TRAN-SITION	SOURCE STATE	TARGET STATE	ACTION

T30	28	23	use PVi, FVo, FV_activated =1,
			Toggle_d = Toggle_h,
			restart device-timer,
			ok_nr_cycles =ok_nr_cycles +1

T31	28	26	Toggle_d = Toggle_h,
			restart device-timer,
			if CRC
			then
			  CE_CRC =1,
			  CE_CRC_count =1,
			  ok_nr_cycles =0,
			else
			  ok_nr_cycles =ok_nr_cycles +1,
			  if CE_CRC_count >0
			  then
			    CE_CRC =1,
			    CE_CRC_count = CE_CRC_count -1,
			  else CE_CRC =0,
			if WD_timeout_count >0
			then
			  WD_timeout =1,
			  WD_timeout_count = WD_timeout_count -1
			else WD_timeout =0

T32	27	26	Use PVi, FVo, FV_activated =1,
			WD_timeout =1,
			WD_timeout_count =1,
			ok_nr_cycles =0,
			restart device timer,
			Toggle_d = Toggle_h

T33	22	26	Use PVi, FVo, FV_activated =1,
			CE_CRC =1,
			CE_CRC_count =1,
			WD_timeout =0,
			ok_nr_cycles =0,
			restart device-timer,
			Toggle_d = Toggle_h

T34	25	26	Use PVi, FVo, FV_activated =1,
			CE_CRC =1,
			CE_CRC_count =1,
			ok_nr_cycles =0,
			restart device-timer,
			Toggle_d = Toggle_h

T35	24	26	Use PVi, FVo, FV_activated =1,
			WD_timeout =1,
			WD_timeout_count =1,
			ok_nr_cycles =0,
			restart device timer,
			Toggle_d = Toggle_h

T36	24	24	restart device timer with F_WD_Time_2 use_TO2_Flag =1

INTERNAL ITEM	TYPE	DEFINITION
RESETxD	Macro	See 7.1.5 and 7.1.6
RUNxD	Macro	See 7.1.5 and 7.1.6
MNR	Variable	MNR is representing the real local MNR within the F-Device. It is not transmitted to its counterpart within the F-Host, but synchronized with those via a Toggle Bit within the Control Byte. That means it changes each time when the Toggle Bit within the Control Byte (Toggle_h) changes its state from 0 → 1 or from 1 → 0.
ok_nr_cycles	Counter	During start-up and after a fault, the F-Device shall set FVo and FV_activated =1 for at least 3 cycles. It is the task of this incremental counter to count these cycles from 0 to 3.

INTERNAL ITEM	TYPE	DEFINITION
CE_CRC_count	Counter	This decremental counter is used to guarantee that the bit "CE_CRC" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0 to 1.
WD_timeout_count	Counter	This decremental counter is used to guarantee the bit "WD_timeout" within the Status Byte is set at least for 1 cycle or for a maximum of 2 cycles. Value range is 0 to 1.
device-timer	Timer	This timer checks whether the next valid safety PDU did arrive in time. The F-Parameter "F_WD_Time" is used to define this watchdog time. Value range is 0 to 65 535 ms.

7.2.4 Sequence diagrams

Figure 30 to Figure 35 show the interaction messages of F-Host and F-Device during start-up phase. Three phases are covered: both partners during start-up, the F-Host temporarily switches power off or the F-Device temporarily switches power off while its partner is still operating. The figures are informing about the states and the corresponding transitions. Numbers within circles represent the states the respective F-Host and F-Device are passing through.

Figure 30 shows the regular start of safety PDU transmissions between F-Host and F-Device after power on. A possible sequence of MonitoringNumbers is shown in Table A.4.

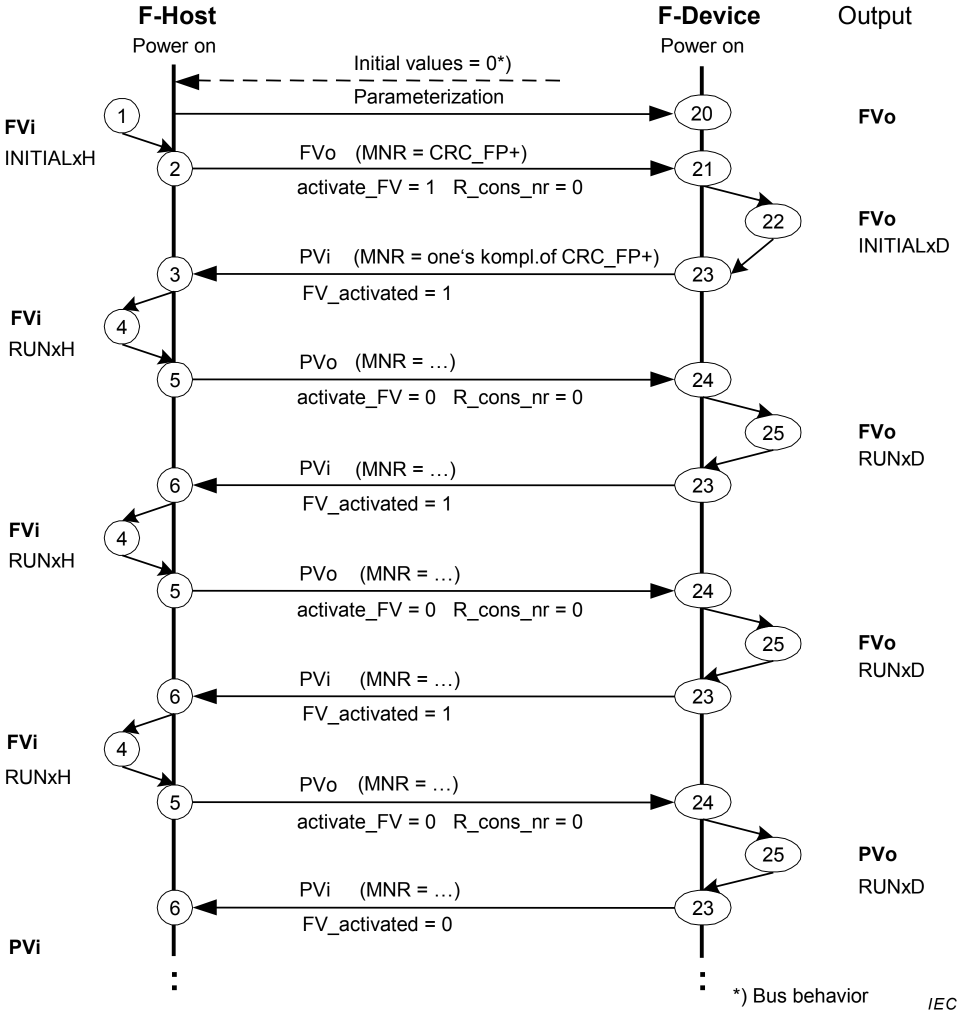

Figure 30 – Interaction F-Host / F-Device during start-up

Figure 31 shows an example with F-Parameter assignment in case the F-Device is already operating and the F-Host is switching from power off to power on.

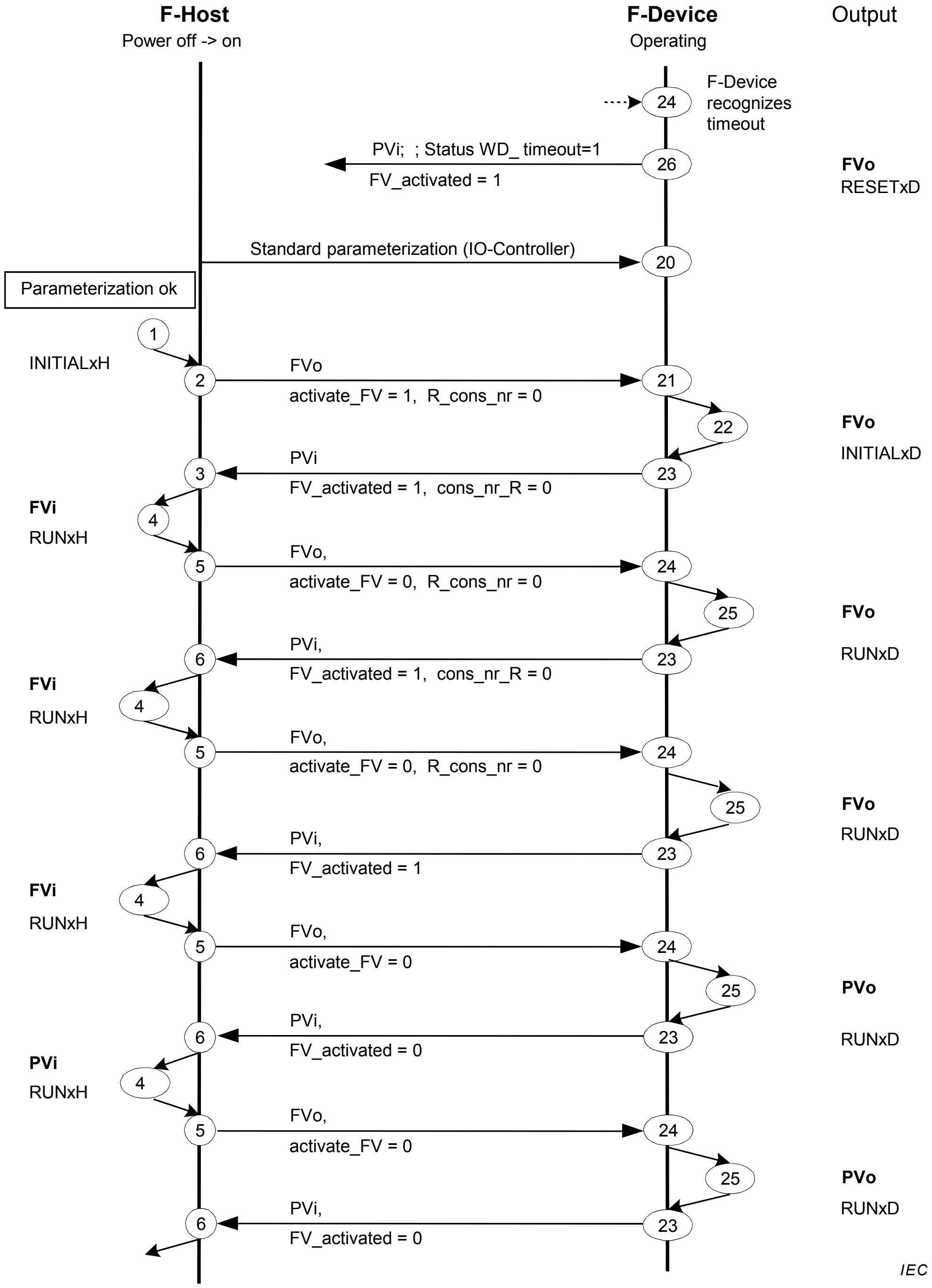

Figure 31 – Interaction F-Host / F-Device during F-Host power off → on

Figure 32 shows an example with F-Parameter assignment in case the F-Host is already operating and the F-Device is switching power on after a delay.

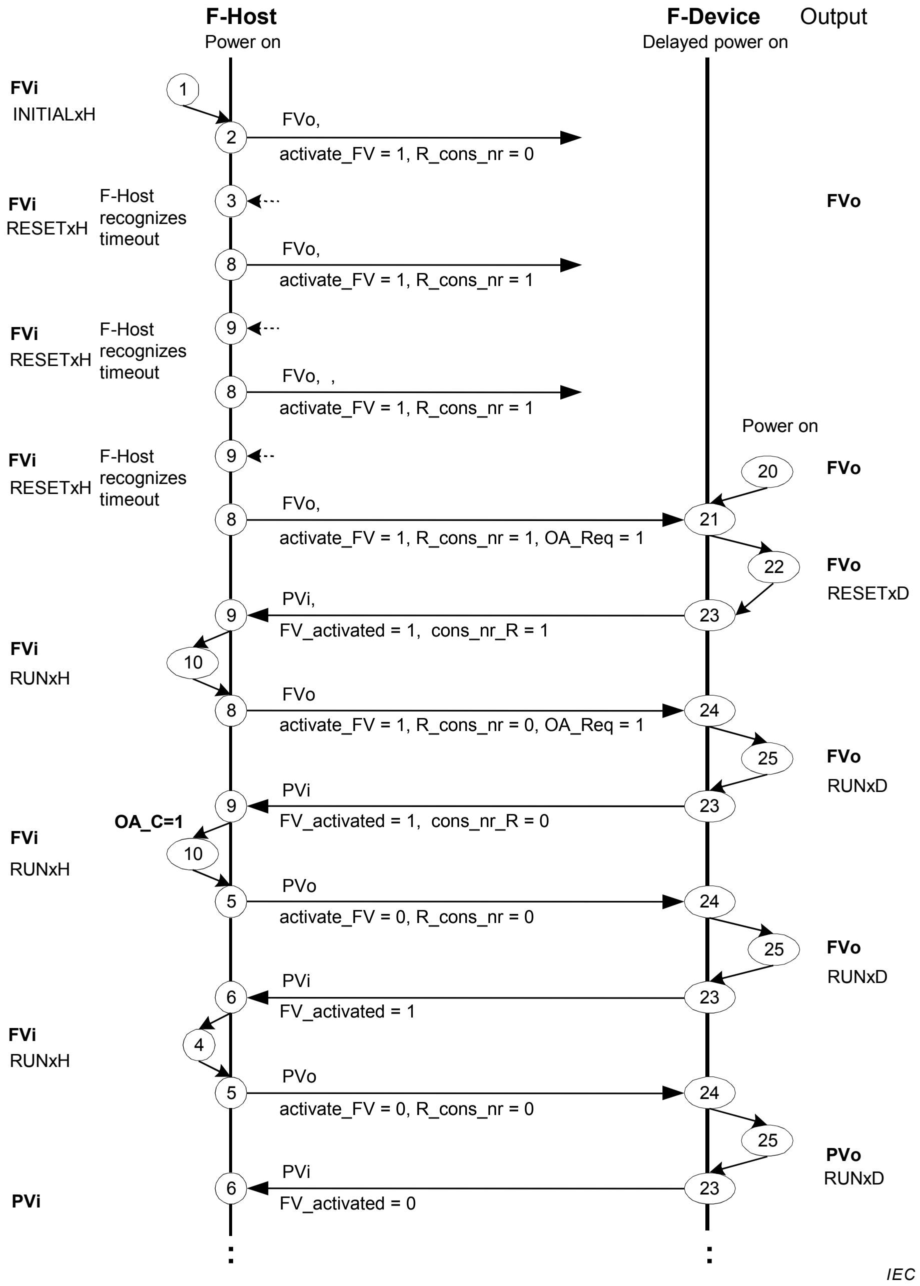
F-Host
Power on
F-Device
Delayed power on
Output
FVi
INITIALxH
1
2
FVo,
activate_FV = 1, R_cons_nr = 0
FVi
RESETxH
F-Host recognizes timeout
3
FVo
8
FVo,
activate_FV = 1, R_cons_nr = 1
FVi
RESETxH
F-Host recognizes timeout
9
8
FVo, ,
activate_FV = 1, R_cons_nr = 1
Power on
FVi
RESETxH
F-Host recognizes timeout
9
20
FVo
8
FVo,
activate_FV = 1, R_cons_nr = 1, OA_Req = 1
21
22
FVo
RESETxD
9
PVi,
FV_activated = 1, cons_nr_R = 1
23
FVi
RUNxH
10
8
FVo
activate_FV = 1, R_cons_nr = 0, OA_Req = 1
24
25
FVo
RUNxD
9
PVi
FV_activated = 1, cons_nr_R = 0
23
OA_C=1
FVi
RUNxH
10
5
PVo
activate_FV = 0, R_cons_nr = 0
24
25
FVo
RUNxD
6
PVi
FV_activated = 1
23
FVi
RUNxH
4
5
PVo
activate_FV = 0, R_cons_nr = 0
24
25
PVo
RUNxD
PVi
6
PVi
FV_activated = 0
23
IEC

Figure 32 – Interaction F-Host / F-Device with delayed power on

Figure 33 corresponds to Figure 32. It shows the case when the F-Host is already operating and the F-Device switches power off and after a delay switches power on again.

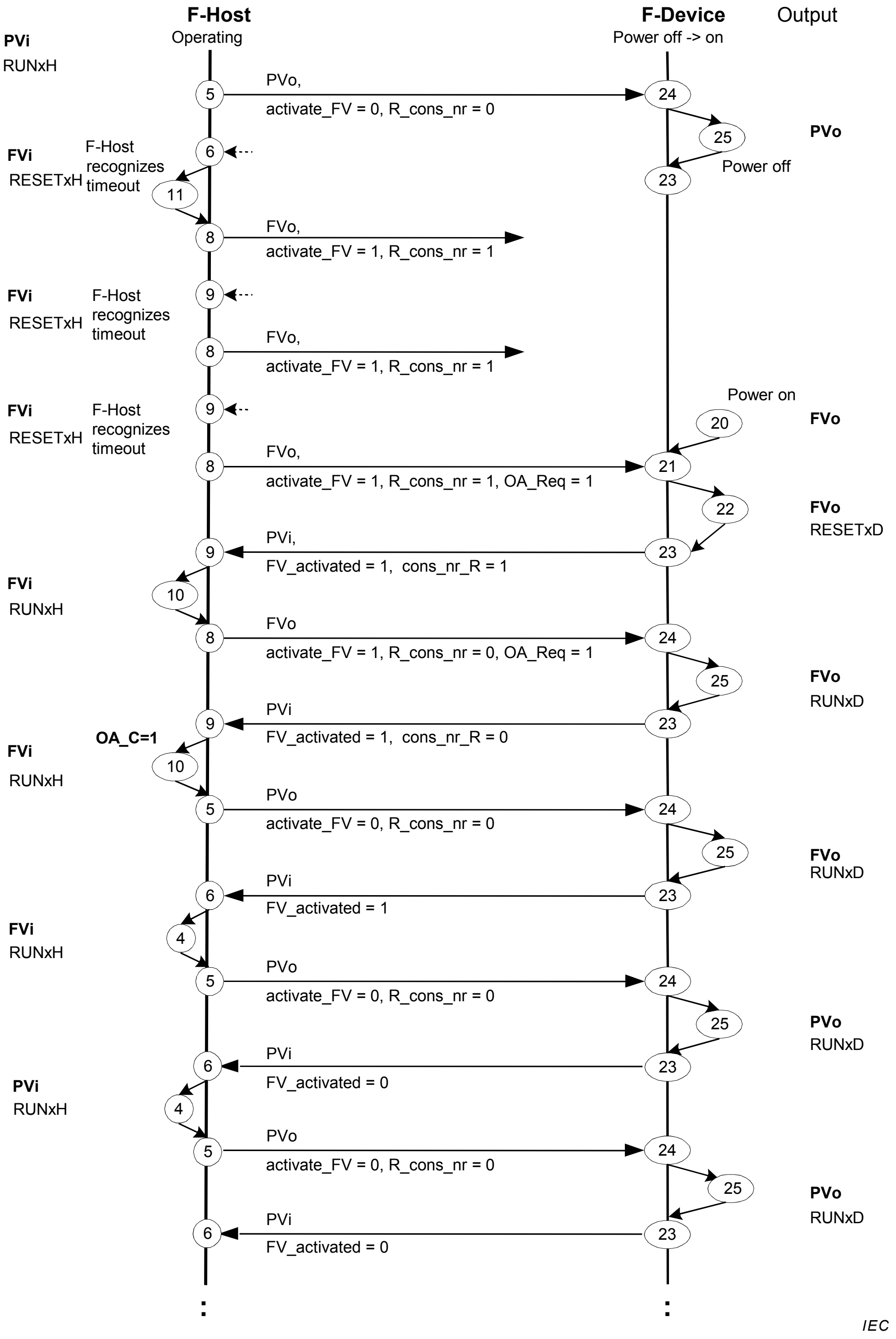

Figure 33 – Interaction F-Host / F-Device during power off → on

Figure 34 shows the interaction messages between F-Host and F-Device while CRC faults are detected on the F-Host side.

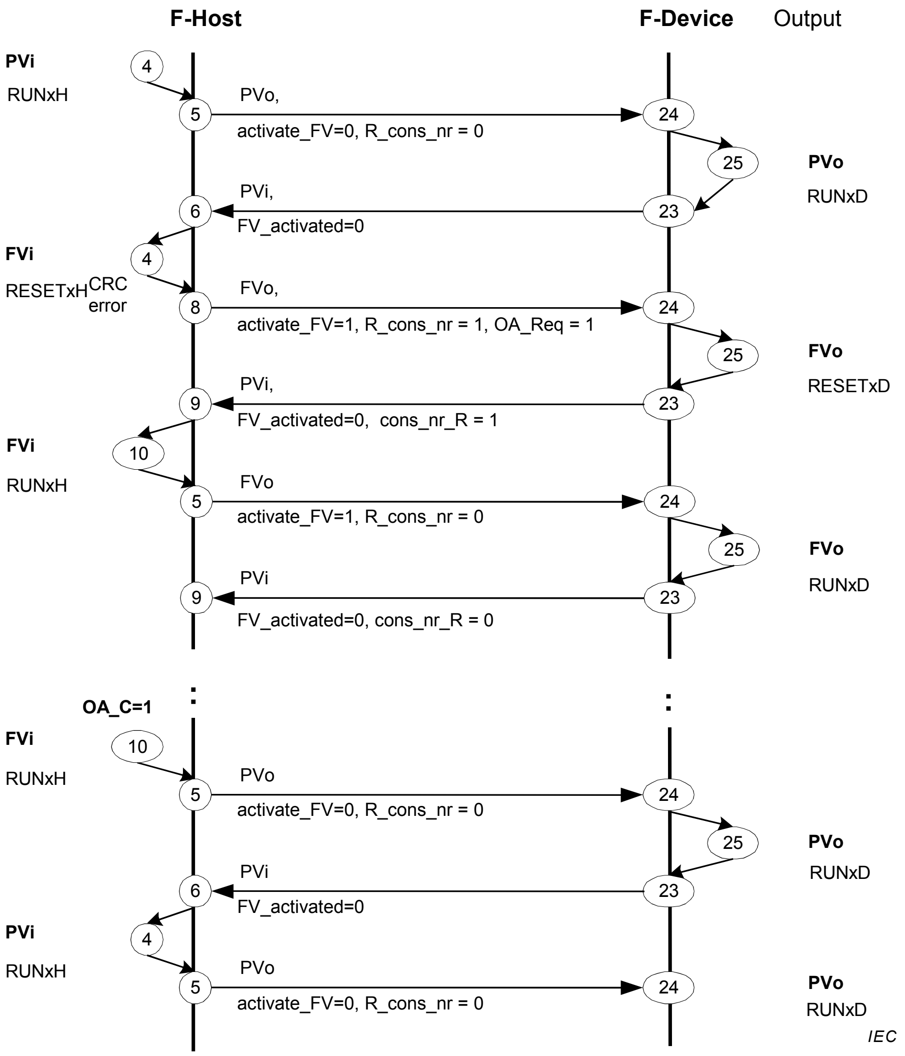

Figure 34 – Interaction F-Host / F-Device while host recognizes CRC error

Figure 35 shows the interaction messages between F-Host and F-Device while CRC faults are detected on the F-Device side.

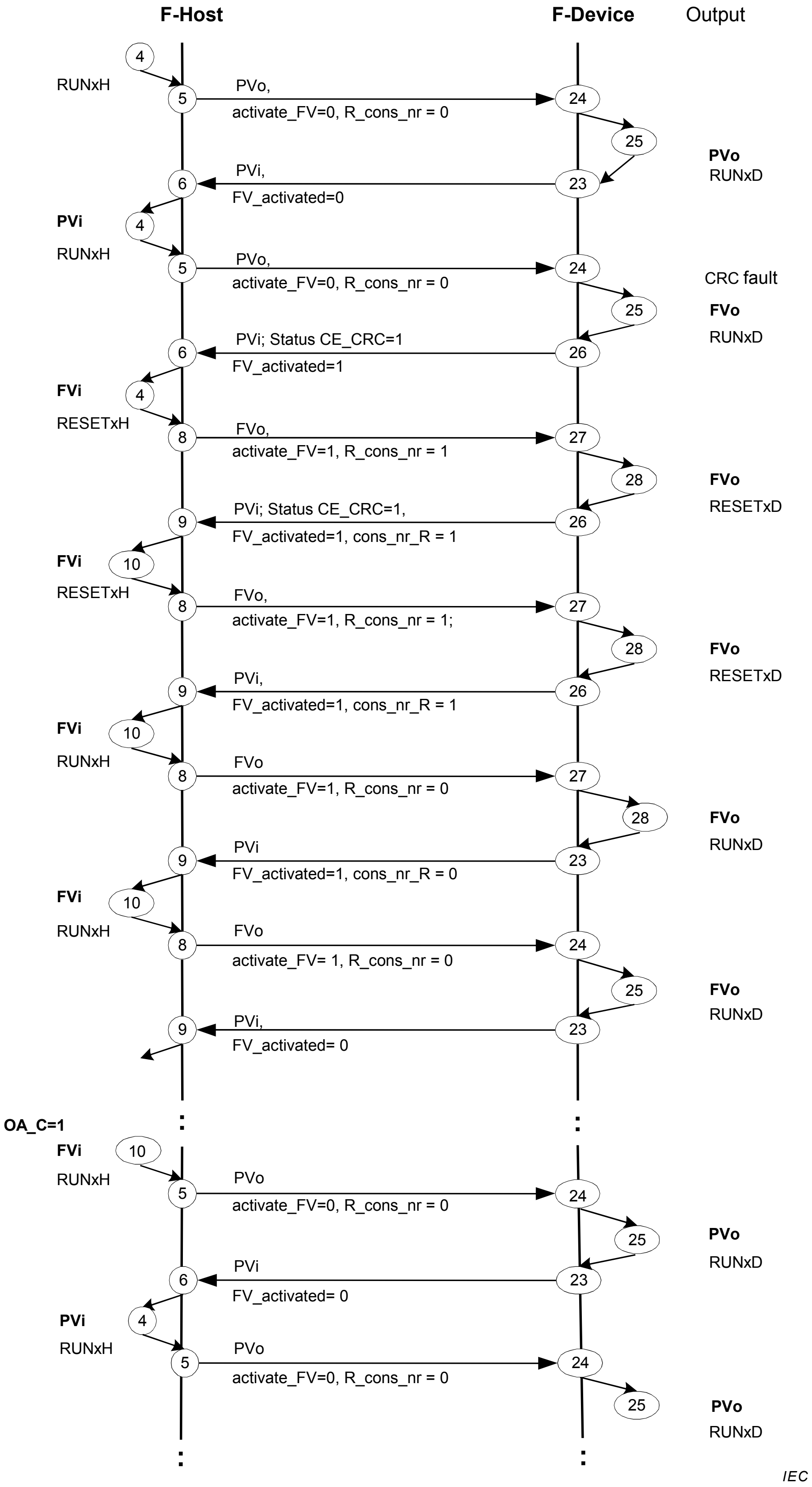

Figure 35 – Interaction F-Host / F-Device while device recognizes CRC error

7.2.5 Timing diagram for a MonitoringNumber reset

Figure 36 demonstrates the consequences of an F communication fault on the MonitoringNumber and depending items.

After a fault, bit 2 ("R_cons_nr") and bit 4 ("activate_FV") of the Control Byte is set (=1). In consequence the MNR is reset and the output values of an F-Output-Device are set to "FVo".

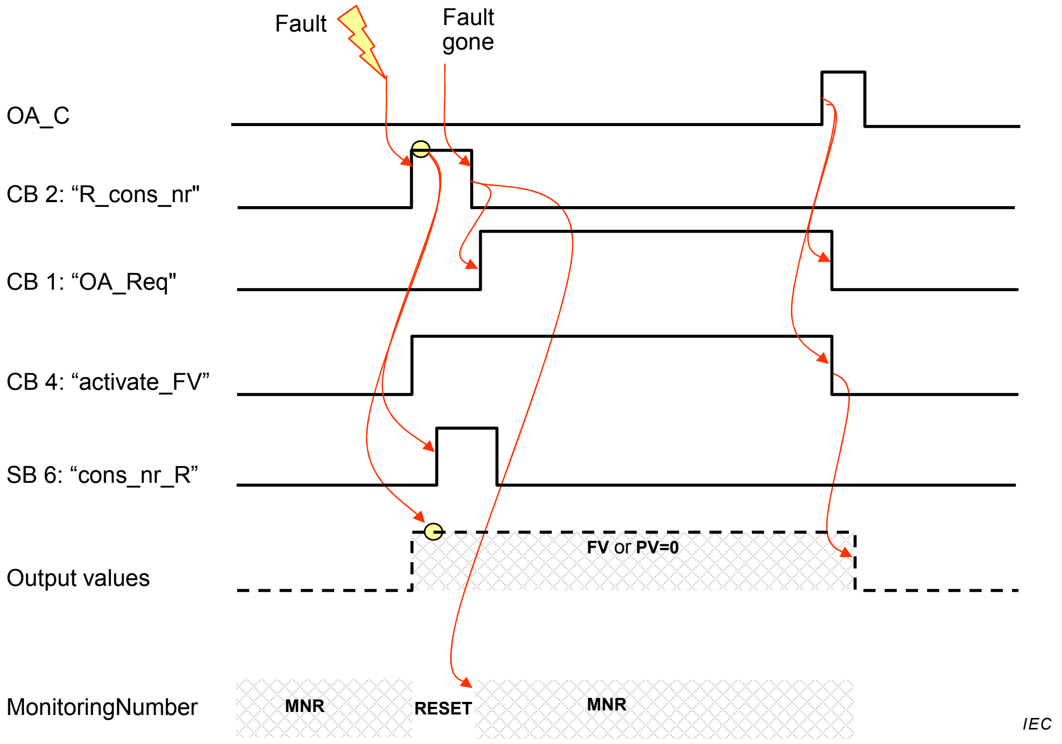

Figure 36 – Impact of the MNR reset signal

Meanwhile the F-Host is sending the signal "OA_Req" as bit 1 of the Control Byte to the F-Device. This signal can be used to indicate the user via LED (9.1) that an error occurred and an Operator Acknowledgment is requested (OA_C). Right after the fault is gone the following actions take place:

- MNR reset resumes its default value (R_cons_nr = 0);
- the MNR restarts.

Right after an Operator Acknowledgment (OA_C = 1) the following actions take place:

- request for an Operator Acknowledgment resumes its default value (OA_Req = 0);
- request to activate fail-safe output state resumes its default value (activate_FV = 0);
- process output values appear again after three message cycles.

7.2.6 Monitoring of safety times

7.2.6.1 Normal operation

Figure 37 demonstrates how the F driver is using the underlying CP 3/RTE communications and how some monitoring times are defined. Meaning of the short arrows: in CP 3/RTE, the IO-Controller sends the same safety PDU more frequently to the F-Device than a new safety PDU is generated by the F driver within the host cycle time in the F-Host. In return the F-Device is sending the (acknowledgment) safety PDU to the IO- Controller more frequently than the F Driver in the F-Device is generating a new safety PDU.

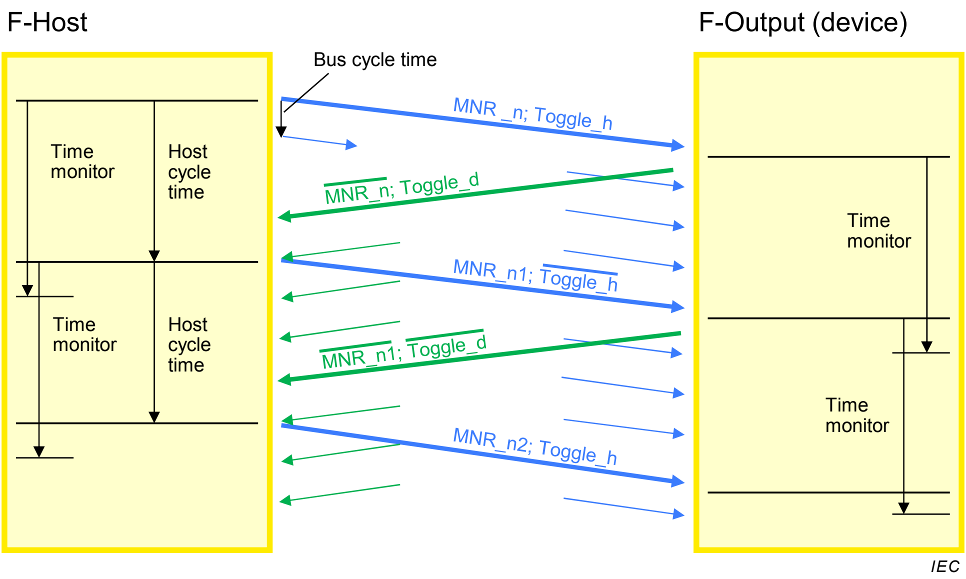

Figure 37 – Monitoring the message transit time F-Host ↔ F-Output

Figure 37 shows the time monitoring within the F-Host and an F-Output device. Figure 38 is showing the time monitoring within the F-Input device and the F-Host. Short arrows in the figures represent FSCP 3/1 PDUs with the currently valid (virtual) MNR but possibly different process values.

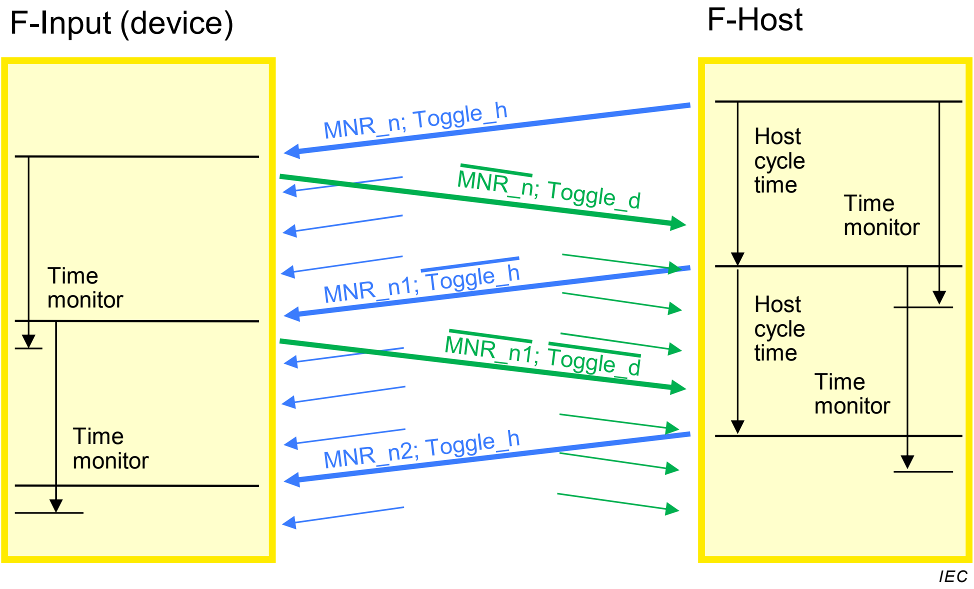

Figure 38 – Monitoring the message transit time F-Input ↔ F-Host

Other timing constraints are listed below:

Startup (Synchronization)
To synchronize after a system start, the F-Host driver starts with the virtual initial MNR (see 7.1.5 and 7.1.6).

F protocol cycle
An F-Input/F-Output returns a safety PDU to the F-Host with the same virtual MNR (F protocol cycle) to acknowledge the reception of a safety PDU.

The F-Host cycle time shall not exceed the F protocol cycle time (it may be shorter).

Time monitor
(Watchdog)

The arrival of a new correct safety PDU at the F-Device within the watchdog time is being monitored. This verification can be performed as often as necessary, but at least once at the end of the monitoring time interval. When the watchdog time expires, the related recipient switches over to a safe state.

The slowest CP 3/RTE cycle time shall not be longer than half of the watchdog time. The F-Host cycle time may be shorter than the watchdog time.

Monitoring the MNR

A new correct safety PDU is characterized by the fact that at least the virtual MNR is changed to the next virtual MNR and that either the entire rest of the safety PDU part is unchanged or has been changed faultlessly. This means that an incorrect change of the virtual MNR is recognized directly by CRC2. This will then lead to a fault reaction.

Safety PDU repetition

A complete safety PDU repetition in the case that a new correct safety PDU has not been received within the watchdog time interval is not supported.

SIL monitor

Every corrupted message of all transmissions related to a safety function (CRC and virtual MNR fault) will be counted during a configurable SIL monitor time period (T). The fail-safe values are set whenever more than one such fault occurred, i.e. one detected corrupted message can be tolerated (*variant A*). Thus, the preallocation is "one corrupted message" at system startup. The cases, where the whole PDU of the message = "0" (for example at start-up), shall not be counted.

In practice it can be shown that the counting actually always remains zero. This is the reason for an optimization of complexity resulting in *variant B*, where the SIL monitor time (T) is set to infinite. In this case, the simplified F-Host state chart of Figure 28 shall be taken into account where any detected corrupted safety PDU is not tolerated and always leads to a safe state.

Whenever such an unlikely event of a detected corrupted message should occur during the shift of production or operation, the responsible operator is assigned to play the role of the SIL-Monitor and can tolerate the indication and acknowledge it. In case of frequent indications more often than once per SIL Monitor time a check of the installation (for example electromagnetic interference), network traffic load, or transmission quality should be performed.

It is up to the F-Host manufacturer to implement variant A. However, a detailed realization is not specified here for the sake of individual adaptations to the particular system environments. The SIL monitor shall only be implemented within the F-Host.

SIL Monitor time period (T)

The SIL monitor time period T is a constant value with the dimension hour (h) that results from the requested SIL and the configured CRC length (9.5.1). Table 12 specifies the SIL monitor times.

Table 12 – SIL monitor times

SIL	Time period (h) protocol BP, LP	Time period (h) protocol XP
3	>100	>10
2	>10	>1

7.2.6.2 Extended watchdog time on request after user interaction

For use cases such as 'Configure in Run' [64] or 'maintenance of fault tolerance systems' a certain time is required to update the affected devices. This update time usually is longer than the regular (primary) watchdog time (F_WD_Time) defined for a safety application. In order to avoid nuisance trips, the F-Host driver can use once only (see Figure 41) a secondary watchdog time (F_WD_Time_2) to extend the primary watchdog time for these cases as shown in Figure 39.

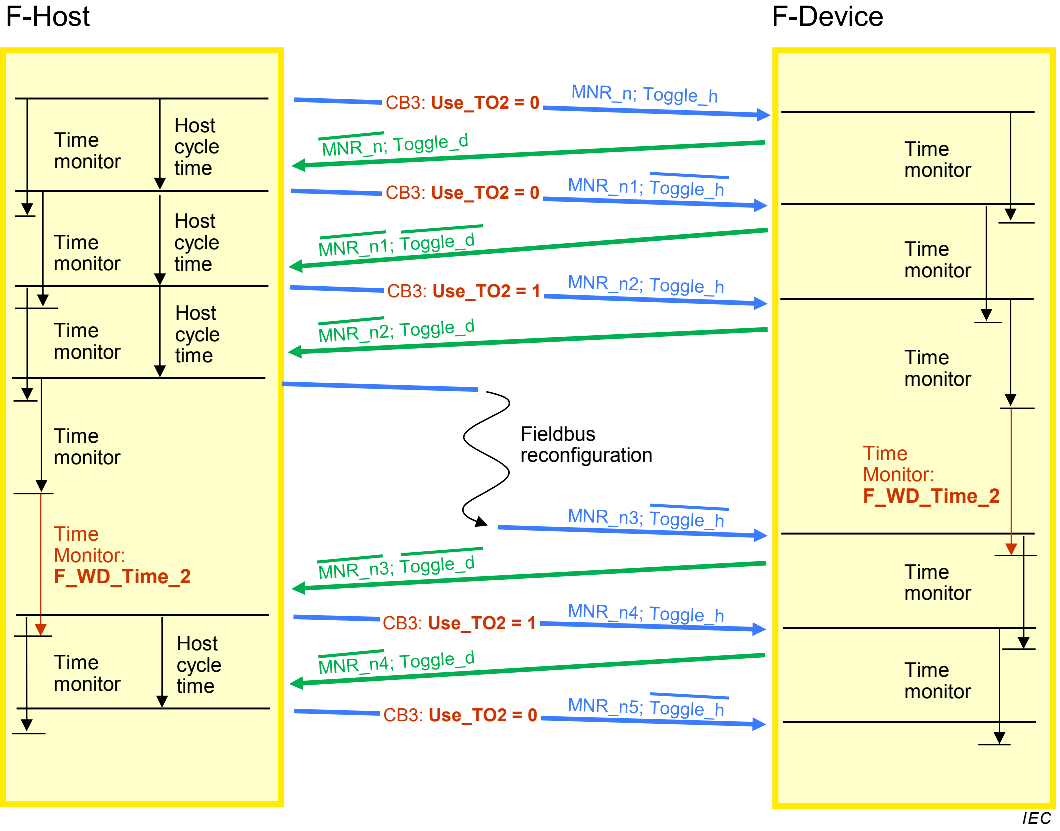

Figure 39 – Extended watchdog time on request

The F-Host shall set and reset Bit 3 (Use_TO2) of the Control Byte for all the F-Devices thus affecting all F-Devices simultaneously (see 6.1).

7.3 Reaction in the event of a malfunction

7.3.1 Unintended repetition

Quote: "The malfunction of a bus device causes old and obsolete safety PDUs to be repeated at the incorrect time so that a recipient would dangerously be disturbed (for example guard door is reported closed albeit it has already been opened)."

Remedial action: The data within the Black Channel are transferred cyclically. Thus, an incorrect message with a safety PDU that is inserted once will immediately be overwritten by a correct