is set to 0.8, the state Intermediate1 is reached and x begins to decrease. The values of *state* and *out* remain unchanged. 0.8 seconds later, x reached the null value. The transition from Intermediate1 to Close is fired and x is set to 20. *state* is now set to *closed* and *out* is set to *in*. And so on. The initial state of the automaton is Open.

Note that the switch is independent from the digital part.

3.2 Electro-valves

All the electro-valves are supposed to have the same behavior. As shown in Figure 9, an electro-valve is an hydraulic equipment which has got two hydraulic ports *Hin* (hydraulic input port) and *Hout* (hydraulic output port), and an electrical port ($E \in \{true, textitfalse$). Its behavior depends on the value of the electrical order connected to E.

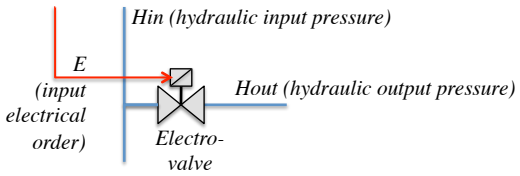


Fig. 9. An electro-valve equipment

- if $E = false$ (the voltage of the electrical order is down), then $Hout = 0$ (no pressure on the hydraulic output side, the hydraulic circuit is open);
- if $E = true$ (the voltage of the electrical order is high), then $Hout = Hin$ (the hydraulic circuit is closed);

Note that the electrical order must be sustained to *true* (i..e, at the high voltage) to maintain the electro-valve in the closed position. Put differently, the electrical order is not a discrete event, but can be seen as an analogical signal.

Because of inertial reasons, we suppose that from the open position to the closed position, the pressure grows up continuously from 0 to *Hin*. In this case study we suppose that the pressure grows up linearly, and that the total duration of the transition phase is **1 second**. In the same way, the pressure goes down continuously from *Hin* to 0. We suppose that the pressure goes down linearly, and that the total duration of the transition phase is 3,6 seconds.

In addition to this normal behavior, any electro-valve can fail. We consider only permanent failures: the electro-valve remains blocked in the closed or the open state. A failure can occur at any time.

3.3 Cylinders

Cylinders are pure hydraulic equipments. As shown on Figure 10, they begin to move when they receive hydraulic pressure, and they stop to move when the pressure goes down or when they reach the end of their race.

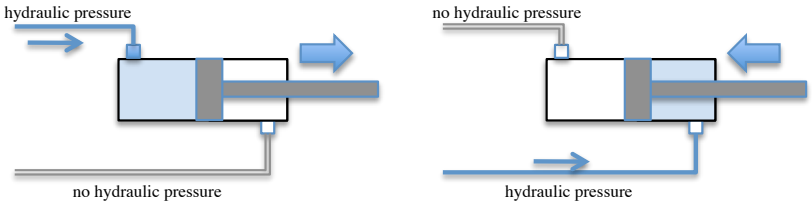


Fig. 10. Extension and retraction of a cylinder

Gear cylinders. Gear cylinders are locked in high or down position by means of a latching box mechanism (the latching boxes are physically on the gears, one for each position). When a gear cylinder is locked in high (resp. down) position and when it receives pressure from the high (resp. down) hydraulic circuit,

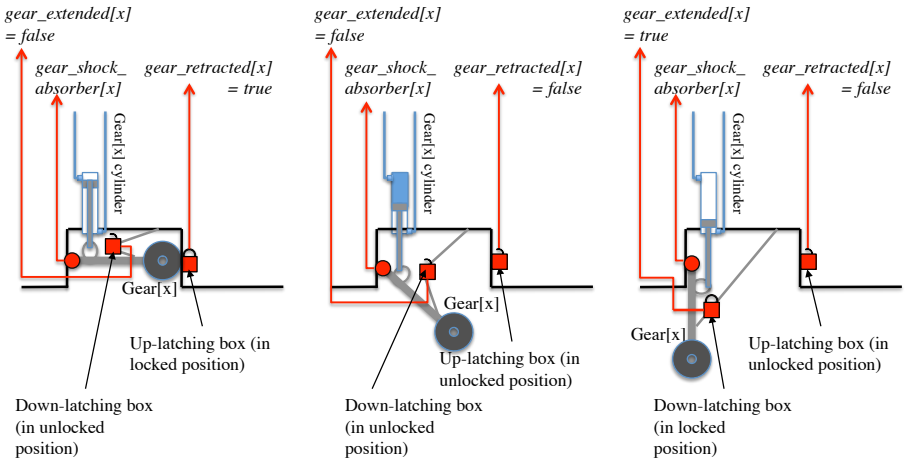
- first it is unlocked from the high (resp. down) position
- then it moves to the down (resp. high) position
- and finally it is locked in the down (resp. high) position.

The behavior of the gear (including the values returned by the gear position sensors) is described on Figure 11.

Door cylinders. Door cylinders are locked (by means of two latching boxes on each door) only in closed position. Doors are maintained open by maintaining pressure in extension circuit. When a door cylinder is locked in closed position and when it receives pressure from the extension hydraulic circuit,

- first it is unlocked from the closed position
- then it moves to the open position
- and finally it is maintained in the open position as long as the pressure is maintained in the hydraulic extension circuit.

The behavior of the door (including the values returned by the door position sensors) is described on Figure 12.



(a) gear in the retracted position (b) gear in the intermediate position (c) gear in the extended position

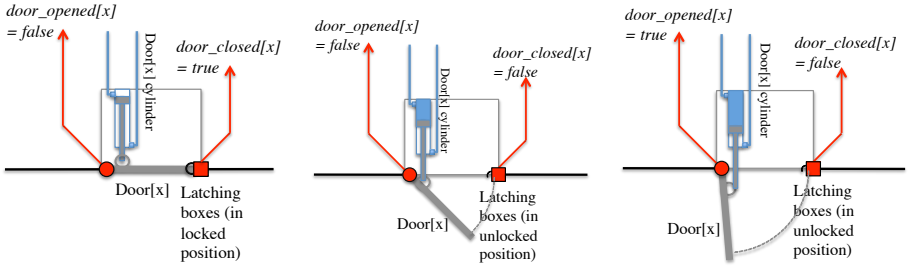
Fig. 11. Integration Gear - cylinder for the block $x \in \{front, right, left\}$ (the door is not represented)

Temporal behavior for the cylinders. All these operations are done automatically with the hydraulic pressure only. No electrical part is involved in cylinders. These operations take a certain amount of time, depending on the position of the cylinder in the aircraft and in the hydraulic circuit. The durations are given in the array below. The values are only mean values. The true durations can vary around these values up to 20%.

duration (in seconds) of ...	front gear	front door	right gear	right door	left gear	left door
unlock in down position	0.8	-	0.8	-	0.8	-
from down to high position	1.6	1.2	2	1.6	2	1.6
lock in high position	0.4	0.3	0.4	0.3	0.4	0.3
unlock in high position	0.8	0.4	0.8	0.4	0.8	0.4
from high to down position	1.2	1.2	1.6	1.5	1.6	1.5
lock in down position	0.4	-	0.4	-	0.4	-

Note that it is possible to stop and to inverse the motion of any cylinder at any time.

An example of the front-gear movement is given on Figure 13. This scenario is based on the mean values given in the previous table. Let us suppose that the front gear is locked in the extended position when the pressure arrives in the retraction circuit (first red arrow on the left). Then the gear is unlocked 0.4s later. It goes up during 1.6s. And finally it is locked in the retracted position 2.4s after the arrival of the pressure in the hydraulic circuit. Let us consider now



(a) door in the closed position (b) door in the intermediate position (c) door in the open position

Fig. 12. Integration Door - cylinder for the block $x \in \{front, right, left\}$ (the gear is not represented)

that the pressure arrives in the extension circuit. The gear is unlocked 0.8s later. It begins moving down. Let us suppose now that the pressure is stopped. Then the cylinder stops as well in the current position. If the pressure arrives again in the retraction circuit, the gear goes up immediately from this current position at normal speed. In the same way, the last part of the scenario describes the extension phase without any interruption.

In addition to this normal behavior, any cylinder can fail. We consider only permanent failures: the cylinder remains blocked in the last position (down, high, or between these two positions). Any failure can occur at any time.

4 Software specification

The aim of the software part of the system is twofold:

1. to control the hydraulic devices according to the pilot orders and to the mechanical devices positions;
2. to monitor the system and to inform the pilot in case of anomaly.

The first objective is described in section 4.1. The second one is described in section 4.3.

4.1 Expected scenarios in normal mode

When the command line is working (in normal mode), the landing system reacts to the pilot orders by actioning or inhibiting the electro-valves of the appropriate cylinders. Two basic scenarios are considered: the outgoing sequence, and the retraction sequence.

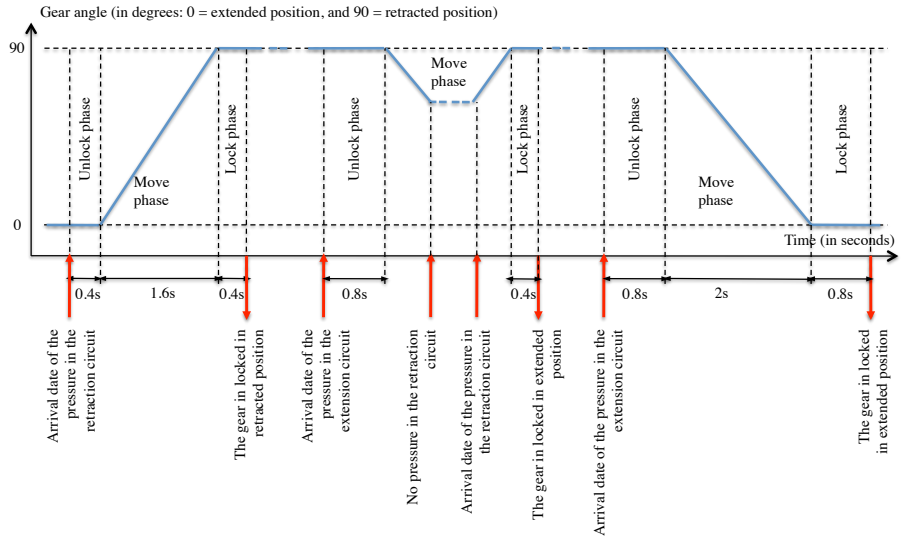


Fig. 13. Example of the front gear angle evolution (angle of the gear w.r.t the vertical: 0 (resp. 90) corresponds to the down (resp. up) position)

Outgoing sequence. The outgoing of gears is decomposed in a sequence of elementary actions. When the gears are locked in retracted position, and the doors are locked in closed position, if the pilot sets the handle to "Down", then the software should have the following sequence of actions:

1. stimulate the general electro-valve isolating the command unit in order to send hydraulic pressure to the maneuvering electro-valves,
2. stimulate the door opening electro-valve,
3. once the three doors are in the open position, stimulate the gear outgoing electro-valve,
4. once the three gears are locked down, stop the stimulation of the gear outgoing electro-valve,
5. stop the stimulation of the door opening electro-valve,
6. stimulate the door closure electro-valve,
7. once the three doors are locked in the closed position, stop the stimulation of the door closure electro-valve,
8. and finally stop stimulating the general electro-valve.

Retraction sequence. In the same way, the retraction of gears is decomposed in a sequence of elementary actions. When the gears are locked in down position, and the doors are locked in closed position, if the pilot sets the handle to "Up", then the software should have the following sequence of actions:

1. stimulate the general electro-valve isolating the command unit, in order to send hydraulic pressure to the maneuvering electro-valves,

2. stimulate the door opening electro-valve,
3. once the three doors are in the open position, if the three shock absorbers are relaxed, then stimulate the gear retraction electro-valve and go to step 4, else (if one of the three shock absorbers is not relaxed) go to step 5,
4. once the three gears are locked up, stop the stimulation of the gear retraction electro-valve,
5. stop the stimulation of the door opening electro-valve,
6. stimulate the door closure electro-valve,
7. once the three doors are locked in the closed position, stop the stimulation of the door closure electro-valve,
8. and finally stop stimulating the general electro-valve.

The previous sequences should be interruptible by counter orders (a retraction order occurs during the let down sequence and conversely) at any time. In that case, the scenario continues from the point where it was interrupted. For instance, if an outgoing sequence is interrupted in the door closure phase (step 6 of the outgoing sequence) by an "Up" order, then the stimulation of the door closure electro-valve is stopped, and the retraction sequence is executed from step 2: the door opening electro-valve is stimulated and the doors begin opening again. Afterwards, the scenario continues up to the final step or up to a new interruption.

Interaction with the cockpit. Each control software $k \in \{1, 2\}$[1] computes the three state booleans $gears\_locked\_down_k$, $gears\_maneuvering_k$ and $anomaly_k$.

- $gears\_locked\_down_k = true$ if and only if the three gears are seen as locked in extended position (sensor $gear\_extended[x] = true\ \forall x \in \{front, right, left\}$).
- $gears\_maneuvering_k = true$ if and only if at least one door or one gear is maneuvering, i.e., at least one door is not locked in closed position or one gear is not locked in extension or retraction position.
- $anomaly_k$ is specified in section 4.3.

4.2 Timing constraints

Because of hydraulic constraints, timing constraints must be satisfied by the control software.

Electro-valve stimulation. Because of inertia of the oil pressure,

- stimulations of the general electro-valve and of the maneuvering electro-valve must be separated by at least 200ms,
- orders to stop the stimulation of the general electro-valve and of the maneuvering electro-valve must be separated by at least 1s.

[1] remember that the digital part of the system is composed of two computing modules, each of them implements an instance of the control software

Contrary orders. Because of inertia of the oil pressure,

- two contrary orders (closure / opening doors, extension / retraction gears) must be separated by at least 100ms.

4.3 Health monitoring and expected scenarios in case of inconsistency

The second objective of the control software is to detect anomalies and to inform the pilot. Anomalies are caused by failures on hydraulic equipment, electrical components, or computing modules.

Generic monitoring. Each sensor is triplicated. The first activity of the control software is to select one of these three values. Let us call X a sensor and $X_i(t)$ $i = 1, 2, 3$ the three values of X received at time t:

- If at t the three channels are considered as valid and are equal, then the value considered by the control software is this common value.
- If at t one channel is different from the two others for the first time (i.e., the three channels were considered as valid up to t), then this channel is considered as invalid and is definitely eliminated. Only the two remaining channels are considered in the future. At time t, the value considered by the control software is the common value of the two remaining channels.
- If a channel has been eliminated previously, and if at t the two remaining channels are not equal, then the sensor is definitely considered as invalid.

An anomaly is detected each time a sensor is definitely considered as invalid.

Analogical switch monitoring.

- If the analogical switch is seen open **1 second** after the handle position has changed, then the switch is considered as invalid.
- If the analogical switch is seen closed **1.5 second** after a time interval of **20 seconds** during which the handle position has not changed, then the switch is considered as invalid.

In these two cases, an anomaly is detected.

Pressure sensor monitoring.

- If the hydraulic circuit is still unpressurized 2 seconds after the general electro-valve has been stimulated, then an anomaly is detected in the hydraulic circuit.
- If the hydraulic circuit is still pressurized 10 seconds after the general electro-valve has been stopped, then an anomaly is detected in the hydraulic circuit.

Doors motion monitoring.

- if the control software does not see the value $door\_closed[x] = false$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the opening electrovalve, then the doors are considered as blocked and an anomaly is detected.
- if the control software does not see the value $door\_open[x] = true$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the opening electrovalve, then the doors are considered as blocked and an anomaly is detected.
- if the control software does not see the value $door\_open[x] = false$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the closure electrovalve, then the doors are considered as blocked and an anomaly is detected.
- if the control software does not see the value $door\_closed[x] = true$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the closure electrovalve, then the doors are considered as blocked and an anomaly is detected.

Gears motion monitoring.

- if the control software does not see the value $gear\_retracted[x] = false$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the retraction electrovalve, then the gears are considered as blocked and an anomaly is detected.
- if the control software does not see the value $gear\_retracted[x] = true$ for all $x \in \{front, left, right\}$ 10 seconds after stimulation of the retraction electrovalve, then the gears are considered as blocked and an anomaly is detected.
- if the control software does not see the value $gear\_extended[x] = false$ for all $x \in \{front, left, right\}$ **7 seconds** after stimulation of the extension electrovalve, then the gears are considered as blocked and an anomaly is detected.
- if the control software does not see the value $gear\_extended[x] = true$ for all $x \in \{front, left, right\}$ 10 seconds after stimulation of the extension electrovalve, then the gears are considered as blocked and an anomaly is detected.

Expected behavior in case of anomaly. Whenever an anomaly is detected, the system is globally considered as invalid. The data $anomaly_k = true$ is sent to the pilot interface (where k is the part number of the module that has detected the anomaly). This message is then maintained forever. The effect of this action is to put on the red light "landing gear system failure".

Otherwise (no anomaly ever happened), the data $anomaly_k = false$ is sent and maintained to the pilot interface. The effect of this action is to keep off the red light "landing gear system failure".

5 Requirements / Properties

The requirements to be proved on the system are divided into two parts: normal mode requirements, and failure mode requirements

5.1 Normal mode requirements

Requirement R_1:

- (R_{11}) When the command line is working (normal mode), if the landing gear command handle 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 handle has been pushed;
- (R_{12}) When the command line is working (normal mode), if the landing gear command handle 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 handle 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.

- (R_{11}bis) When the command line is working (normal mode), if the landing gear command handle has been pushed DOWN and stays DOWN, then eventually the gears will be locked down and the doors will be seen closed;
- (R_{12}bis) When the command line is working (normal mode), if the landing gear command handle has been pushed UP and stays UP, then eventually the gears will be locked retracted and the doors will be seen closed.

Requirement R_2:

- (R_{21}) When the command line is working (normal mode), if the landing gear command handle remains in the DOWN position, then retraction sequence is not observed.
- (R_{22}) When the command line is working (normal mode), if the landing gear command handle remains in the UP position, then outgoing sequence is not observed.

Requirement R_3:

- (R_{31}) 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.
- (R_{32}) 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.

Requirement R_4:

- (R_{41}) When the command line is working (normal mode), opening and closure doors electro-valves are not stimulated simultaneously.
- (R_{42}) When the command line is working (normal mode), outgoing and retraction gears electro-valves are not stimulated simultaneously.

Requirement R_5:

– (R_{51})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.

5.2 Failure mode requirements

Requirement R_6:

– (R_{61}) If one of the three doors is still seen locked in the closed position more than **7 seconds** after stimulating the opening electro-valve, then the boolean output *normal_mode* is set to *false*.
– (R_{62}) If one of the three doors is still seen locked in the open position more than **7 seconds** after stimulating the closure electro-valve, then the boolean output *normal_mode* is set to *false*.
– (R_{63}) If one of the three gears is still seen locked in the down position more than **7 seconds** after stimulating the retraction electro-valve, then the boolean output *normal_mode* is set to *false*.
– (R_{64}) If one of the three gears is still seen locked in the up position more than **7 seconds** after stimulating the outgoing electro-valve, then the boolean output *normal_mode* is set to *false*.

Requirement R_7:

– (R_{71}) If one of the three doors is not seen locked in the open position more than **7 seconds** after stimulating the opening electro-valve, then the boolean output *normal_mode* is set to *false*.
– (R_{72}) If one of the three doors is not seen locked in the closed position more than **7 seconds** after stimulating the closure electro-valve, then the boolean output *normal_mode* is set to *false*.
– (R_{73}) 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*.
– (R_{74}) 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*.

Requirement R_8:

– (R_{81}) When at least one computing module is working, if the landing gear command handle 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.
– (R_{82}) When at least one computing module is working, if the landing gear command handle 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.