7 COMMUNICATION SYSTEM CAPABILITY REQUIREMENTS

This chapter provides requirements applicable to the full communication system (i.e., the network or bus or other interconnection topology and the end-points).

7.1 Generic capability requirements

SAVOIR-OCS-GEN-010

OCS non-time-critical transfer capability

The (OCS) shall support the transfer of non-time-critical data.

Rationale: The (OCS) shall provide the capabilities of performing the transfer of data that is not sensitive to timing.

Comment: No constraint regarding the type of medium to be used for such data transfer are imposed by this specification. The only stringent requirements related to it is SAVOIR-OCS-GEN-010, i.e. that transfer of non-time-critical data does not lead to a violation of timing requirements related to time-critical data transfers.

Verification Method: RoD, T

SAVOIR-OCS-GEN-020

OCS time-critical transfer capability

The (OCS) shall support the transfer of time-critical data.

Rationale: The (OCS) shall provide the capabilities of performing the transfer of data whose correctness is associated to timeliness.

Comment: In such case, the class of communication used will have bounded latency or deterministic characteristics.

Verification Method: RoD, T

SAVOIR-OCS-GEN-030

Transfer timing requirements

Each time-critical data transfer shall be associated with timing requirements.

Rationale: *Time critical implies a timely constraint transmission. To achieve this transmission, several values will be given to characterize those constraints (e.g, maximum latency and maximum jitter) which stems from the needs of clients of the communication system (e.g., communication needs of the AOCS application to transfer commands to actuators).*

Verification Method: RoD, T

SAVOIR-OCS-GEN-040

OCS concurrent transfer capability

The (OCS) shall support the transfer of non-time-critical data and time-critical data concurrently.

Rationale: *The cohabitation of time-critical and non-time-critical data is a key feature. For example, non-time-critical science packets transfer in parallel of time-critical telecommand transmission. Time-critical delivery is necessary for Command & Control, but less important for Science telemetry, and a major benefit of new communication technologies is the merging of both traffics in a single communication system.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-050

OCS transmission of SDU

The (OCS) shall support the transmission of a SDU on the communication system.

Rationale: *As per the definition of SDU. When crossing a communication layer the SDU is not altered or modified. The focus of this requirement is exclusively on SDU transfer. The use of techniques that would entail use of several PDU at lower levels (such as segmentation of messages) are beyond the scope of this specification.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-060

OCS transmission of SDU

The (OCS) shall provide a service for stream-type SDU segmentation into packets.

Rationale: *Support of data transmission in the form of data streams that could also be used for big packets.*

Comment: *This requirements is expected to be tailored out for all implementation which would not support this mechanism*

Verification Method: RoD, T

SAVOIR-OCS-GEN-070

Support for synchronous and asynchronous SDU transmission

The (OCS) shall support synchronous and asynchronous SDU transmission.

Rationale: *Support of different transmission paradigms: full periodic (i.e., time-triggered) transmission model or event-based or sporadic model.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-080

OCS transmission of time-critical data as synchronous SDU

The (OCS) shall support time-critical data delivery for synchronous SDU transmission.

Rationale: *Support of transmission of time-critical SDU sent periodically, possibly with traffic optimization in case of configurable scheduling.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-090

OCS transmission of time-critical data as asynchronous SDU

The (OCS) shall support time-critical data delivery for asynchronous SDU transmission.

Rationale: *Not all SDU are necessarily generated at application level according to a predefined schedule. Some asynchronous data needing time-critical delivery could be generated (for instance, instrument/equipment mode change, configuration table update within a 1/8Hz time-slot every 1Hz, etc...).*

Verification Method: RoD, T

SAVOIR-OCS-GEN-100

Differentiation between time-critical and non-time-critical SDUs

The (OCS) shall ensure time-critical SDUs are identifiable from non-time-critical SDUs.

Rationale: *To enable different handling of the SDU from the host-system standpoint (interruptions, high priority, etc.) and to enable data segregation at least between time-critical and non-time-critical packets, routing and guardian mechanisms for schedule enforcement.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-110

OCS initiators

The (OCS) shall support one or more initiators on the same communication system.

Rationale: *In order to improve communication system performances and de-centralize the time-slot attribution management. The objective is to enable paradigms alternative to master-slave architecture such a routed de-centralized architecture with a multi-master approach compatible with both poll or push communication strategies.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-120

Allocation of communication resources

The (OCS) shall support the allocation of dedicated communication resources to enable specific communication between an emitter and a receiver.

Rationale: *To better distinguish different kinds of communications even when using the same medium (e.g., to discriminate time-critical transmission from others). Examples of resource that could be used is one of or a combination of:*

- an interface
- bandwidth
- time slot
- any elements that define a communication mean.

Comment: *This requirement could be implemented by using virtual channels but any equivalent concept could be developed in future. This will depend on the adopted technology, and other resources could be imagined.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-130

OCS enforcement of communication resource allocation

The (OCS) shall guarantee that when dedicated resources have been allocated to handle a specific communication, only the elements associated to this communication have access to these resources.

Rationale: *So, as to avoid unauthorized communications that may disrupt other communications. For instance, an error shall be reported if an initiator intends to access to another virtual channel or use a time-slot allocated to another user.*

Comment: *The elements associated to the communication being emitter(s), receiver(s) and controller(s) if any.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-140

OCS concurrent transactions with distinct initiators

The (OCS) shall permit concurrent transactions from distinct initiators.

Rationale: *concurrent transactions shall be permitted to share (for example) the same time-slot and potentially the same link: as the data exchange is predictable, the system engineer has enough input information to allocate bandwidths during the same slot and manage the potential collisions according to its allocation.*

Comment: *This requirements is expected to be tailored out for implementations based on e.g.,bus with master-slave protocols*

Verification Method: RoD, T

SAVOIR-OCS-GEN-150

OCS multiple transactions support

The (OCS) shall permit multiple transactions from an initiator within its allocated bandwidth within identified conditions.

Rationale: *this requirement aims at fostering an efficient usage of the available bandwidth, in conditions depending on the communication technology.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-160

OCS dynamic re-allocation of bandwidth

The (OCS) shall provide dynamic re-allocation of bandwidth not used by its owner channel without impacting the fulfilment of timing requirements related to other transfers.

Rationale: *this requirement targets an efficient usage of the available bandwidth.*

Comment: *As the bandwidth is re-allocated, this requirement does not enter in conflict with requirement SAVOIR-OCS-GEN-120. Once the bandwidth is allocated, it is not available anymore, therefore if a service requires extra bandwidth which might not be available.In such case, either the services will be not be authorized, work with degraded performances or a bandwidth un-allocation mechanism might be necessary. This should be tested during simulation, unit tests and integration to avoid instability. This requirement requires some non-trivial capabilities, so it is likely tailored out in some implementations.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-170

Support of guaranteed bounded latency

The (OCS) shall support communication with guaranteed bounded latency.

Rationale: *Guaranteed bounded latency is expected to cover most of the time-critical needs of satellite systems.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-180

Support of deterministic communication

The (OCS) support deterministic communication.

Rationale: *This requirement concerns the mechanisms and policy offered by the solution in order to achieve a deterministic communication (under the definition of determinism specified in this document). This requirement and SAVOIR-OCS-GEN-020 are distinct but linked: transfer time critical data implies the use of deterministic communication means, but deterministic communication can be used for non-time critical data. There is not necessarily reciprocity.*

Verification Method: RoD, T

SAVOIR-OCS-GEN-190

OCS communication resource use

The (OCS) shall enable the target to answer the initiator using the bandwidth allocated to the initiator, when a single medium is used for communication in both directions, unless a bandwidth is already allocated for each direction.

Rationale: A transaction might imply several exchanges in both directions (initiator to target and target to initiator). The bandwidth allocated to a medium is to ensure a full transaction over a medium, therefore there is no distinction on the sense the message is transmitted.

Comment: This requirement aims at providing a default behaviour to avoid blocking the communication (typically no bandwidth allocated, thus communication impossible). Any bandwidth allocated by the system supersedes this default behaviour.

Verification Method: RoD, T

SAVOIR-OCS-GEN-200

OCS time-distribution service

The (OCS) shall provide a time-distribution service.

Rationale: For performance and to reduce system complexity, a support of time-distribution at the lowest feasible level (network / protocol / service level), without support from applications is required.

Verification Method: RoD, T

SAVOIR-OCS-GEN-210

OCS transmission of SDU

The (OCS) shall provide an interruption distribution service.

Rationale: interruptions allow immediate high priority data transfer. If interruptions are a system requirement, they can be handled at communication or network level (and not only application level), for instance by providing a distributed interruption service at network level or using a pre-emptive communication system.

Comment: This requirement requires equivalent capabilities from the underlying communication technology, and is expected to be tailored out for those not offering them.

Verification Method: RoD, T

7.2 Quality of Service Requirements

Three level of Quality of Service are defined for the OCS depending on the service expected at receiver level. This service implies requirements on the communication system that are specified in this chapter:

- QoS 0 - At most once: This corresponds to a QoS class through which the receiver receives at most once each message sent by the sender (no duplication or retransmission of SDU is authorised).
- QoS 1 - At least once: This corresponds to a QoS class through which the receiver receives at least once each message sent by the sender (duplication/retransmission of SDU is authorised).
- QoS 2 - Exactly once. This corresponds to a QoS class through which the receiver receives exactly once each message sent by the sender (through a protocol mechanism, depending on the communication system).

The QoS aims at defining the level of certainty a packet will be delivered to its destination and is one of the characteristics used for the definition of the different classes of communication.

7.2.1 QoS 0 – "At most once"

SAVOIR-OCS-GEN-220

Support for QoS 0 – At Most once

The (OCS) shall implement "QoS 0 – At most once", by ensuring that the emitter will not emit a single SDU more than once.

Rationale: *There will be a single attempt to send the SDU; which will reach its destination if no failure occur in the communication system between sending and receiving host systems. If the medium is not ready or another packet will supersede or flush the current one, the packet is not received at all.*

Comment: *This QoS level is also known as "best effort".*

Verification Method: RoD, T

SAVOIR-OCS-GEN-230

Non-dependence of emitter logic

When implementing a communication protocol with "QoS 0 – At most once", the (OCS) shall ensure that the emitter logic of transmission is not bounded to the proper reception of SDUs it is sending.

Rationale: The emitter shall not take into consideration whether the packet has been properly received.

Verification Method: RoD, T

SAVOIR-OCS-GEN-240

Guaranteed non re-emission of SDU

When implementing a communication protocol with "QoS 0 – At most once", the (OCS) shall ensure that neither the receiver nor any element of the communication path will trigger a mechanism to re-emit any SDU.

Rationale: As the emitter does not necessarily store the sent SDU, retransmission is not possible. QoS 0 does not involve acknowledgement, handshake or equivalent mechanisms.

Verification Method: RoD, T

7.2.2 QoS 1 – "At least once"

This section defines the requirements related to "QoS 1 – At least once".

The following diagram summarises the transaction states for "QoS 1 – At least once" and provides a visual reminder of which requirement defined in the section addresses a transition from a state to another.

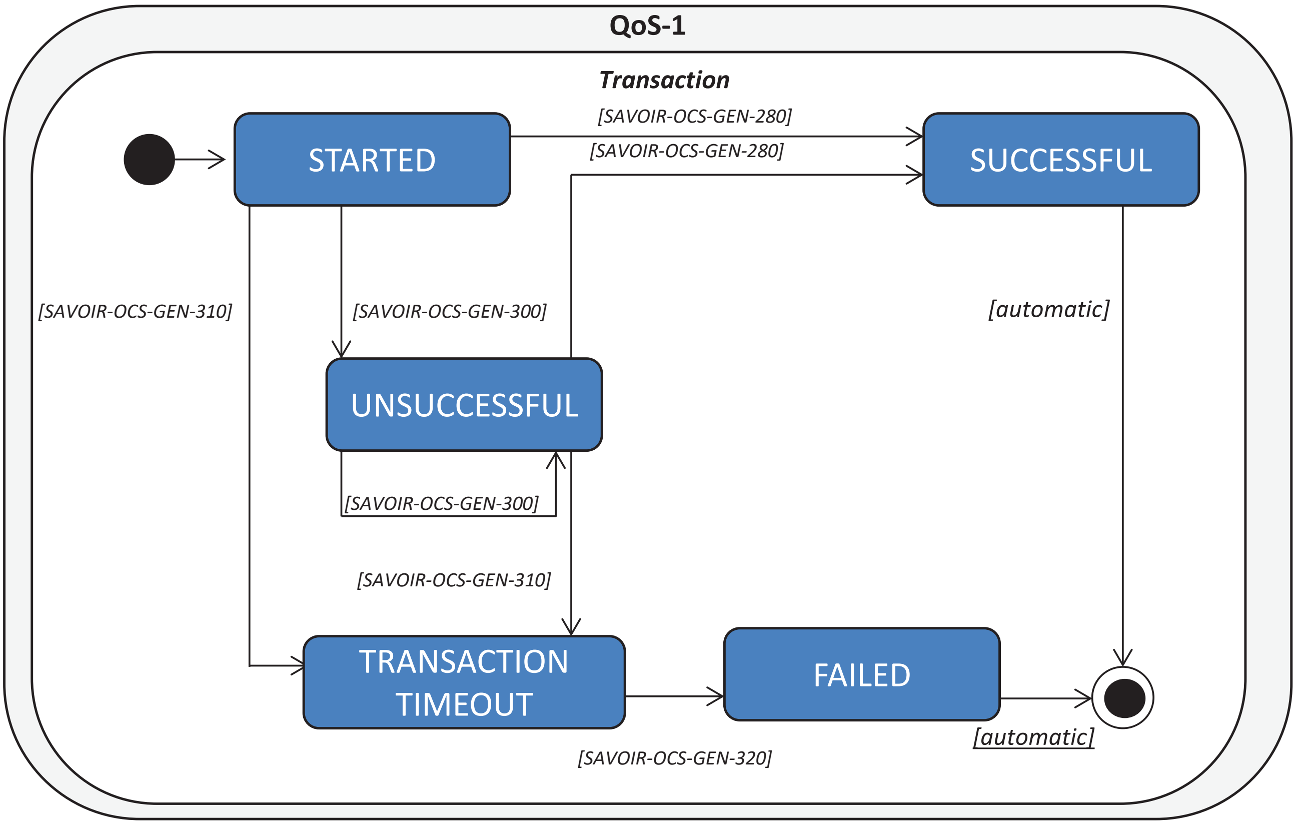

Figure 6: Transaction states and transitions for "QoS 1 – At least once"

Several means are possible to enable QoS 1 which implies duplication of SDUs either as inherent in the sending protocol implementation (e.g. (re-emission, systematic double/triple emission with majority voting or any other means) or due to unsuccessful transmission (reception of an explicit notification).

QoS 1 is characterised by a global timeout (to ensure the "at least once" semantics be verifiable in finite time).

An implementation for QoS 1 can add additional mechanisms (such as configurable number of maximum re-transmission attempts upon unsuccessful transmission). These were however considered design requirements and are not included in the specification.

SAVOIR-OCS-GEN-250

Support for QoS 1 – At least once

The (OCS) shall implement “QoS 1 – At least once”, by ensuring that the receiver receives a SDU at least once.

Rationale: There will be one or several attempts to send the SDU at the same time or after some timespan. Retry mechanisms can be implemented and ensure packet delivery to its destination end. Mechanisms such as packet sequence numbers may be used to discriminate between the packets received several times (sequence numbers allow to identify and sort the duplicates).

Verification Method: RoD, T

SAVOIR-OCS-GEN-260

QoS 1 states

At each a given time instant, a “QoS 1 – At least once” transaction can be in one and only one of the following states:

- Started
- Unsuccessful
- Transaction timeout
- Successful
- Failed

Rationale: Establish the logical states of the transaction.

Verification Method: RoD, T

SAVOIR-OCS-GEN-270

QoS 1 - acknowledgment of reception

When implementing a communication protocol with "QoS 1 – At least once", whenever the receiver receives a well-formed SDU, then it shall acknowledge reception.

Rationale: This can be implement in specific protocol mechanism (e.g., an SDU in the form of a packet) in different forms: either an actual acknowledgement SDU to communicate the error-free reception of a SDU, a non-acknowledgement transmitted only in case of error, or even a combination of both, for instance as often done in board-to-ground RF protocols). Because of this feature, the wording "acknowledge" or "acknowledgement" will refer to the action of confirming the good reception or not of a SDU, without detailing the corresponding mechanism.

Verification Method: RoD, T

SAVOIR-OCS-GEN-280

QoS 1 - successful transaction

When implementing a communication protocol with "QoS 1 – At least once", if the transaction is not in "failed" state and the receiver acknowledges reception of a sent SDU, then the transaction is considered as successful.

Rationale: Provide a success criterion for a transaction (an acknowledgement SDU or absence of failure signalling after a time-out).

Verification Method: RoD, T

SAVOIR-OCS-GEN-290

QoS 1 - OCS non-acknowledgment

When implementing a communication protocol with "QoS 1 – At least once", whenever the receiver receives an anomalous SDU, then it shall signal it through a non-acknowledgement of reception (flag or non-acknowledgement or other).

Rationale: Counterpart to SDU acknowledgement, once again without enforcing a specific mechanism: a non-acknowledgement can be an actual SDU or an absence of acknowledgement depending on the protocol strategy.

Verification Method: RoD, T

SAVOIR-OCS-GEN-300

QoS 1 – Unsuccessful transaction

When implementing a communication protocol with "QoS 1 – At least once", if the transaction is neither in failed state nor in timeout state and the receiver did not acknowledge the reception of the SDU, then the transaction is considered as unsuccessful.

Rationale: Provide a criterion to consider a transaction unsuccessful and possibly trigger a retransmission.

Verification Method: RoD, T

SAVOIR-OCS-GEN-310

QoS 1 – Transaction timeout

When implementing a communication protocol with "QoS 1 – At least once", if in the scope of a transaction neither an acknowledgment of reception nor a non-acknowledgement of reception of the sent SDU is produced within a finite timespan <OCS QoS-1 transaction timeout>, then the transaction shall be considered in "transaction timeout".

Rationale: This requirement covers the fail silent error case (depending on the protocol, the acknowledgement or non-acknowledgment is not sent on the receiver end), and the loss of the SDU or acknowledgement packet (if foreseen by the protocol) in an intermediary point (router, switch, bridge or else).

Comment: the length of the timespan is implementation dependent.

Verification Method: RoD, T

SAVOIR-OCS-GEN-320

QoS 1 – Failed transaction on timeout occurrence

When implementing a communication protocol with "QoS 1 – At least once", if a "transaction timeout" occurs, then the transaction shall be considered as "failed".

Rationale: This requirement provides a policy to address the transaction timeout case. The transaction timeout for "QoS 1 – At least once" shall be then considered as global to the transaction.

Verification Method: RoD, T

SAVOIR-OCS-GEN-330

QoS 1 – No re-transmission in timeout or failed state

The (OCS) shall ensure that no SDU for the transaction shall be sent or retransmitted when the transaction is in “Transaction Timeout” or “Failed” state.

Rationale: Prevent message (re)-transmission when guarantees on the delivery of the message cannot be ensured anymore.

Verification Method: RoD, T

SAVOIR-OCS-GEN-340

QoS 1 – Reaction to failure state occurrence

Whenever a transaction is considered as “Failed”, a flag shall be raised.

Rationale: In case of failure of transmission by the (OCS), a flag has to be raised. The anomaly can be mapped to an FDIR event according to the FDIR mechanisms possibly in place to manage this error case.

Comment: the notification process is implementation dependent, it can be through a dedicated SDU, service call or any other action or mechanism.

Verification Method: RoD, T

7.2.3 QoS 2 – "Exactly once"

This section defines the requirements related to "QoS 2 – Exactly once".

The following diagram summarises the transaction states for "QoS 2 – Exactly once" and a visual reminder of which requirement defined in the section addresses a transition from a state to another.

QoS 2 is characterized by a global timeout (to make the "exactly once" semantics verifiable in a finite amount of time).

An implementation for QoS 2 can add additional mechanisms (such as configurable number of maximum re-transmission attempts upon unsuccessful transmission). These mechanisms are considered as design requirements, and are not included in the specification.

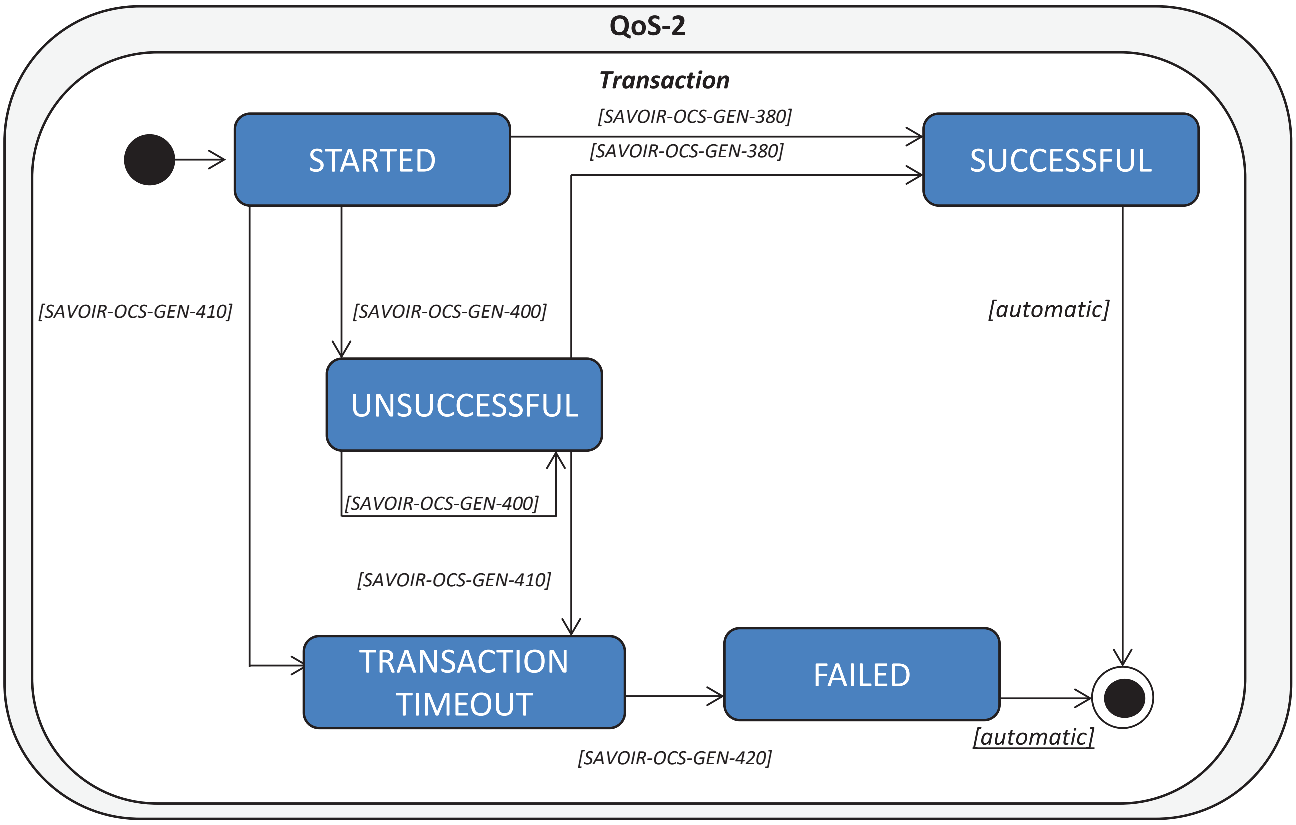

Figure 7: Transaction states and transitions for "QoS 2 - Exactly once "

SAVOIR-OCS-GEN-350

Support for QoS 2 – "Exactly once"

The (OCS) shall implement "QoS 2 – Exactly once", by ensuring that the receiver receives each SDU exactly once.

Rationale: There will be one or several attempts to send the SDU at the same time or after some timespan. The difference with QoS-1 is that whatever the chosen mechanism, the receiver will receive exactly once the SDU. This can be used with highly critical command like those used for reconfiguration.

Verification Method: RoD, T

SAVOIR-OCS-GEN-360

QoS 2 states

At each a given time instant, a "QoS 2 – Exactly once" transaction can be in one and only one of the following states:

- Started
- Unsuccessful
- Transaction timeout
- Successful
- Failed.

Rationale: Establish the logical states of the transaction.

Verification Method: RoD, T

SAVOIR-OCS-GEN-370

QoS 2 – OCS acknowledgment

When implementing a communication protocol with "QoS 2 – Exactly once", whenever the receiver receives a well-formed SDU, then it shall acknowledge its reception.

Rationale: Mechanism (typically a packet) to communicate acknowledgment of reception or success-silent process, for instance through the signalling of failed transactions only).

Verification Method: RoD, T

SAVOIR-OCS-GEN-380

QoS 2 – successful transaction

When implementing a communication protocol with "QoS 2 – Exactly once", if the transaction is not in "failed" state and the receiver acknowledges reception of the sent SDU, then the transaction shall be considered as successful.

Rationale: Provide a success criterion for a transaction.

Verification Method: RoD, T

SAVOIR-OCS-GEN-390

QoS 2 - OCS non-acknowledgment

When implementing a communication protocol with "QoS 2 – Exactly once", whenever the receiver receives an anomalous SDU, then it shall signal it through a non-acknowledgement of reception (flag or non-acknowledgement or other).

Rationale: Mechanism (typically an SDU in the form of a packet) to communicate non-acknowledgment of reception.

Verification Method: RoD, T

SAVOIR-OCS-GEN-400

QoS 2 – Unsuccessful transaction

When implementing a communication protocol with "QoS 2 – Exactly once", if the transaction is neither in failed state nor in timeout state, and the receiver did not acknowledge reception of the sent SDU, then the transaction shall be considered as unsuccessful.

Rationale: Provide a fail criterion for a transaction.

Verification Method: RoD, T

SAVOIR-OCS-GEN-410

QoS 2 –Transaction timeout

When implementing a communication protocol with “QoS 2 – Exactly once”, if in the scope of a transaction neither an acknowledgment of reception nor a non-acknowledgement of reception of the sent SDU is produced within a finite timespan <OCS QoS-2 transaction timeout>, then the transaction shall be considered in “transaction timeout”.

Rationale: Provide a timeout fail criteria for a transaction.

Comment: The length of the timespan is implementation-dependent.

Verification Method: RoD, T

SAVOIR-OCS-GEN-420

QoS 2 – Failed transaction on timeout occurrence

When implementing a communication protocol with “QoS 2 – Exactly once”, if a “transaction timeout” occurs, then the transaction shall be considered as failed.

Rationale: This requirement provides a policy to consider the transaction timeout a sufficient reason to consider the transaction failed. The timeout for “QoS 2 – Exactly once” shall be then considered as global to the transaction. The use of timeout to consider a transaction unsuccessful is necessary to make the intended exactly-once semantics verifiable and avoid the “Two Generals’ Problems” or its “Byzantine Generals’ Problem” generalization (e.g., in case of multicast), which is proved to be unsolvable. Other protocols can choose to implement QoS 2 without any retransmission through duplication/triplication of SDUs and voting. This requirement would still apply.

Verification Method: RoD, T

SAVOIR-OCS-GEN-430

QoS 2 – Reaction to failure state occurrence

Whenever a transaction is considered as "Failed", a flag shall be raised.

Rationale: *In case of failure of transmission, a flag has to be raised. The anomaly can be mapped to an FDIR event according to the FDIR mechanisms possibly in place to manage this error case.*

Comment: *The notification process is implementation dependent, it can be through a dedicated SDU, service call or any other action or mechanism*

Verification Method: RoD, T

SAVOIR-OCS-GEN-440

QoS 2 –Transaction monitoring

When implementing a communication protocol with "QoS 2 – Exactly once", the (OCS) shall ensure that every transaction is monitored and it is carried on until successful completion or raising of a flag for the failed state.

Rationale: *The "failed" condition is considered a necessary condition to close a transaction with an error.*

Verification Method: RoD, T

7.3 Class of communication requirements

The SAVOIR (OCS) communication classes have been defined in order to classify communication traffic of current and future avionics systems according to their communication needs.

The definition took into account needs of existing operational missions as well as perspective mission still in early analysis phase (e.g., phase A).

The definition of those classes therefore is not bound to a single mission but aims at covering a large domain of future missions.

The classification is performed by combining the following aspects:

- Frequency: it indicates the expected communication frequency for a communication, in case it is expected to exhibit a periodic behavior.
- Size: it indicates the expected size of single data exchange (without accounting for any overhead caused by the communication technology or the communication protocol).

- Required level of determinism: whether no guarantees at all, guaranteed bounded latency or determinism are required for the communication exchange;
- Required QoS: whether an at most once (QoS 0), at least once (QoS 1) or exactly one (QoS 2) guarantee is required because of the specific nature of the transmitted SDU or application needs.
- Timestamp: whether a timestamp (relative or absolute) is mandatory or not.

The goal is not to define all possible classes of communications according to the combinatorial of the aspects above, but to single out just the classes that are meaningful according to the analysis of mission / avionics needs.

A summary of the classes is presented below:

Class	Freq of data exchange scale (Hz)		QoS			Data Rate scale		Jitter	Latence	Level of determism			Timestamp
	Min	Max	0	1	2	Min	Max	ms	ms	None	guaranteed bounded latency	deterministic	Mandatory / Optional
1	0,1	1	X	X		100 bits/s	10 kbits/s	10	10		X		Optional
2-a	4	32		X	X		1 Mbits /s	5-10	10			X	Optional
2-b	4	32		X	X		1 Mbits /s	5-10	10		X		Mandatory
3	8	10			X		250 kbits /s	5	10			X	Optional
4	0,1	1	X	X		100 Mbits/s		up to 100	up to 100	X	X		Optional
5-a	10	1000		X	X		3 Mbits/s	0,5 -1	0,5			X	Optional
5-b	10	1000		X	X		3 Mbits/s	0,5 -1	0,5		X		Mandatory
6	1	10		X	X	100 Mbits/s		2	10			X	Mandatory
7	1	10	X	X		100 bits/s	1 kbits/s	1	2			X	Optional

Figure 8: Summary of SAVOIR (OCS) Communication Classes

The requirements are from the point of view of a user of the communication system. They point out the data to be exchanged between user applications. They should therefore be interpreted as user data rate rather than transmission data rate.

The communication classes are defined as follows:

Class 1: Low frequency, small / medium data size, non-time critical

This class is characterized by low frequency of message exchange (~1Hz or lower frequency) and small size of messages (10-100bits per message).

The level of determinism that is required is best effort or guaranteed bounded latency.

Time stamping is optional.

Acquisition data from sensors used in low rate AOCS cycles, Payload HK telemetry or data from processes with slow dynamics (such as thermal acquisitions) are example of such class.

Class 2: Medium frequency, Medium data size, time critical, medium QoS

This class is characterized by medium frequency of message exchange (4-32Hz), low or medium data size of messages (in the lower cases 10 bits – 30Kbits, but generalised to 1 Mbit/s).

This class mostly gathers medium frequency sensors such as Star Trackers and GNSS, for which occasional deviations from the expected message traffic profile could be tolerated without severe performance degradation.

This class requires either communication determinism or guaranteed bounded latency complemented with timestamp (as specified by subclass 2-a or 2-b respectively).

At least once is considered as the minimum expected support for QoS.

Class 3: Medium frequency, Medium data size, time critical, high QoS

This class is similar to Class 2.

It is characterized by medium frequency of message exchange (8-10Hz), low or medium data size of messages (10 bits – 30Kbits, generalized up to 250 kbits/s).

A high level of determinism is required, and combined with high QoS requirements (exactly once).

This class gathers, for example, medium frequency actuators, such as thruster assemblies, reaction wheels and control gyros. The higher QoS is linked to the fact that contrarily to Class 2, deviations from the expected message traffic profile could lead to light or severe mission degradation (e.g., receiving twice thruster commands with degradation of equipment or incorrect guidance profile).

Time stamping is optional considering the required communication determinism.

Class 4: Low frequency, Big data size, non-time critical, low QoS

Class 4 represents low frequency exchanges of big quantity of non-time-critical data.

Best effort or guaranteed bounded latency would be sufficient for this class.

In this case, the sizing aspect is therefore the amount of data rather than requirements for its delivery.

This class gathers, for example, payload science traffic.

Time stamping is optional.

Class 5: High frequency, Medium data size, time critical, medium QoS

This class is a more stringent version of Class 2.

As per class 2, a subclass (5-a) with high level of determinism is defined, combined with stringent QoS requirements as in class 2-a, yet the frequency of data exchanges can be quite high (e.g., 1000Hz, which is not unheard in other domains, yet not used on current spacecrafts).

Alternatively, a subclass (5-b) with guaranteed bounded latency with mandatory timestamp is expected to be feasible for the needs of the applications represented by this class.

The sizing factor for this class is therefore the frequency of exchanges combined with medium / high requirements on determinism.

Class 6: Medium frequency, Big data size, time critical, medium QoS

Class 6 represents data exchanges of medium frequency, with a big or extremely big quantity of data (e.g., ~40Mbits), with determinism requirements.

This class of data exchanges is unheard of in current platform avionics.

This class gathers, for example, navigation cameras whose data can be used directly in an AOCS loop.

The sizing factors for this class are then the medium frequency, combined with very big quantity of data and high determinism, as data is used in AOCS loops.

Time stamping is made mandatory considering the time criticality.

Class 7: Medium frequency, Small data size, time critical, low jitter, high QoS

Finally, class 7 is dedicated to time synchronization messages that would be used to synchronize software applications on end systems.

(We are not therefore addressing bus or network synchronization in this class).

The sizing factors for this class are the determinism, high QoS and extremely low jitter for the exchanges (e.g., for future avionics, in the order of few microseconds).

The timestamp is made optional as the cargo itself could be smaller than the timestamp (7-8 octets in CUC/CDS format). The size of the frame shall not be a drawback for determinism implementation.

The requirements in the following document sections correspond to the implementation of such classes by the On-board Communication System.

7.3.1 Class of Communication 1

SAVOIR-OCS-CAP-450

Support for Communication Class 1

The (OCS) shall support Communication Class 1.

Rationale: Low frequency, small / medium data size, non-time critical

Verification Method: RoD, T

SAVOIR-OCS-CAP-460

Class of Communication 1 - QoS

Class of Communication 1 shall support:

- "QoS 0 – At most once"
- and "QoS 1 – At least once".

Rationale: Leave the freedom to choose the most appropriate QoS level according to the application needs.

Verification Method: RoD, T

SAVOIR-OCS-CAP-470

Class of Communication 1 – Guaranteed Bounded Latency

The class of communication 1 shall ensure communication with "Guaranteed Bounded Latency".

Verification Method: RoD, T

SAVOIR-OCS-CAP-480

Class of Communication 1 - Frequency

The class of communication 1 shall support a communication cycle corresponding to a frequency within a 0,1 Hz – 1Hz scale.

Rationale: So as to respect frequency defined for Class 1.

Verification Method: RoD, T

SAVOIR-OCS-CAP-490

Class of Communication 1 – Data rate

The class of communication 1 shall support data rate communication within a 0,1-10 kbits/s range.

Verification Method: RoD, T

SAVOIR-OCS-CAP-500

Class of Communication 1 - Jitter

The class of communication 1 shall ensure a communication jitter of less than 10ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-510

Class of Communication 1 - Latency

The class of communication 1 shall ensure a communication latency of less than 10ms.

Verification Method: RoD, A, T

7.3.2 Class of Communication 2

Class of communication 2 is divided in 2 subclasses: 2-a and 2-b. This section defines the common characteristics and the specificities of those subclasses.

SAVOIR-OCS-CAP-520

Support for Communication Class 2

The (OCS) shall support at least one between Communication Class 2-a and 2-b.

Verification Method: RoD, T

SAVOIR-OCS-CAP-530

Class of Communication 2a - QoS

The class of communication 2-a shall support at least one among:

- "QoS 1 – At least once"
- and "QoS 2 – Exactly once".

Verification Method: RoD, T

SAVOIR-OCS-CAP-540

Class of Communication 2-a - Determinism

The class of communication 2-a shall ensure deterministic communication.

Verification Method: RoD, T

SAVOIR-OCS-CAP-550

Class of Communication 2-b - QoS

The class of communication 2-b shall support:

- "QoS 1 – At least once"
- and "QoS 2 – Exactly once".

Rationale: Leave the freedom to choose the most appropriate QoS level according to the application needs.

Verification Method: RoD, T

SAVOIR-OCS-CAP-560

Class of Communication 2-b – Guaranteed bounded latency

The class of communication 2-b shall ensure communication with "Guaranteed bounded latency".

Verification Method: RoD, T

SAVOIR-OCS-CAP-570

Class of Communication 2-a and 2-b - Frequency

The class of communication 2-a and 2-b shall support communication cycles corresponding to a frequency within a 4 Hz – 32 Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-580

Class of Communication 2-a and 2-b – Data rate

The class of communication 2-a and 2-b shall support data rate communication up to 1 Mbits/s.

Verification Method: RoD, T

SAVOIR-OCS-CAP-590

Class of Communication 2-a and 2-b - Jitter

The class of communication 2-a and 2-b shall ensure a communication jitter of less than 10ms.

Comment: This is a minimum requirement. For Class 2 it is advised to have a jitter of less than 5ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-600

Class of Communication 2-a and 2-b - Latency

The class of communication 2-a and 2-b shall ensure a communication latency of less than 10ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-610

Class of Communication 2-b - Timestamp

The class of communication 2-b shall support the implementation of a time stamping mechanism.

Comment: Considered important for 2-b. For 2-a timestamp is considered not strictly necessary, as the communication is already deterministic.

Verification Method: RoD, T

7.3.3 Class of Communication 3

SAVOIR-OCS-CAP-620

Support for Communication Class 3

The (OCS) shall support Communication Class 3.

Verification Method: RoD, T

SAVOIR-OCS-CAP-630

Class of Communication 3 - QoS

The class of communication 3 shall support "QoS 2 – Exactly once".

Verification Method: RoD, T

SAVOIR-OCS-CAP-640

Class of Communication 3 – Deterministic Communication

The class of communication 3 shall ensure deterministic communication.

Verification Method: RoD, T

SAVOIR-OCS-CAP-650

Class of Communication 3 – Frequency

The class of communication 3 shall support communication cycle corresponding to a frequency within a 8 Hz – 10Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-660

Class of Communication 3 – Data rate

The class of communication 3 shall support data rate communication up to 250 kbits/s.

Verification Method: RoD, T

SAVOIR-OCS-CAP-670

Class of Communication 3 – Jitter

The class of communication 3 shall ensure a communication jitter of less than 5ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-680

Class of Communication 3 – Latency

The class of communication 3 shall ensure a communication latency of less than 10ms.

Verification Method: RoD, A, T

7.3.4 Class of Communication 4

SAVOIR-OCS-CAP-690

Support for Communication Class 4

The (OCS) shall support Communication Class 4.

Verification Method: RoD, T

SAVOIR-OCS-CAP-700

Class of Communication 4 – QoS

The class of communication 4 shall support:

- "QoS 0 – At most once"
- and "QoS 1 – At least once".

Rationale: Leave the freedom to choose the most appropriate QoS level according to the application needs.

Verification Method: RoD, T

SAVOIR-OCS-CAP-710

Class of Communication 4 – Guaranteed bounded latency

The class of communication 4 shall ensure communication with "Guaranteed bounded latency".

Comment: This is however to be intended as recommendation. If the implementation does not support such guarantees, then communication class 4 will be carried out with no timing guarantees, as this is not considered essential for much of the data that would use this type of class.

Verification Method: RoD, T

SAVOIR-OCS-CAP-720

Class of Communication 4 – Frequency

The class of communication 4 shall support communication cycle corresponding to a frequency within a 0,1 Hz – 1Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-730

Class of Communication 4 – Data rate

The class of communication 4 shall support data rate communication of at least 100 Mbits/s.

Verification Method: RoD, T

SAVOIR-OCS-CAP-740

Class of Communication 4 – Jitter

The class of communication 4 shall ensure a communication jitter of less than 100ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-750

Class of Communication 4 – Latency

The class of communication 4 shall ensure a communication latency of less than 100ms.

Verification Method: RoD, A, T

7.3.5 Class of Communication 5

Class of communication 5 is divided in 2 subclasses: 5-a and 5-b. This section defines the common characteristics and the specificities of those subclasses.

SAVOIR-OCS-CAP-760

Support for Communication Class 5

The (OCS) should support at least one between class of communication 5-a and 5-b.

Verification Method: RoD, T

SAVOIR-OCS-CAP-770

Class of Communication 5-a – QoS

The class of communication 5-a shall support at least one among:

- "QoS 1 – At least once"
- and "QoS 2 – Exactly once".

Verification Method: RoD, T

SAVOIR-OCS-CAP-780

Class of Communication 5-a – Deterministic Communication

The class of communication 5-a shall ensure deterministic communication.

Verification Method: RoD, T

SAVOIR-OCS-CAP-790

Class of Communication 5-b – QoS

The class of communication 5-b shall support:

- "QoS 1 – At least once"
- and "QoS 2 – Exactly once.

Rationale: Leave the freedom to choose the most appropriate QoS level according to the application needs.

Verification Method: RoD, T

SAVOIR-OCS-CAP-800

Class of Communication 5-b – Guaranteed bounded latency

The class of communication 5-b shall ensure communication with “Guaranteed bounded latency”.

Verification Method: RoD, T

SAVOIR-OCS-CAP-810

Class of Communication 5 – Frequency

The class of communication 5-a and 5-b shall support communication cycle corresponding to a frequency within a 10 Hz – 1000 Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-820

Class of Communication 5 – Data rate

The class of communication 5-a and 5-b shall support data rate communication up to 3,0 Mbits/s.

Verification Method: RoD, T

SAVOIR-OCS-CAP-830

Class of Communication 5 – Jitter

The class of communication 5-a and 5-b shall ensure a communication jitter of less than 1ms.

Comment: It would be however recommended to ensure a communication jitter of less than 0,5 ms

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-840

Class of Communication 5 – Latency

The class of communication 5-a and 5-b shall ensure a communication latency of less than 0,5ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-850

Class of Communication 5-b – Timestamp

The class of communication 5-b shall support the implementation of a time stamping mechanism.

Rationale: This complements the use of a guaranteed bounded latency communication.

Verification Method: RoD, T

7.3.6 Class of Communication 6

SAVOIR-OCS-CAP-860

Support for Communication Class 6

The (OCS) shall support Communication Class 6.

Verification Method: RoD, T

SAVOIR-OCS-CAP-870

Class of Communication 6 – QoS

The class of communication 6 shall support at least one among:

- "QoS 1 – At least once"
- and "QoS 2 – Exactly once".

Rationale: Leave the freedom to choose the most appropriate QoS level according to the application needs.

Verification Method: RoD, T

SAVOIR-OCS-CAP-880

Class of Communication 6 – Deterministic Communication

The class of communication 6 shall ensure deterministic communication.

Verification Method: RoD, T

SAVOIR-OCS-CAP-890

Class of Communication 6 – Frequency

The class of communication 6 shall support communication cycle corresponding to a frequency within a 1 Hz – 10Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-900

Class of Communication 6 – Data rate

The class of communication 6 shall support data rate communication of at least 100 Mbits/s.

Verification Method: RoD, T

SAVOIR-OCS-CAP-910

Class of Communication 6 – Jitter

The class of communication 6 shall ensure a communication jitter of less than 2ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-920

Class of Communication 6 – Latency

The class of communication 6 shall ensure a communication latency of less than 10ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-930

Class of Communication 6 – Timestamp

The class of communication 6 shall support the implementation of a time stamping mechanism.

Rationale: the application needs originating this class may require a high precision in data timing.

Verification Method: RoD, T

7.3.7 Class of Communication 7

SAVOIR-OCS-CAP-940

Support for Communication Class 7

The (OCS) shall support Communication Class 7.

Verification Method: RoD, T

SAVOIR-OCS-CAP-950

Class of Communication 7 – QoS

The class of communication 7 shall support “QoS 0 – At most once”.

Verification Method: RoD, T

SAVOIR-OCS-CAP-960

Class of Communication 7 – Additional QoS

The class of communication 7 shall support “QoS 1 – At least once”.

Rationale: A QoS 1 can be appropriate for some implementations, but this can be tailored out if unnecessary.

Verification Method: RoD, T

SAVOIR-OCS-CAP-970

Class of Communication 7 – Deterministic Communication

The class of communication 7 shall ensure deterministic communication.

Verification Method: RoD, T

SAVOIR-OCS-CAP-980

Class of Communication 7 – Frequency

The class of communication 7 shall support communication cycle corresponding to a frequency within a 1 Hz – 10Hz scale.

Verification Method: RoD, T

SAVOIR-OCS-CAP-990

Class of Communication 7 – Data rate

The class of communication 7 shall support data rate communication in a 0,1-1,0 kbits/s range.

Verification Method: RoD, T

SAVOIR-OCS-CAP-1000

Class of Communication 7 – Jitter

The class of communication 7 shall ensure a communication jitter of less than 1ms.

Verification Method: RoD, A, T

SAVOIR-OCS-CAP-1010

Class of Communication 7 – Latency

The class of communication 7 shall ensure a communication latency of less than 2ms.

Verification Method: RoD, A, T

8 COMMUNICATION SYSTEM REDUNDANCY REQUIREMENTS

The following requirements address the type of redundancy support for the communication system.

SAVOIR-OCS-RED-010

Support for cold-redundancy

The (OCS) shall support the implementation of a cold-redundant communication system architecture.

Rationale: The (OCS) paradigm shall be applicable in cold-redundant communication systems, in order to design a fault-tolerant architecture.

Verification Method: RoD, T

SAVOIR-OCS-RED-020

Support for warm redundancy

The (OCS) shall support the implementation of a warm-redundant communication system architecture.

Rationale: The (OCS) paradigm shall support the possibility of relying on a warm-redundant communication system.

Verification Method: RoD, T

SAVOIR-OCS-RED-030

Support for hot redundancy

The (OCS) shall support the implementation of a hot-redundant communication system architecture.

Rationale: The (OCS) paradigm shall support the use of architectures that are based on hot redundancy.

Verification Method: RoD, T

9 COMMUNICATION SYSTEM ERROR HANDLING AND FDIR REQUIREMENTS

This chapter concerns the requirements related to error handling and FDIR for the On-board Communication System.

SAVOIR-OCS-FDIR-010

FDIR mechanisms

The (OCS) shall provide mechanisms for error detection at datalink, network and transport level.

Rationale: In this chapter we assume the OSI model with the following layers: 1) physical; 2) datalink; 3) network; 4) transport; 5) session; 6) presentation; 7) application. The mechanism are used to detect errors at each appropriate level: e.g., bandwidth usage, communication health status, node status, etc....

Verification Method: RoD, T

SAVOIR-OCS-FDIR-020

Reporting of errors at datalink level

Repeated occurrences of errors at datalink level shall be reported to a dedicated entity.

Rationale: it is expected that the datalink layer itself will manage sporadic occurrences of errors through dedicated mechanisms (e.g., error control codes in the form of parity bits). It is considered instead that repeated occurrences of such errors shall be escalated to be addressed at higher level.

Comment: The entity such information is reported to depends on the network or bus topology or functioning (whether there is one or more masters, a guardian or else is implementation dependent). It is either the local host or a centralized network manager, or (ideally) both

Verification Method: RoD, T

SAVOIR-OCS-FDIR-030

Trigger for error reporting at datalink level

The number of occurrences of errors at datalink level <OCS Datalink Repeated Error Threshold> that triggers an error report shall be configurable.

Rationale: To adjust to link quality, mission phases with increased amount of errors.

Verification Method: RoD, T

SAVOIR-OCS-FDIR-040

Reporting of errors at network level

Errors at network level shall be reported to a dedicated entity.

Rationale: observability and diagnostic capability is required to operate networks properly. This dedicated entity can be a register accessible by the communication medium, by external communication links or even be connected to a distributed interrupts broadcast mechanism. The error to be reported include at least: routing errors, packet forwarding errors, node health status.

Comment: The entity such information is reported to depends on the network or bus topology or functioning (whether there is one or more masters, a guardian or else is implementation dependent).

Verification Method: RoD, T

SAVOIR-OCS-FDIR-050

Reporting of errors at transport level

Errors at transport level shall be reported to a dedicated entity.

Rationale: Errors at transport level include e.g., the triggering of retransmission due to timeout, the triggering of retransmission due to reception of a non-acknowledge packet. No specific means to report such errors is imposed (it could be a reporting per-occurrence of the error, a statistic reporting on a time window, according to the needs of the recovery policy).

Comment: The entity such information is reported to depends on the network or bus topology or functioning (whether there is one or more masters, a guardian or else is implementation dependent).

Verification Method: RoD, T

SAVOIR-OCS-FDIR-060

Trigger for error reporting at transport level

The number of occurrences of errors at transport level <OCS Transport Repeated Error Threshold> that triggers an error report shall be configurable.

Rationale: To adjust to link quality, mission phases with increased amount of errors.

Verification Method: RoD, T

SAVOIR-OCS-FDIR-070

Anomalous packet detection

The (OCS) shall rely on a mechanism to detect anomalous packets.

Rationale: anomalous according to protocol specificities or alteration of its cargo. It is expected that this level of checks is implemented in lower layers (i.e., communication protocols).

Verification Method: RoD, T

SAVOIR-OCS-FDIR-080

Reporting of Errors at Network Level

Reporting of errors originated at network layer shall include at least the following information:

- the origin and / or destination of the packet (mandatory)
- the cause of the error, if known (optional)
- the transmission time (optional)

Rationale: It can be used to generate statistics (through a dedicated service for instance) or be the trigger and the base of FDIR mechanism. According to the protocol in use, it could not be possible to known both the origin and destination of the packet, yet at least one of them is known.

Verification Method: RoD, T

SAVOIR-OCS-FDIR-090

Reporting of Errors at Transport Level

Reporting of errors originated at transport layer shall include at least the following information:

- the origin and / or destination of the packet (mandatory),
- the number of re-emission of packets for the transaction (mandatory),
- the number of non-acknowledgment messages received by the sender (optional),
- the cause of the error, if known (optional),
- the transmission time (optional).

Rationale: It can be used to allow to generate statistics (though a dedicated service for instance) or be the trigger and the base of FDIR mechanism.

Verification Method: RoD, T

SAVOIR-OCS-FDIR-100

Detection of duplicated packets

Duplicated packets shall be detected by the receiver and a single instance must be processed.

Rationale: The receiver side shall be robust to arrival of duplicated packets.

Comment: A duplicated packet can be result of a normal protocol behavior (e.g., for a communication based on "QoS 1 – at least once" for instance). Detection of duplicated packet can be based on sequence number, for instance, or other mechanism. The cargo of the packet is not a proper way to discriminate whether a packet has been duplicated (a sensor can measure twice in a row the same value).

Verification Method: RoD, T

SAVOIR-OCS-FDIR-110

Reporting of missing packet

Missing packets detected by the receiver shall be reported either to the source or to the local host.

Rationale: A packet that never reached its destination can characterize a communication system failure (node malfunction, routing function unreliable…).

Comment: In case of acknowledged transactions, this requirement is obviously implemented. In other cases, packet loss can be detected through the sequence numbering or comparing the number of initiated transactions by the sender and received packets (erroneous or not) by the receiver. In the worst case, it is acknowledged that a lost packet may be detected at receiver side quite long time after packet loss (e.g., only when a subsequent packet is received to check the sequence number, which can occur after an arbitrary long timespan). The entity such information is to be reported to depends on the network or bus topology or functioning (whether there is one or more master, a guardian or else is implementation dependent)

Verification Method: RoD, T

10 SYSTEM-LEVEL COMMUNICATION REQUIREMENTS

This section aims at defining the requirements of entities interfaced with the On-board Communication System. Those entities would be part of the communication system (as they may trigger action regarding the overall functioning of the communication system). It is important that their interfaces and mechanism are appropriately defined to benefit from the OCS without altering the performances and QoS established via this OCS Specification.

SAVOIR-OCS-SYS-010

Dedicated Entity for high-level management functions

The (OCS) shall provide a dedicated entity ensuring one or several of the following functions:

- Bandwidth allocation
- (OCS) FDIR management
- Error monitoring

Rationale: *This entity will act as supervisor or manager and trigger high-level actions according to the (OCS) behaviour and health. This entity will be able to interact with higher-level logical components.*

Comment: *The dedicated entity could be required only for certain type of architectures and mission types, so the requirement can be tailored out if the effort to implement is considered disproportionate for some missions.*

Verification Method: RoD, T

SAVOIR-OCS-SYS-020

Solicited retrieval of monitoring information

End-points of the communication system shall send health status and information only after being solicited by the entity monitoring of the (OCS).

Rationale: *The information has to be collected from the monitored nodes intentionally. Error logs of each node shall not be autonomously transmitted in an unsolicited manner, as this could create communication traffic side effects.*

Verification Method: RoD, T