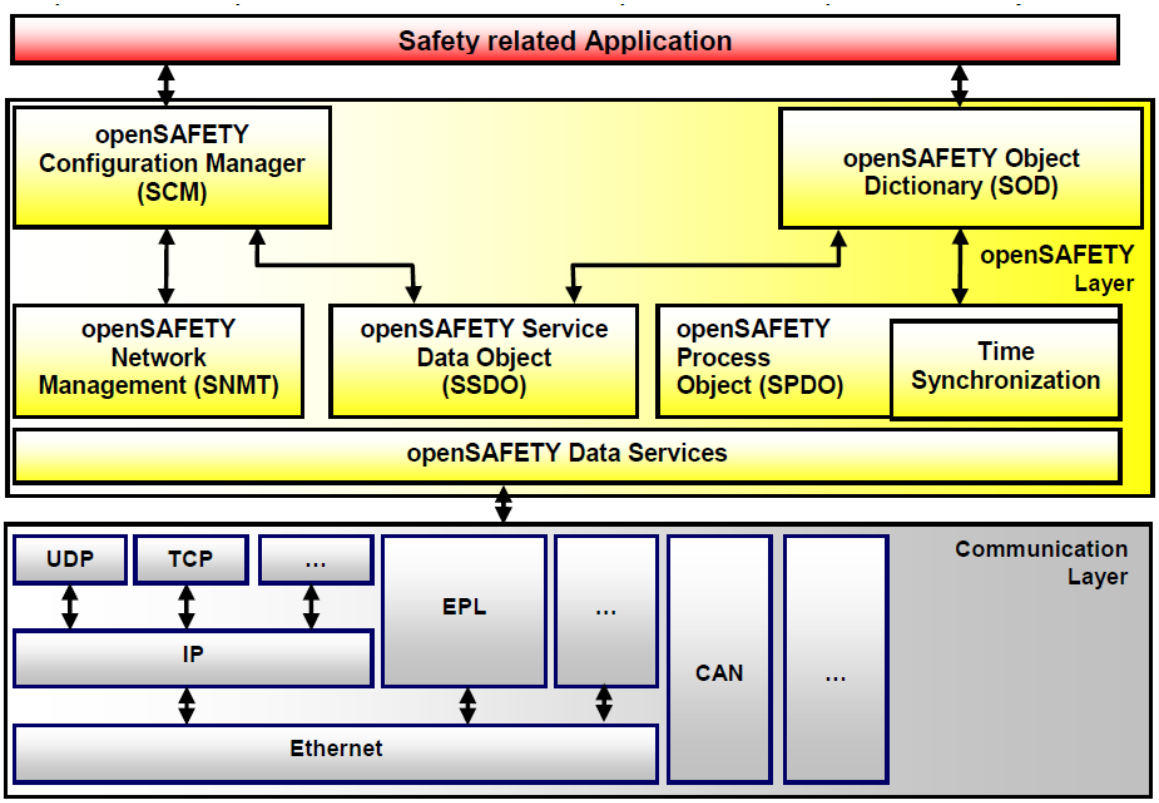
openSAFETY over UDP

Exported from Confluence on 2024 January 24

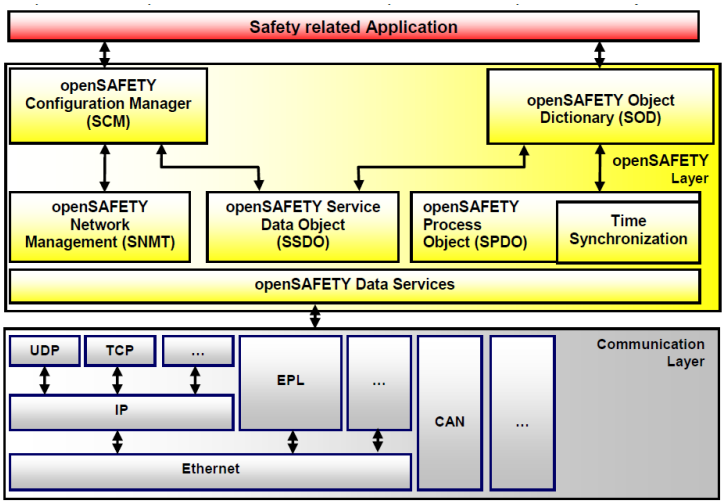
BnR Generic pdf Template Version 2

Table of Contents

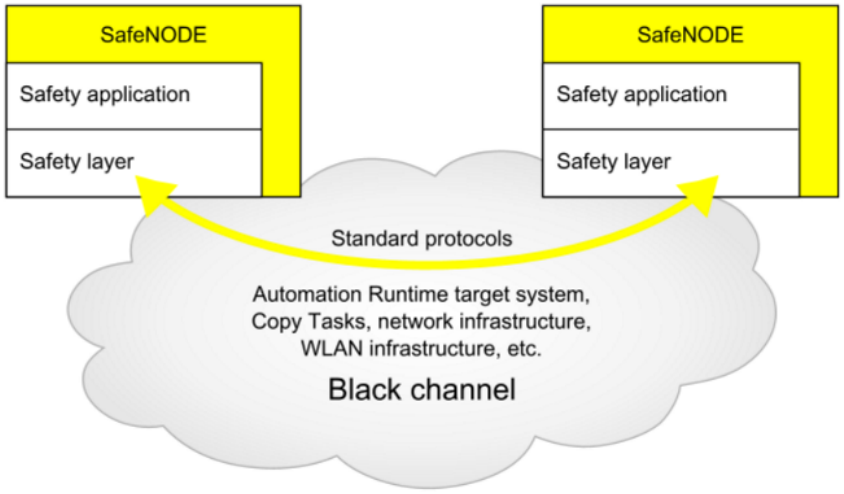
openSAFETY over UDP Reference Model



Communication Model

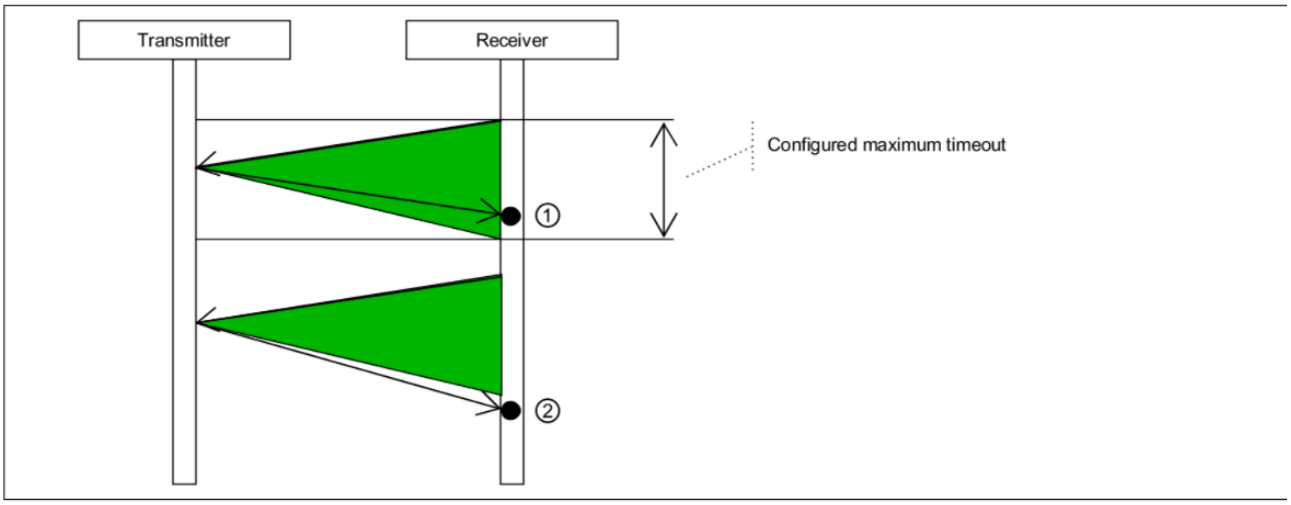


Black channel principle - Safety layer



- The black channel principle makes it possible to transfer safety-related data over a communication channel that cannot be used for safety purposes.
- The data is safeguarded in a separate safety-related protocol, or "safety layer", independent of the transfer.
- A safety layer communication relationship is usually a point-to-point connection, where the endpoints of the connection must always be implemented in a node that can be used for safety purposes (SafeNODE).
- All components in between are part of the black channel. No safety-related properties are therefore expected for these components.

Monitoring the safety response time in openSAFETY



①	Delay within the configured timeout
②	Delay too long

The figure shows the mechanisms for monitoring the response time.

openSAFETYindependently monitors the age of received packets using timestamps and checks them against a configured expectation. For this, the receiver measures the time from transmitting a request frame to receiving the associated response frame. The measured time is checked against configured timeout limits.

The maximum permissible time for receiving the response frame is the decisive parameter for time monitoring in openSAFETY. If the response frame does not reach the receiver before the maximum permissible time has elapsed, the openSAFETYconnection changes to state FAILSAFE. The maximum permissible time is therefore subsequently referred to as the timeout.

In general, a large timeout increases the stability of openSAFETYcommunication against delays and packet loss but extends the maximum safety response time (for additional information, see chapter Safety response time).

The timeout for a communication path results from the following SafeDESIGNERparameters:

("Additional tolerated packet loss" + 1)* "Safe data duration".

The timeout must take into account all transfer times of the packet from the transmitter (e.g.safe input channel on the SafeIOmodule) to the receiver (e.g.SafeLOGICcontroller). Automation Studio function "Network Analyzer"can be used to provide support in determining the timeout (for additional information about the "Network Analyzer", see sectionDiagnostics and service → Diagnostics tools → Network Analyzer). This tool can be used to determine the typical data transmission time from the receiver to the transmitter or from the transmitter to the receiver.

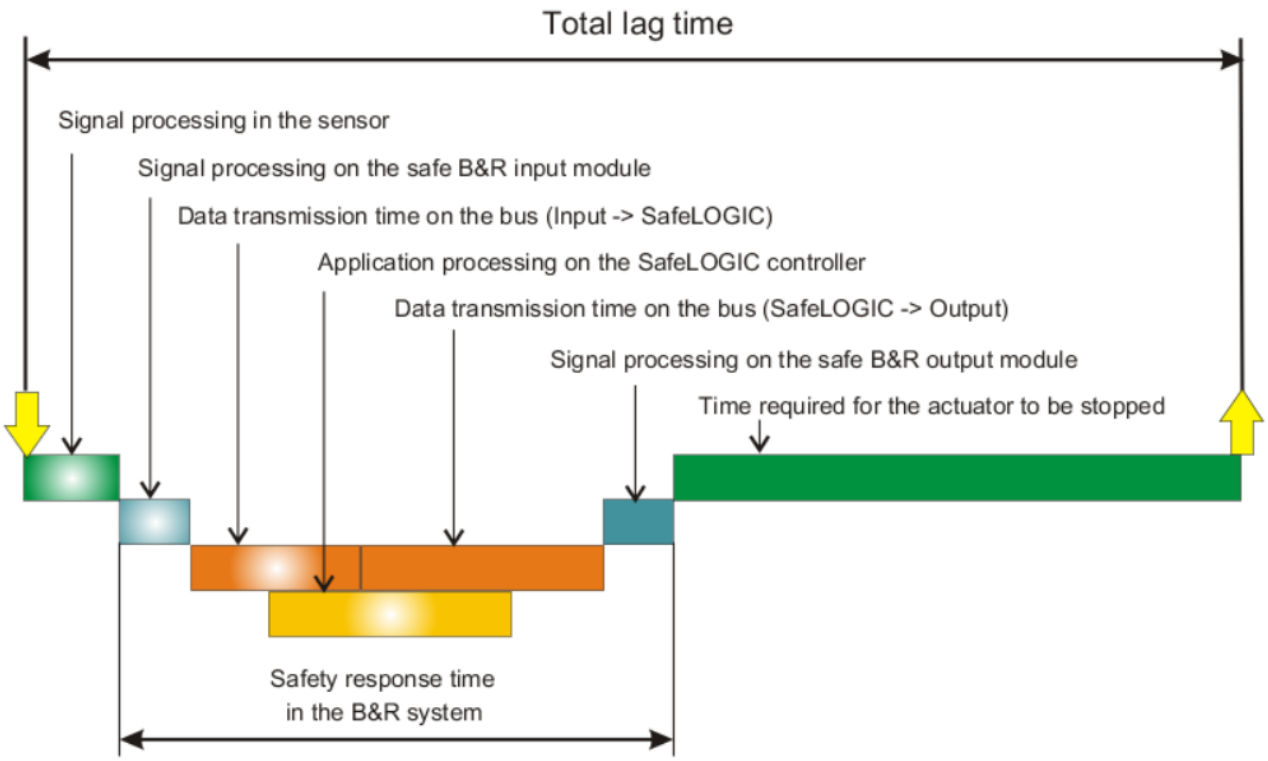
The following rule applies for establishing openSAFETYcommunication:

"Value of the Network Analyzer" * 2 + SafeLOGIC cycle time * 2 ≤Configured timeout ≤Maximum safety response time for communication

The maximum permissible safety response time is application-specific and must be determined depending on the respective safety function.

From a safety point of view, the timeout has 2 important consequences:

- In the event of delays on the black channel (e.g.packet loss, wireless communication), the transmitter's data may arrive at the receiver with a significant time delay. The timeout specifies how long this delay is accepted. The timeout is thus a direct part of the calculation of the safety response time, as described above.
- Data may be lost on the black channel. The timeout specifies how much data loss is accepted. If a safety-related event is shorter than the timeout, it is no longer guaranteed that this event will be detected on the receiver (for additional information, see chapter Minimum signal lengths).


Total lag time
Signal processing in the sensor
Signal processing on the safe B&R input module
Data transmission time on the bus (Input -> SafeLOGIC)
Application processing on the SafeLOGIC controller
Data transmission time on the bus (SafeLOGIC -> Output)
Signal processing on the safe B&R output module
Time required for the actuator to be stopped
Safety response time
in the B&R system