EUCHNER

More than safety.

EKS FSA on Siemens S7-300 – operating mode selection with touchscreen

Contents

Components/modules used

EUCHNER

Description	Order no./item designation
EKS Profinet *FSA* or EKS Profibus *FSA*	106306 / EKS-A-IIXA-G01-ST02/03/04 100378 / EKS-A-IDXA-G01-ST09/03/04
EKS Electronic-Key	077859 / EKS-A-K1RDWT32-EU 084735 / EKS-A-K1BKWT32-EU 091045 / EKS-A-K1BLWT32-EU 094839 / EKS-A-K1GNWT32-EU 094840 / EKS-A-K1YEWT32-EU

Tip: More information and downloads about the aforementioned EUCHNER products can be found at www.EUCHNER.de. Simply enter the order number in the search box.

Others

Description	Item
S7-300, CPU 315F-2 PN/DP	6ES7315-2FJ14-0AB0

Abbreviations

Designation	Abbreviation
EKS *FSA* EKS	The EKS with *FSA* functionality and databus interface used in this application (refer to the EUCHNER components used)
PLC	The conventional control system that is used and that offers PLC functionality. The PLC has connections for the bus systems used.
F-PLC	The fail-safe PLC used in this application. The F-PLC shares a data range with the PLC via marker words
HMI	The human-machine interface comprising a screen with touch-sensitive surface or softkeys.
MW	Memory word, a 16-bit data word for data exchange between the F-PLC and the PLC
PL	Performance Level according to EN ISO 13849-1
PL_r	Performance Level required according to EN ISO 13849-1
SRASW	Safety-related application software according to EN ISO 13849-1

Functional description

General

Operating mode selection is to be realized on a machine using the EKS *FSA* as an access system. The operating mode is selected via a touchscreen or other control elements, e.g. softkeys in the HMI (human-machine-interface). Operation is therefore possible via the standard user interface; no key-operated rotary switch is required. Evaluation and switchover of the operating mode are realized via a safe programmable logic controller (F-PLC). Data distribution is performed via a standard programmable logic controller (PLC).

Example of an Electronic-Key structure

The data on the Electronic-Key are structured as follows, for example: Other structures are possible.

Byte no.	Description	Type	Length	Explanation
103 – 104	KEYCRC	CRC	2 bytes	Checksum over a certain part of the Electronic-Key as copy protection. Refer to the EKM manual and application example AP000169-5-… for details about the checksum.
105 – 112	Expiry date	Date	8 bytes	Electronic-Key expiry date
113 – 114	Authorization level	Word	2 bytes	Authorization level for access to the machine.
115	Department	Byte	1 byte	Number describing a limited quantity of machines or installations.
116 – 123	KeyID	KeyID	8 bytes	The KeyID is a number that is permanently pre-programmed on the Electronic-Key by EUCHNER. This number is different for each Electronic-Key. This number can be used to identify workers.

This is only a very simple example. The data range on the Electronic-Key is structured according to the requirements for access to machines or installations. Additional data, e.g. identification data or data for other areas or departments, can also be created on the Electronic-Key. Supplementary data for which there is no memory space on the Electronic-Key can be stored in the EKM database. Please refer to the application “Definition of the Electronic-Key structure on an EKS Electronic-Key” (AP000169-1-…) for details about structuring the data range on the EKS Electronic-Key.

KEYCRC, which is used to calculate a checksum over the Electronic-Key content, is an important field for preventing the copying of Electronic-Keys. This field must be calculated and monitored in the control system as well. This permits the creation of effective protection against counterfeit or copied Electronic-Keys. An example for this can be found in the application AP000169-5.…

Defining the Electronic-Key structure is the most important step in using the EKS. This defines the capabilities of the EKS Electronic-Key.

The “Authorization level” field has a special meaning for this application. Certain operating modes are released for individual users with this field, which permits compliance with the requirement in the Machinery Directive for restriction of operating mode selection to certain groups of persons.

Value supply for the authorization level with five operating modes:

Binary value	Hexadecimal value
0000 1111 0000 1111	0F0FH
0000 1111 1111 0000	0FF0H
0011 0011 0011 0011	3333H
0011 0011 1100 1100	33CCH
0011 1100 0011 1100	3C3CH

Table 1

The values are selected to ensure a Hamming distance of 8. KEYCRC additionally prevents falsification of the Electronic-Key. A theoretical maximum of 31 different operating modes could be selected with this coding. The value zero must not be used. This value is necessary in order to recognize a removed Electronic-Key. To ensure data transfer between the various systems via the bus, the codes for operating mode selection must be selected according to the value supply. Therefore, these data words must also continue to be used within the program.

Definition of the data words for the operating-mode level

In order to avoid errors due to overwriting of the memory in the PLC, the meaning of operating mode selection in the various memory locations used **must** change values. For this purpose, Table 2 or Table 4 defines the meaning of operating mode selection in the respective variable or in the data word. This is done by means of constants.

Variable or data word	Definition Operating mode	Hex	Comment
Value range for MW01 and ReadAuthorization, Electronic-Key content (the Electronic-Key must be written according to these values)	RE_MSO_0	0F0FH	Mode of Safe Operation 0: Manual mode
	RE_MSO_1	0FF0H	Mode of Safe Operation 1: Automatic mode
	RE_MSO_2	3333H	Mode of Safe Operation 2: Setup mode
	RE_MSO_3	33CCH	Mode of Safe Operation 3: Automatic mode with manual intervention
	RE_MSO_4	3C3CH	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MW03 and SelectMSO	SE_MSO_0	0FF0H	Mode of Safe Operation 0: Manual mode
	SE_MSO_1	3333H	Mode of Safe Operation 1: Automatic mode
	SE_MSO_2	33CCH	Mode of Safe Operation 2: Setup mode
	SE_MSO_3	3C3CH	Mode of Safe Operation 3: Automatic mode with manual intervention
	SE_MSO_4	0F0FH	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MW05 and CheckMSO	CH_MSO_0	3333H	Mode of Safe Operation 0: Manual mode
	CH_MSO_1	33CCH	Mode of Safe Operation 1: Automatic mode
	CH_MSO_2	3C3CH	Mode of Safe Operation 2: Setup mode
	CH_MSO_3	0F0FH	Mode of Safe Operation 3: Automatic mode with manual intervention
	CH_MSO_4	0FF0H	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MW07 and SwitchMSO	SW_MSO_0	33CCH	Mode of Safe Operation 0: Manual mode
	SW_MSO_1	3C3CH	Mode of Safe Operation 1: Automatic mode
	SW_MSO_2	0F0FH	Mode of Safe Operation 2: Setup mode
	SW_MSO_3	0FF0H	Mode of Safe Operation 3: Automatic mode with manual intervention
	SW_MSO_4	3333H	Mode of Safe Operation Service: Mode for servicing and setup

Table 2

The values represent a hierarchical order – MSO 1 and MSO 2 are contained in MSO 3, for example.

Important: These values must be used to ensure data transfer on the bus between the PLC and the HMI.

Value supply for the authorization level with three operating modes:

If only up to three different operating modes are required for a machine or installation, a data byte with the Hamming distance 5 can be used instead of the data word. The procedure of the changing values for the meaning of operating mode selection must also be used here.

Binary value	Hexadecimal value
00011111	1FH
11100011	E3H
11111100	FCH

Table 3

Definition of the data bytes for the operating-mode level

IMPORTANT: The definition of the data bytes must correspond exactly to the schema in Table 4. In particular, the values for automatic mode must be assigned according to the table!

Variable or data byte	Definition Operating mode	Hex	Comment
Value range for MB01 and ReadAuthorization	RA_MSO_1	1FH	Mode of Safe Operation 1: Automatic mode
	RA_MSO_2	E3H	Mode of Safe Operation 2: Setup mode
	RA_MSO_3	FCH	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MB03 and SelectMSO	SE_MSO_1	E3H	Mode of Safe Operation 1: Automatic mode
	SE_MSO_2	FCH	Mode of Safe Operation 2: Setup mode
	SE_MSO_3	1FH	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MB05 and CheckMSO	CH_MSO_1	1FH	Mode of Safe Operation 1: Automatic mode
	CH_MSO_2	FCH	Mode of Safe Operation 2: Setup mode
	CH_MSO_3	E3H	Mode of Safe Operation Service: Mode for servicing and setup
Value range for MB07 and SwitchMSO	SW_MSO_1	E3H	Mode of Safe Operation 1: Automatic mode
	SW_MSO_2	1FH	Mode of Safe Operation 2: Setup mode
	SW_MSO_3	FCH	Mode of Safe Operation Service: Mode for servicing and setup

Table 4

The values represent a hierarchical order – MSO 1 and MSO 2 are contained in MSO 3, for example.

Important: These values must be used to ensure data transfer on the bus between the PLC and the HMI.

Block diagram and description

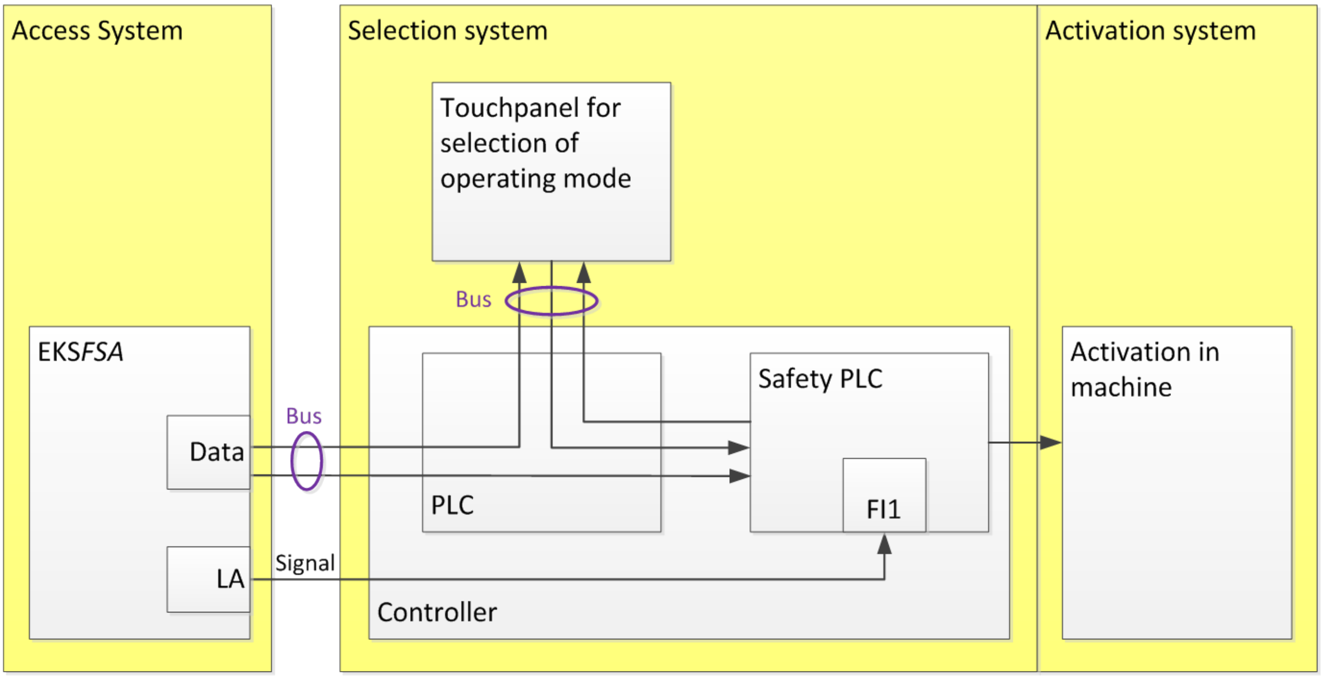


Figure 1

The EKS *FSA* is connected to the PLC via the bus. Data are sent only to the PLC. The PLC internally forwards the data to the safety PLC (F-PLC) via marker words (MW..). Any communication with the HMI is permissible, typically via a bus. Switching channel LA of the EKS *FSA* must be connected to a safe input of the F-PLC. FI1 is used in the example. The safe PLC is responsible for switching the operating mode. This could be internal signals to the PLC. First and foremost, however, the safety equipment for the selected operating mode is also switched on via outputs. It must be observed that this part of operating mode selection is also relevant to safety and therefore must fulfill the required Performance Level (PL_r) of operating mode selection.

General notes about programming

The procedures in the four different devices are structured so that the F-PLC automatically detects as many errors as possible based on the data generated and forwarded by the various devices.

The depiction in the diagrams below is a logical sequence that is not automatically observed in a PLC or in an F-PLC with cyclical processing. Therefore, programming must be performed so that each step is executed only once. For example, this can take the form of a simple status machine programmed to process only one of the single steps from the diagrams below per PLC cycle. Only when the single step has been completed does switchover to the next step take place.

Prior to every single step, a check according to Figure 3 or Figure 8 must be programmed in the PLC, in the HMI and in the F-PLC to ensure that the EKS state is always detected correctly and is reset to the original state if the Electronic-Key is pulled out during program processing, for example. These checks prior to each step monitor that all control system parts run in parallel and that the system switches back from a possible error once the software portions are being executed properly again.

Once a sequence has been completed, at least the “plug in before each step” or “unplug before each step” routine must then be performed.

Inserting an EKS Electronic-Key

The entire sequence is depicted in the flowcharts in Figures 2.1 to 2.3. Transfer variables are shown in red.

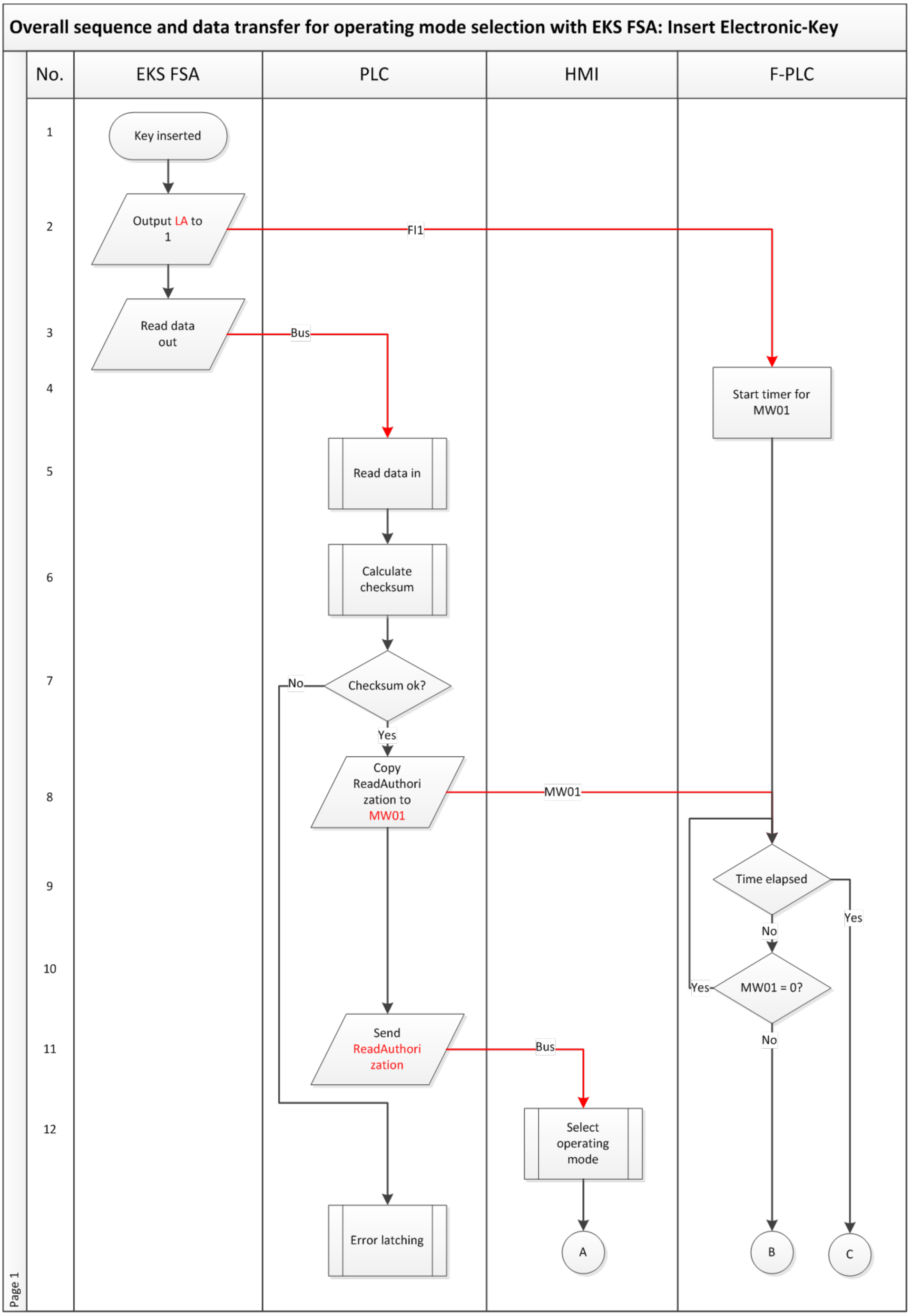


Figure 2.1

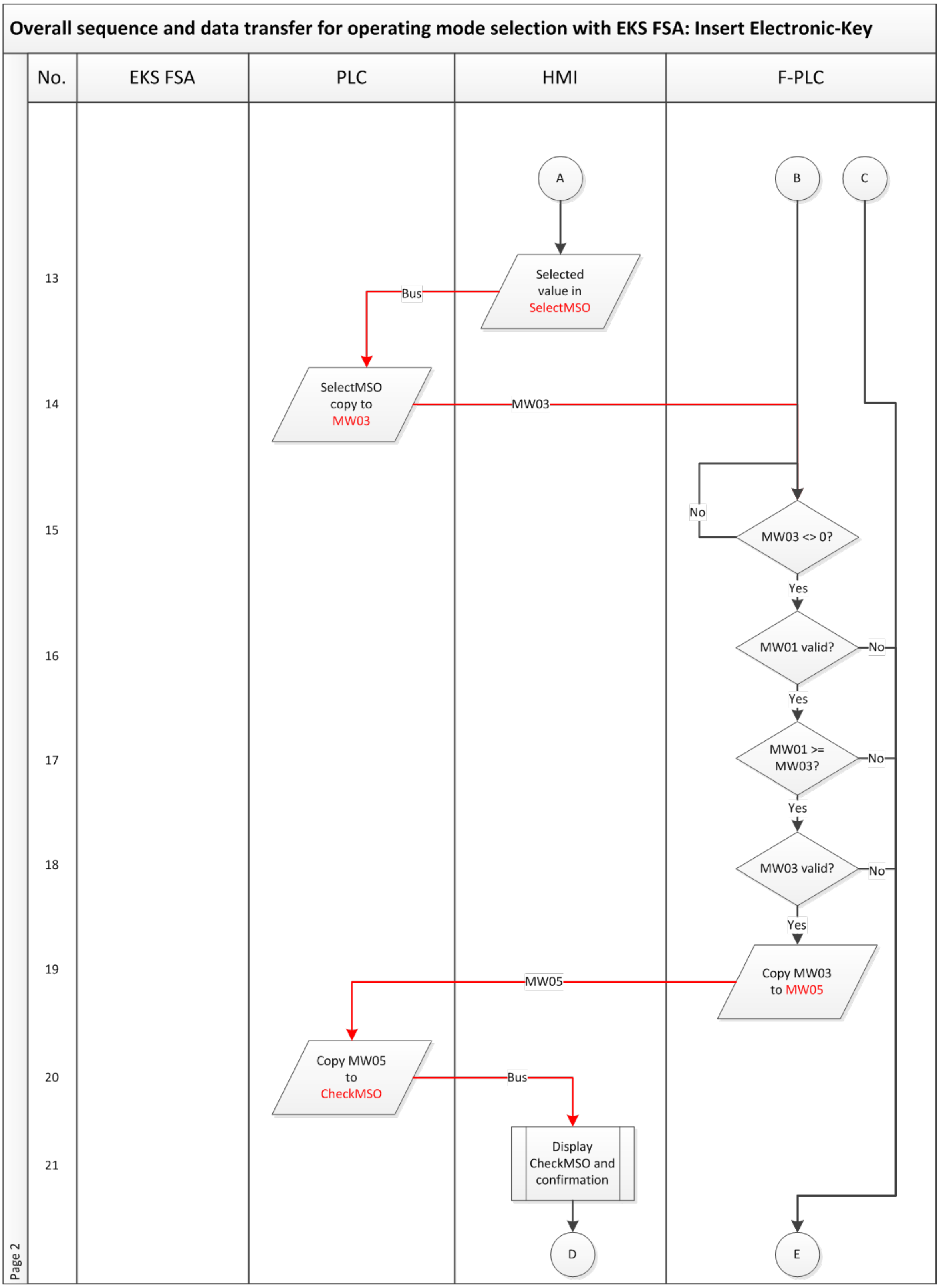

Overall sequence and data transfer for operating mode selection with EKS FSA: Insert Electronic-Key
No.
EKS FSA
PLC
HMI
F-PLC
A
B
C
13
Selected value in SelectMSO
Bus
14
SelectMSO copy to MW03
MW03
15
No
MW03 <> 0?
Yes
16
MW01 valid?
No
Yes
17
MW01 >= MW03?
No
Yes
18
MW03 valid?
No
Yes
19
Copy MW03 to MW05
MW05
20
Copy MW05 to CheckMSO
Bus
21
Display CheckMSO and confirmation
D
E
Page 2

Figure 2.2

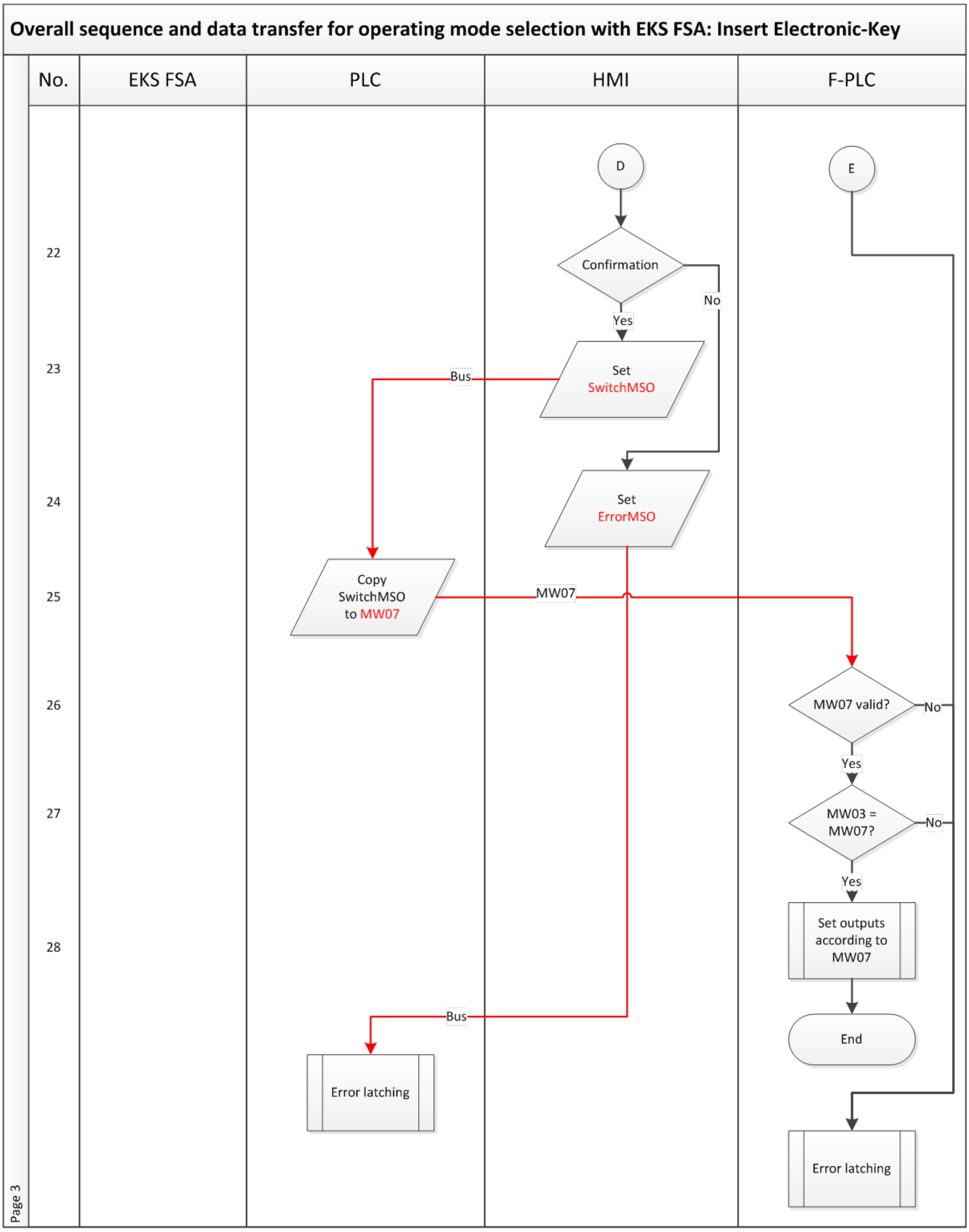

Overall sequence and data transfer for operating mode selection with EKS FSA: Insert Electronic-Key
No.
EKS FSA
PLC
HMI
F-PLC
D
E
22
Confirmation
No
Yes
23
Set
SwitchMSO
Bus
24
Set
ErrorMSO
25
Copy
SwitchMSO
to MW07
MW07
26
MW07 valid?
No
Yes
27
MW03 =
MW07?
No
Yes
28
Set outputs
according to
MW07
End
Bus
Error latching
Error latching
Page 3

Figure 2.3

Step	System	Description
1	EKS *FSA*	A user inserts an Electronic-Key.
2	EKS *FSA*	When an Electronic-Key is inserted, output LA is set to 1 if the Electronic-Key is a valid Electronic-Key. The content of the Electronic-Key is not considered.
3	EKS *FSA*	The EKS *FSA* reads out the Electronic-Key. The Electronic-Key format is detected in this process, and the data are sent only if everything is correct.
4	F-PLC	A time expectation (approx. 1 s) is started in the safe PLC for transmission of the associated data from the PLC after the setting of safe input FI1. All further data must have been read in by the EKS *FSA* and reported to the F-PLC via the various systems before the time elapses.
5	PLC	All Electronic-Key data are read in by the PLC in the defined input range and are copied over into a global data block from there.
6	PLC	The checksum of the Electronic-Key content is calculated. Information about whether the checksum is OK is then returned as a bit. (Refer to application AP000169-5… for this purpose)
7	PLC	Check as to whether the checksum calculation produced the same result as the one written on the Electronic-Key. (Refer to application AP000169-5… for this purpose)
8	PLC	The data from the range of the data block at the access authorization location are copied unchanged over to marker word MW01 to provide the data to the F-PLC. It must be borne in mind here that the definition of the value range for MW01 and the ReadAuthorization from Table 2 or Table 4 must be used. The data must already be on the Electronic-Key in this form.
9	F-PLC	Check of whether the time has elapsed. This monitors whether both the EKS and the PLC function properly.
10	F-PLC	It is checked whether new data arrived from the PLC. This is identified by any value other than 0 appearing in MW01.
11	PLC	The PLC sends the content of ReadAuthorization to the HMI via the bus system. It must be borne in mind here that the definition of the value range for MW01 and the ReadAuthorization from Table 2 or Table 4 must be used. The data must already be on the Electronic-Key in this form.
12	HMI	A screen in which the operating mode can be selected is generated or made accessible in the HMI. An operating mode is selected via a touchscreen or via softkeys. The highest operating mode that can be input must not exceed the access authorization on the EKS Electronic-Key corresponding to MW01 or ReadAuthorization.
13	HMI	The HMI sends the operating mode selected by the user over the bus. It must be borne in mind here that the definition of the value range for MW03 and SelectMSO from Table 2 or Table 4 must be used.
14	PLC	The selected operating mode is copied unchanged from the input range of the bus connection into marker word MW03 in order to transfer it to the F-PLC.
15	F-PLC	It is checked whether new data arrived from the PLC. This is identified by any value other than 0 appearing in MW03.
16	F-PLC	MW01 must contain one of the permissible codes. If an impermissible code appears, the system must branch to error mode. It must be borne in mind here that the definition of the value range for MW01 and for SelectMSO from Table 2 or Table 4 must be used. Figure 4 contains a sequence that describes this step in detail.
17	F-PLC	The selected operating mode must be within the permissible range. It must be borne in mind here that the definition of the value range for MW01 and ReadAuthorization, as well as MW03 and SelectMSO, from Table 2 or Table 4 must be used. Figure 4 contains a sequence that describes this step in detail.
18	F-PLC	MW03 must contain one of the permissible codes. If an impermissible code appears, the system must branch to error mode. It must be borne in mind here that the definition of the value range for MW03 and SelectMSO from Table 2 or Table 4 must be used. Figure 5 contains a sequence that describes this step in detail.

19	F-PLC	Only if the check produced an OK result will feedback be provided in MW05. It must be borne in mind here that the definition of the value range for MW05 and CheckMSO from Table 2 or Table 4 must be used. Figure 5 contains a sequence that describes this step in detail.
20	PLC	Marker word MW05 from the PLC is copied over unchanged into the output range for the HMI so that it can be read in the HMI.
21	HMI	The operating mode reported back in MW05 must be displayed in the HMI so that the user can confirm it. It is asked whether everything is OK (check as to whether the displayed operating mode corresponds to the previously selected one, or Yes or No). A new input field must be produced in the HMI for this purpose; the previously used input field from step 12 must not be used. The acknowledgment must be input in a different position (in both the X and the Y coordinates) on the touchscreen to the previous operating mode from step 12. The acknowledgment must not be at the same place on the touchscreen where the selected operating mode was confirmed.
22	HMI	The user must confirm the displayed operating mode.
23	HMI	Once the operating mode has been acknowledged, the value for the selected operating mode is written to SwitchMSO and is sent to the PLC via the bus. It must be borne in mind here that the definition of the value range for MW07 and SwitchMSO from Table 2 or Table 4 must be used.
24	HMI	As negative acknowledgment, the HMI identifies that an error occurred. This information is sent via the bus.
25	PLC	The selected operating mode is copied from the input range of the bus connection into marker word MW07 in order to transfer it to the F-PLC.
26	F-PLC	MW07 must contain one of the permissible codes. If an impermissible code appears, the system must branch to error mode. It must be borne in mind here that the definition of the value range for MW07 and SelectMSO from Table 2 or Table 4 must be used. Figure 6 contains a sequence that describes this step in detail.
27	F-PLC	A comparison is performed to determine whether the originally selected operating mode MW03 corresponds to the acknowledged operating mode MW07. Figure 6 contains a sequence that describes this step in detail.
28	F-PLC	If it corresponds, switchover to the new operating mode from MW07 takes place.

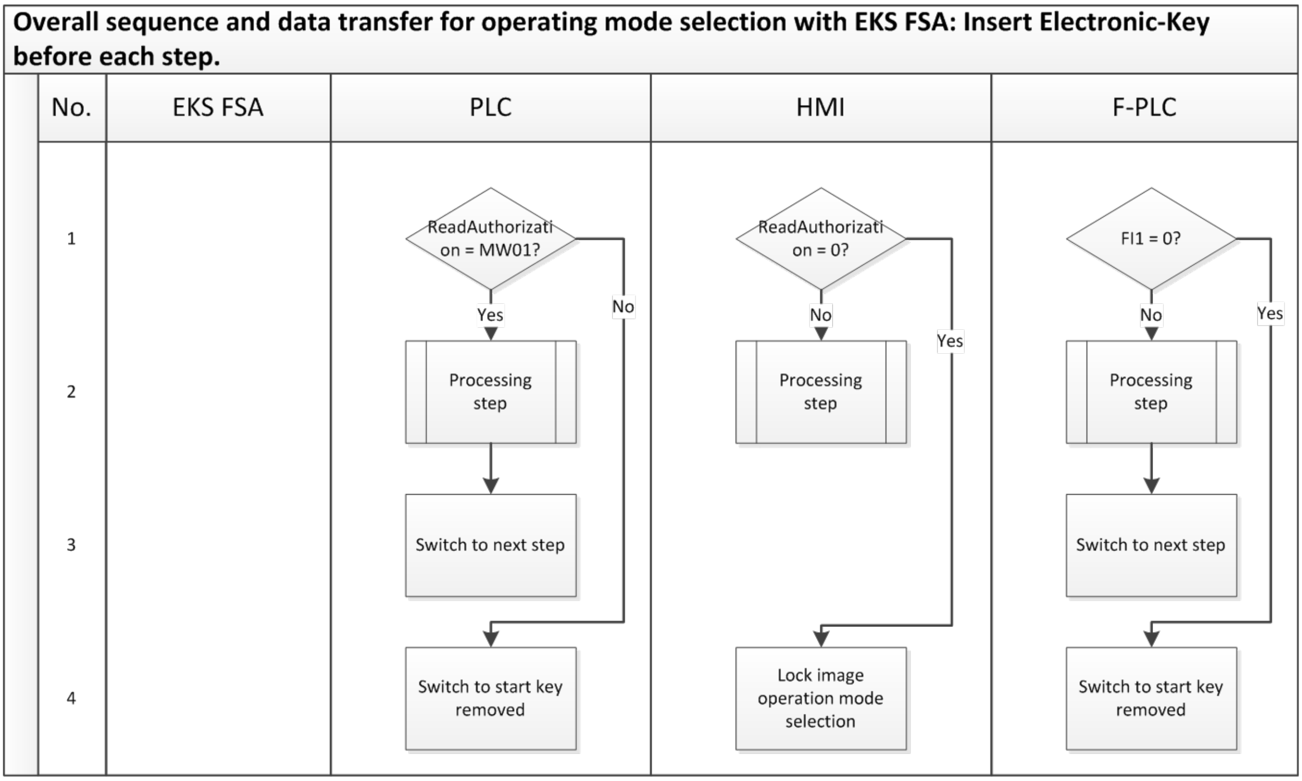
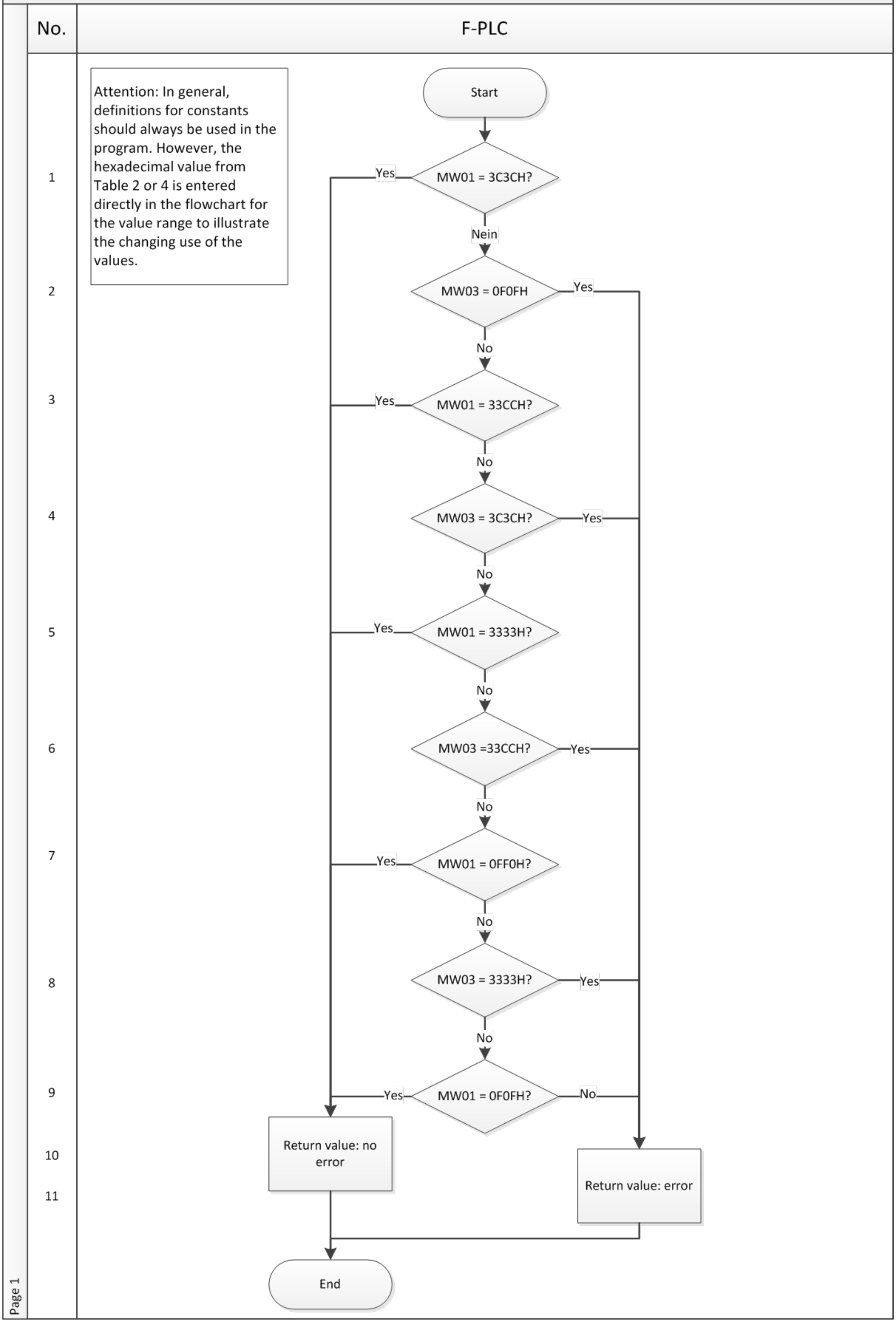

Overall sequence and data transfer for operating mode selection with EKS FSA: Insert Electronic-Key before each step.
No.
EKS FSA
PLC
HMI
F-PLC
1
2
3
4
ReadAuthorization = MW01?
Yes
No
Processing step
Switch to next step
Switch to start key removed
ReadAuthorization = 0?
No
Yes
Processing step
Lock image operation mode selection
FI1 = 0?
No
Yes
Processing step
Switch to next step
Switch to start key removed

Figure 3

The synchronous sequence in the PLC, HMI and F-PLC systems can reveal differences in the systems (channels). For this reason, the sequence from Figure 3 must be programmed or called before every individual step in the sequence diagram from Figures 2. These sequence steps must also be processed prior to the error routine. This ensures that system recovery can be realized by removal of the Electronic-Key if a fault is not permanent (e.g. initiated by the user).

Step	System	Description
1	PLC	It is checked whether the data in the input range are unchanged compared to the last data forwarded to the F-PLC. It must be borne in mind here that the definition of MW01 and the ReadAuthorization from Table 2 or Table 4 must be used. As the same values are used for the variables, a direct comparison can be made.
1	HMI	It is checked whether a PLC release for the “Operating mode input” screen still exists.
1	F-PLC	It is checked whether the EKS *FSA* still displays that an Electronic-Key is inserted.
2	PLC HMI F-PLC	The step to be run from the sequence diagram in Figure 2 is processed.
3	PLC F-PLC	In the status, it is switched to the next step from the sequence diagram in Figure 2.
4	PLC	It is switched to the start of the “Electronic-Key is removed” routine.
4	HMI	Access to the operating mode selection screen is blocked.
4	F-PLC	It is switched to the start of the “Electronic-Key is removed” routine.

Subroutine on Electronic-Key insertion: Step 16 and step 17 (MW01 valid and MW01 >= MW03)

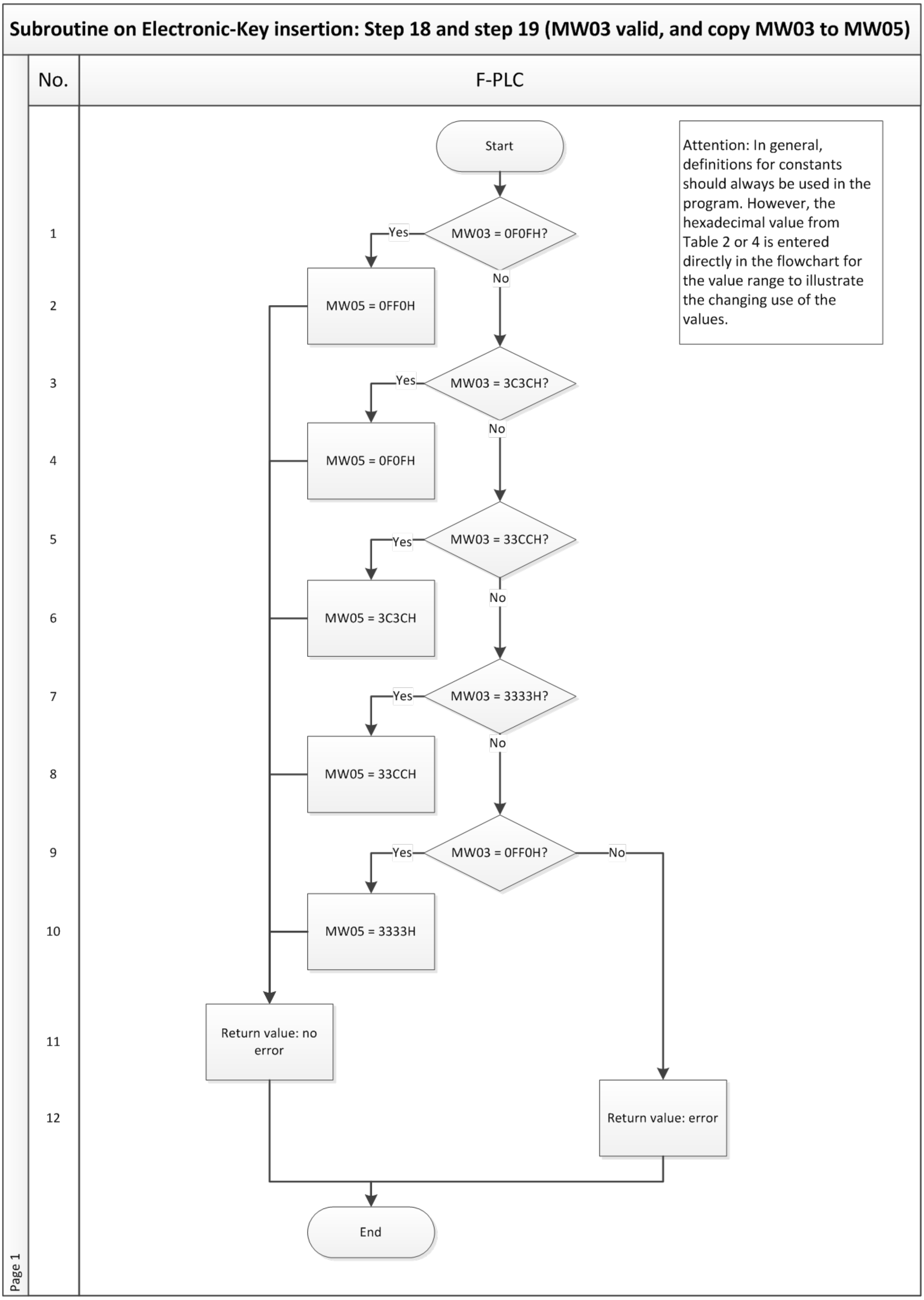


Attention: In general, definitions for constants should always be used in the program. However, the hexadecimal value from Table 2 or 4 is entered directly in the flowchart for the value range to illustrate the changing use of the values.

Figure 4

Subject to technical modifications; no responsibility is accepted for the accuracy of this information. © EUCHNER 2015

Step	System	Description
1	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW01 (permissible operating mode). In MW01, this is indicated by the value 3C3CH. If YES, every selected operating mode is valid as long as the transmitted data word has a valid value in MW03 (check in step 18). Work can continue without an error message.
2	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 0F0FH. If YES, an impermissible operating mode was selected, because there is no authorization for this operating mode in MW01.
3	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW01 (permissible operating mode). In MW01, this is indicated by the value 33CCH. If YES, every selected operating mode is valid as long as the transmitted data word has a valid value in MW03 (check in step 18). Work can continue without an error message.
4	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3C3CH. If YES, an impermissible operating mode was selected, because there is no authorization for this operating mode in MW01.
5	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW01 (permissible operating mode). In MW01, this is indicated by the value 3333H. If YES, every selected operating mode is valid as long as the transmitted data word has a valid value in MW03 (check in step 18). Work can continue without an error message.
6	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 33CCH. If YES, an impermissible operating mode was selected, because there is no authorization for this operating mode in MW01.
7	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW01 (permissible operating mode). In MW01, this is indicated by the value 0FF0H. If YES, every selected operating mode is valid as long as the transmitted data word has a valid value in MW03 (check in step 18). Work can continue without an error message.
8	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3333H. If YES, an impermissible operating mode was selected, because there is no authorization for this operating mode in MW01.
9	F-PLC	It is checked whether the last authorization level (MSO 0) is stored in MW01 (permissible operating mode). In MW01, this is indicated by the value 0F0FH. If YES, the selected operating mode is valid as long as the transmitted data word has a valid value in MW03 (check in step 18). Work can continue without an error message. If No, MW01 is invalid.
10	F-PLC	It is reported that no error occurred.
11	F-PLC	It is reported that an error occurred.

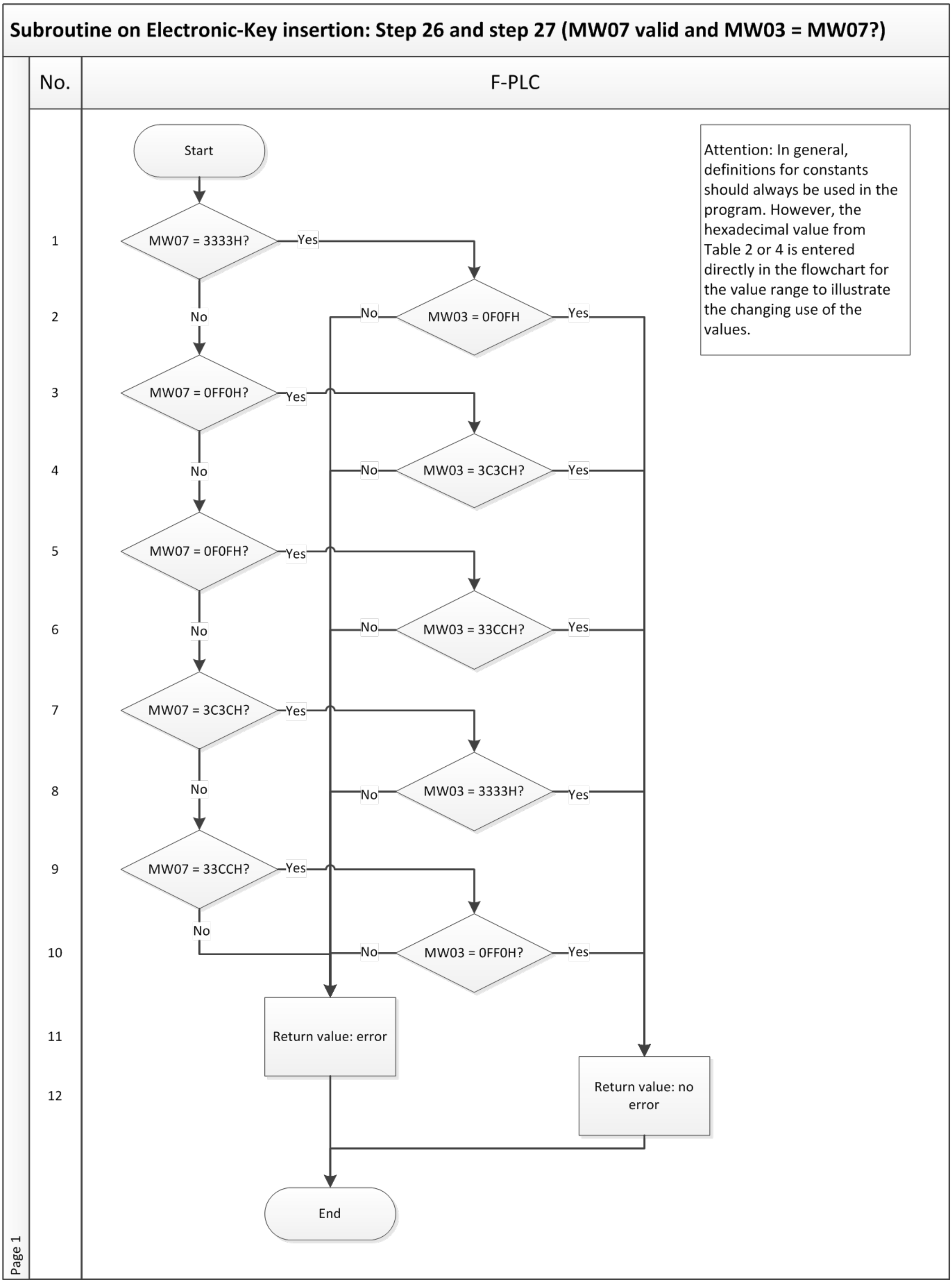


Attention: In general, definitions for constants should always be used in the program. However, the hexadecimal value from Table 2 or 4 is entered directly in the flowchart for the value range to illustrate the changing use of the values.

Figure 5

Subject to technical modifications; no responsibility is accepted for the accuracy of this information. © EUCHNER 2015

Step	System	Description
1	F-PLC	It is checked whether authorization level MSO 4 is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 0F0FH. If YES, the associated value can be stored in MW05. IF NO, the check continues.
2	F-PLC	The value for authorization level MSO 4 is stored in MW05 (operating mode to be checked). In MW05, this is indicated by the value 0FF0H.
3	F-PLC	It is checked whether authorization level MSO 3 is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3C3CH. If YES, the associated value can be stored in MW05. IF NO, the check continues.
4	F-PLC	The value for authorization level MSO 3 is stored in MW05 (operating mode to be checked). In MW05, this is indicated by the value 0F0FH.
5	F-PLC	It is checked whether authorization level MSO 2 is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 33CCH. If YES, the associated value can be stored in MW05. IF NO, the check continues.
6	F-PLC	The value for authorization level MSO 2 is stored in MW05 (operating mode to be checked). In MW05, this is indicated by the value 3C3CH.
7	F-PLC	It is checked whether authorization level MSO 1 is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3333H. If YES, the associated value can be stored in MW05. IF NO, the check continues.
8	F-PLC	The value for authorization level MSO 1 is stored in MW05 (operating mode to be checked). In MW05, this is indicated by the value 33CCH.
9	F-PLC	It is checked whether authorization level MSO 0 is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 0FF0H. If YES, the associated value can be stored in MW05. If NO, an error is reported.
10	F-PLC	The value for authorization level MSO 0 is stored in MW05 (operating mode to be checked). In MW05, this is indicated by the value 3333H.
11	F-PLC	It is reported that no error occurred.
12	F-PLC	It is reported that an error occurred.



Attention: In general, definitions for constants should always be used in the program. However, the hexadecimal value from Table 2 or 4 is entered directly in the flowchart for the value range to illustrate the changing use of the values.

Figure 6

Step	System	Description
1	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW07 (acknowledged operating mode). In MW07, this is indicated by the value 3333H. If YES, it can be checked whether this is also true for the previously selected operating mode.
2	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 0F0FH. If YES, switchover to this operating mode can take place.
3	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW07 (acknowledged operating mode). In MW07, this is indicated by the value 0FF0H. If YES, it can be checked whether this is also true for the previously selected operating mode.
4	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3C3CH. If YES, switchover to this operating mode can take place.
5	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW07 (acknowledged operating mode). In MW07, this is indicated by the value 0FF0H. If YES, it can be checked whether this is also true for the previously selected operating mode.
6	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 33CCH. If YES, switchover to this operating mode can take place.
7	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW07 (acknowledged operating mode). In MW07, this is indicated by the value 3C3CH. If YES, it can be checked whether this is also true for the previously selected operating mode.
8	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 3333H. If YES, switchover to this operating mode can take place.
9	F-PLC	It is checked whether the last authorization level (MSO 0) is stored in MW07 (acknowledged operating mode). In MW07, this is indicated by the value 33CCH. If YES, it can be checked whether this is also true for the previously selected operating mode.
10	F-PLC	It is checked whether the last authorization level (MSO 0) is stored in MW03 (selected operating mode). In MW03, this is indicated by the value 0FF0H. If YES, switchover to this operating mode can take place.
11	F-PLC	It is reported that no error occurred.
12	F-PLC	It is reported that an error occurred.

Removing an EKS Electronic-Key

The entire sequence is depicted in the flowcharts in Figures 7.1 to 7.2. Transfer variables are shown in red.

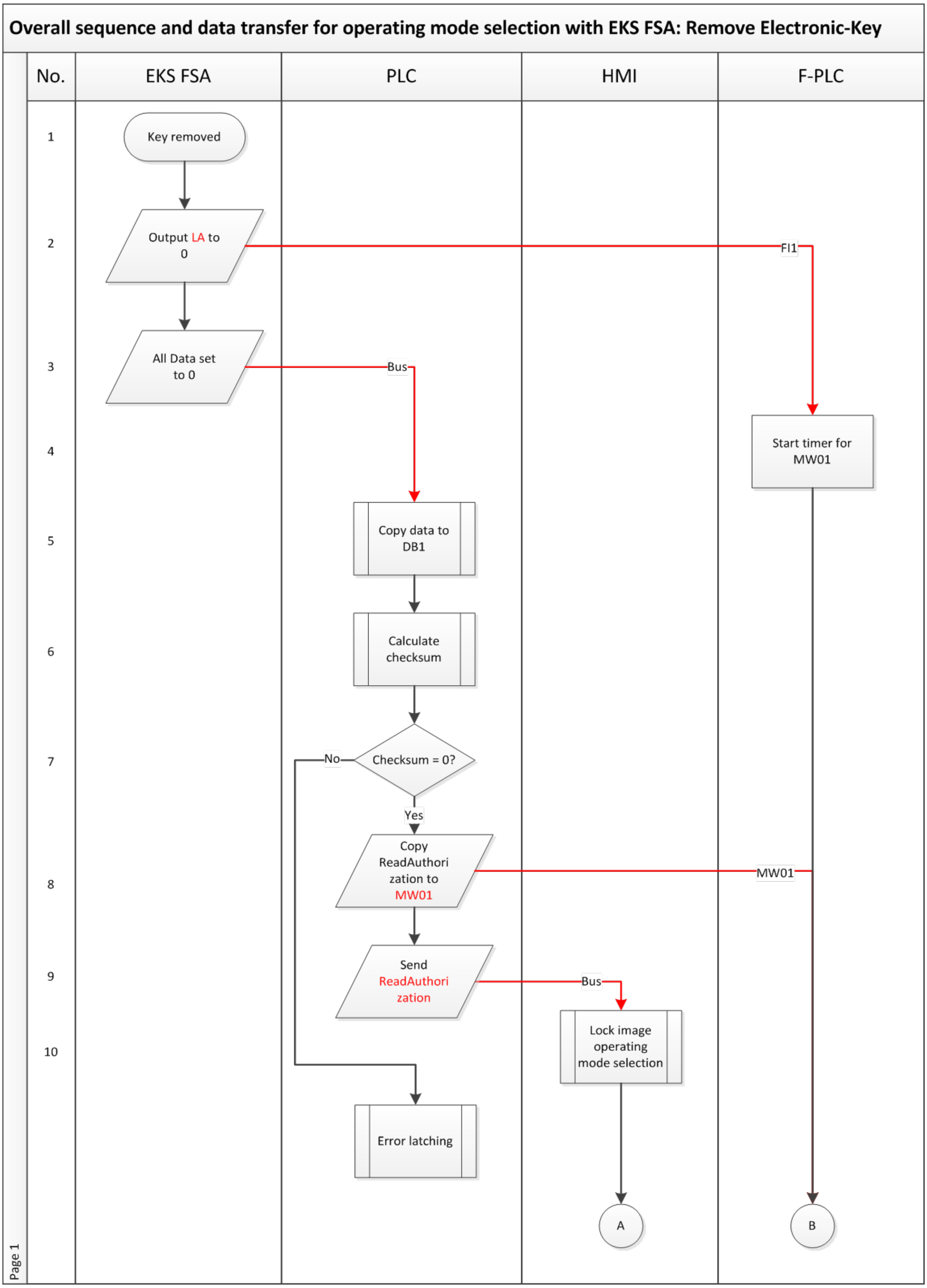


Figure 7.1

Overall sequence and data transfer for operating mode selection with EKS FSA: Remove Electronic-Key

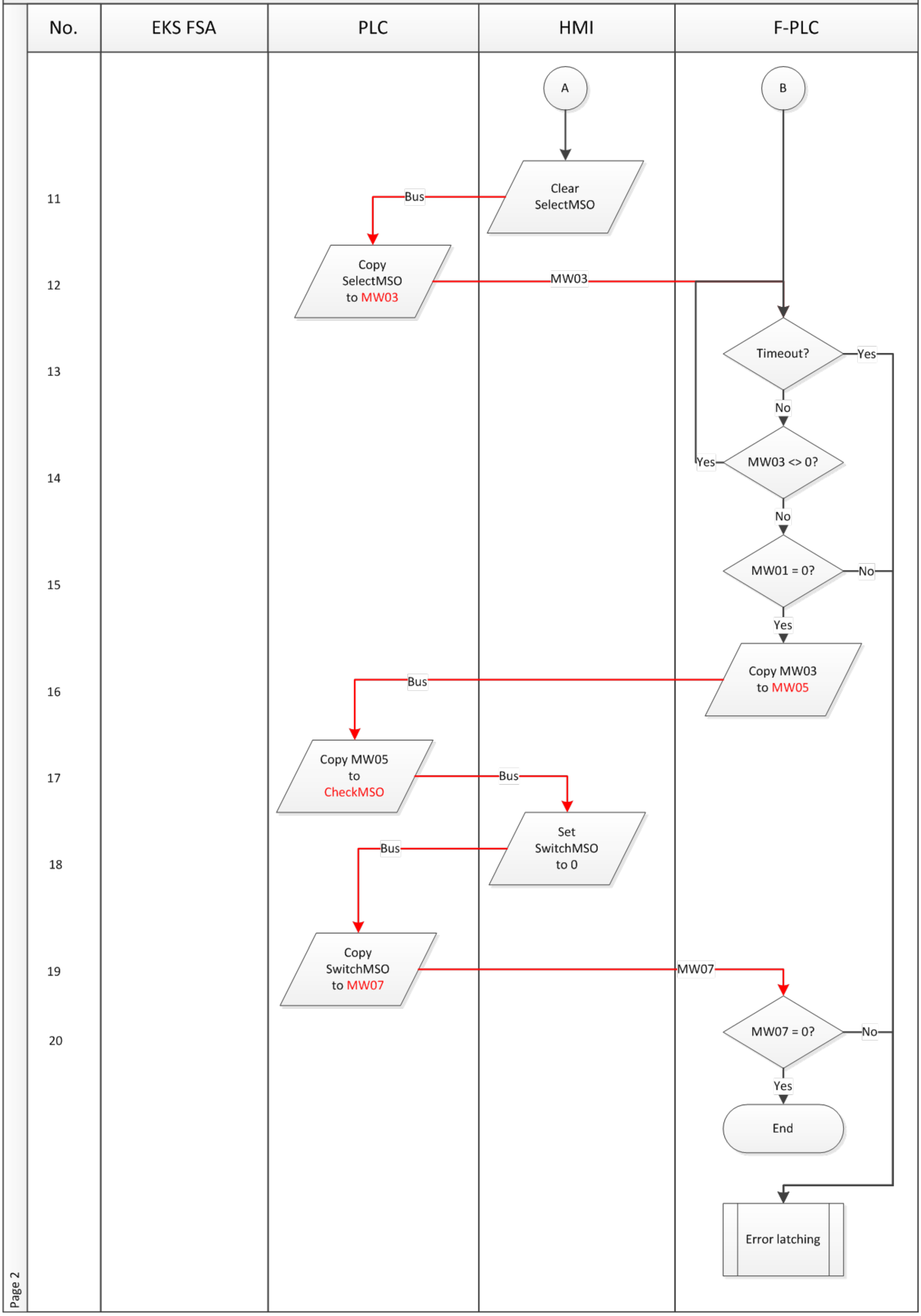


Figure 7.2

Description:

Step	System	Description
1	EKS *FSA*	A user removes an Electronic-Key.
2	EKS *FSA*	When an Electronic-Key is removed, output LA is set to 0.
3	EKS *FSA*	Without an Electronic-Key, the EKS *FSA* sends only zeros as data over the bus.
4	F-PLC	A time expectation (approx. 1 s) is started in the safe PLC for transmission of the associated data (zeros) from the PLC after safe input FI1 is erased.
5	PLC	All Electronic-Key data are read in by the PLC in the defined input range and are copied over into a global data block from there.
6	PLC	The checksum of the Electronic-Key content is calculated. Information about whether the checksum is OK is then returned as a bit. (Refer to application AP000169-5… for this purpose)
7	PLC	The checksum calculation must result in 0.
8	PLC	The data from the range of the data block at the access authorization location are copied over to marker word MW01 to provide the data to the F-PLC.
9	PLC	The PLC sends the content of ReadAuthorization to the HMI via the bus system.
10	HMI	Owing to the lack of access authorization, the HMI must block the operating mode selection screen to prevent any more changes. The currently selected operating mode remains active and must continue to be displayed.
11	HMI	As feedback, the HMI returns the zero as the newly selected operating mode.
12	PLC	The data from the HMI are copied over into marker word MW03 so that they are accessible for the F-PLC.
13	F-PLC	Max. the set time is waited.
14	F-PLC	It is checked whether zeros are sent as data in marker word MW03 by the HMI and PLC. This checks the correct sequence by the PLC and the HMI.
15	F-PLC	It is checked whether a zero is sent in marker word MW01 as well.
16	F-PLC	To continue checking the path through the PLC and HMI, the MW05 is set to zero in response.
17	PLC	The PLC copies data word MW05 directly over to the output range and forwards the data to the HMI.
18	HMI	The HMI returns the zero as the acknowledged operating mode.
19	PLC	The data from the HMI are copied over into marker word MW07 so that they are accessible for the F-PLC.
20	F-PLC	The F-PLC checks whether the zero was returned in this marker word MW07.

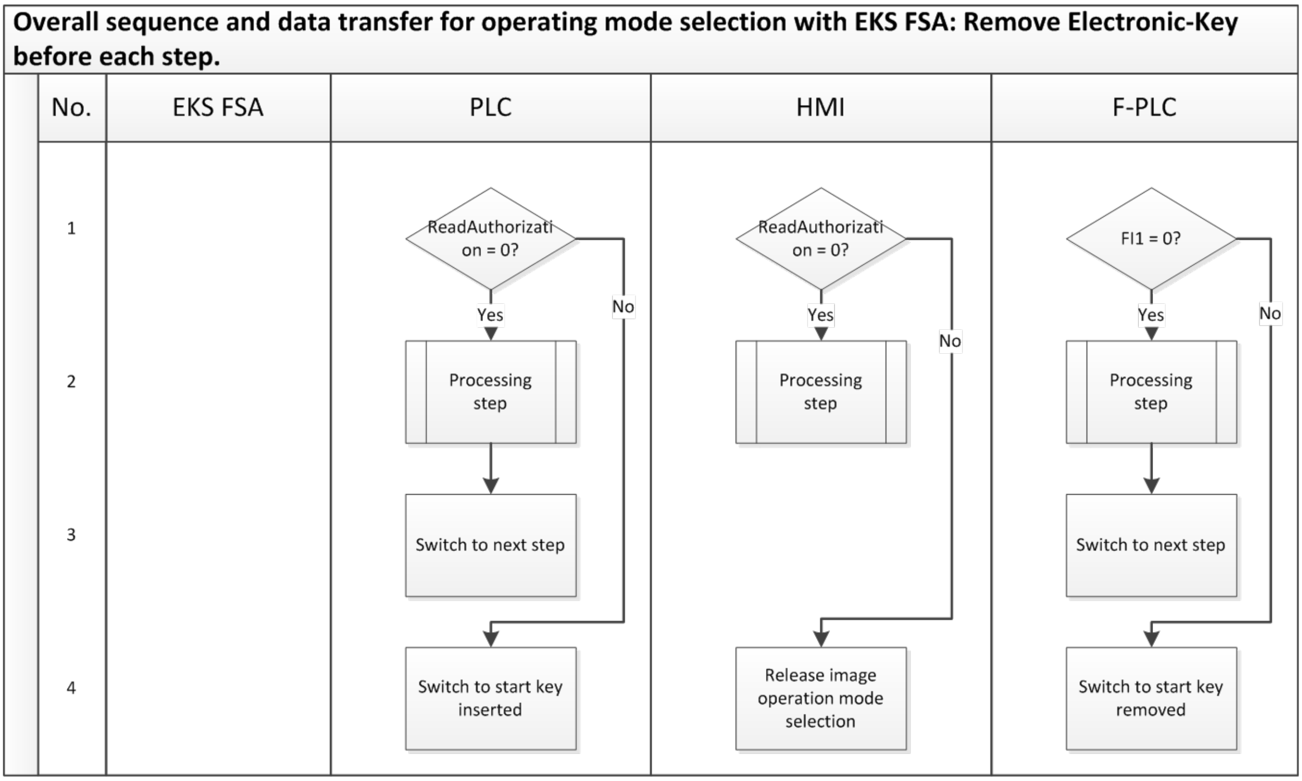

Overall sequence and data transfer for operating mode selection with EKS FSA: Remove Electronic-Key before each step.
No.
EKS FSA
PLC
HMI
F-PLC
1
2
3
4
ReadAuthorization = 0?
Yes
No
Processing step
Switch to next step
Switch to start key inserted
ReadAuthorization = 0?
Yes
No
Processing step
Release image operation mode selection
FI1 = 0?
Yes
No
Processing step
Switch to next step
Switch to start key removed

Figure 8

The synchronous sequence in the PLC, HMI and F-PLC systems can reveal differences in the systems (channels). This represents fault detection as defined in EN ISO 13849-1. For this reason, the sequence from Figure 8 must be programmed or called before every individual step in the sequence diagram from Figure 7.
These sequence steps must also be processed prior to the error routine. This ensures that system recovery can be realized by insertion of the Electronic-Key if a fault is not permanent (e.g. initiated by the user).

Step	System	Description
1	PLC	It is checked whether the data in the input range are still zeros.
1	HMI	It is checked whether a PLC block for the “Operating mode input” screen still exists.
1	F-PLC	It is checked whether the EKS *FSA* still displays that no Electronic-Key is inserted.
2	PLC HMI F-PLC	The step to be run from the sequence diagram in Figure 4 is processed.
3	PLC F-PLC	In the status, it is switched to the next step from the sequence diagram in Figure 4.
4	PLC	It is switched to the start of the “Electronic-Key is inserted” routine.
4	HMI	Access to the operating mode selection screen is enabled.
4	F-PLC	It is switched to the start of the “Electronic-Key is inserted” routine.

Principle circuit diagram

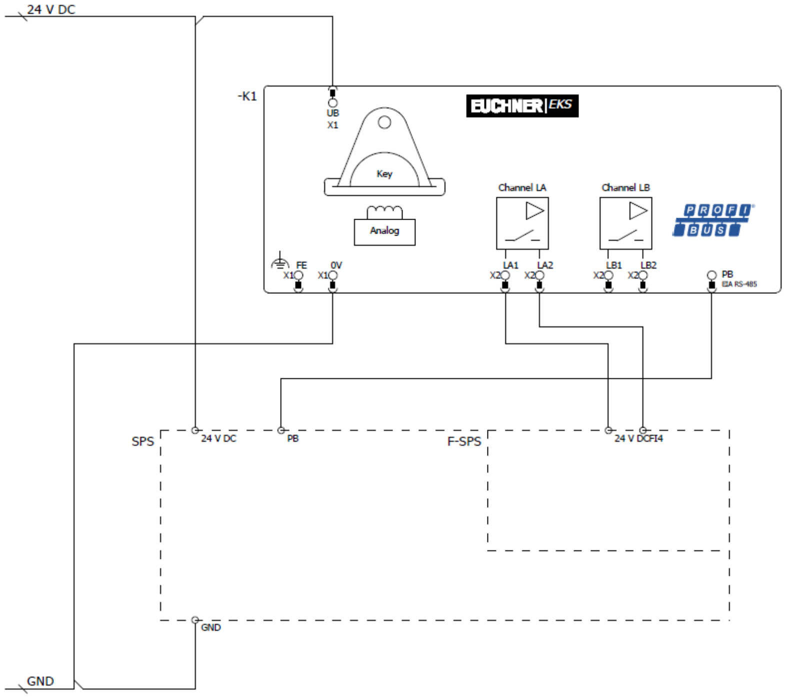


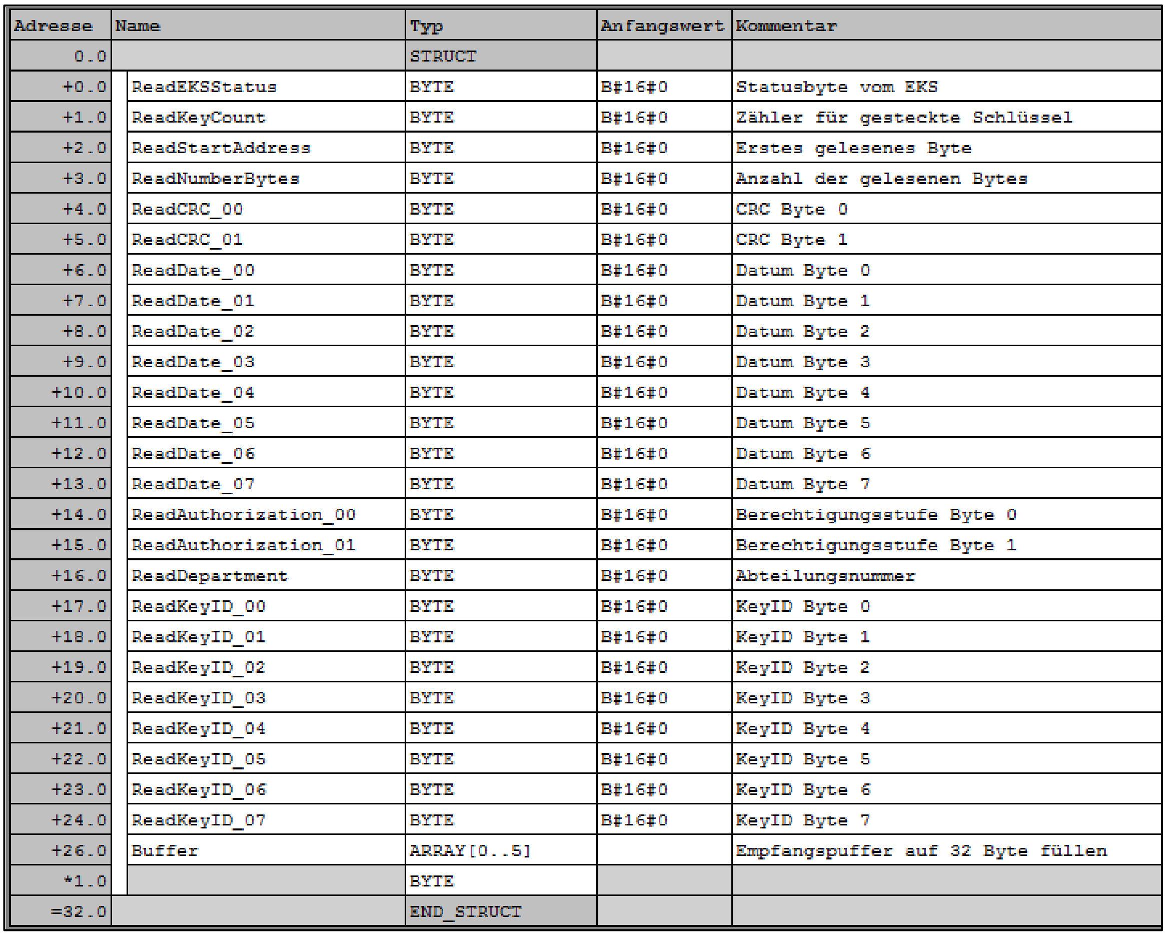
Figure 9

Data in the control system

Global data block

A global data block containing the content of the Electronic-Key is created when an Electronic-Key is inserted. If no Electronic-Key is inserted, the content of the data block is set to zero by the EKS transmission. This allows all routines and memory areas to be checked for a proper sequence.
The data are created in a structured manner in the data block for reading, with all data items longer than one byte being created as individual bytes to circumvent the even-numbered alignment in the control system.

DB1, ReadBufferEKS
The data block shown in Figure 10 is suitable for example AP000169-3…, in which the EKS is used with Profibus.
Data block DB1 must have a somewhat different structure with a Profinet EKS. Bytes 1 to 3 are not used for Profinet (ReadKeyCount, ReadStartAddress, ReadNumberBytes). The corresponding lines are omitted in DB1 for the EKS Profinet.



Adresse	Name	Typ	Anfangswert	Kommentar
0.0		STRUCT		
+0.0	ReadEKSStatus	BYTE	B#16#0	Statusbyte vom EKS
+1.0	ReadKeyCount	BYTE	B#16#0	Zähler für gesteckte Schlüssel
+2.0	ReadStartAddress	BYTE	B#16#0	Erstes gelesenes Byte
+3.0	ReadNumberBytes	BYTE	B#16#0	Anzahl der gelesenen Bytes
+4.0	ReadCRC_00	BYTE	B#16#0	CRC Byte 0
+5.0	ReadCRC_01	BYTE	B#16#0	CRC Byte 1
+6.0	ReadDate_00	BYTE	B#16#0	Datum Byte 0
+7.0	ReadDate_01	BYTE	B#16#0	Datum Byte 1
+8.0	ReadDate_02	BYTE	B#16#0	Datum Byte 2
+9.0	ReadDate_03	BYTE	B#16#0	Datum Byte 3
+10.0	ReadDate_04	BYTE	B#16#0	Datum Byte 4
+11.0	ReadDate_05	BYTE	B#16#0	Datum Byte 5
+12.0	ReadDate_06	BYTE	B#16#0	Datum Byte 6
+13.0	ReadDate_07	BYTE	B#16#0	Datum Byte 7
+14.0	ReadAuthorization_00	BYTE	B#16#0	Berechtigungsstufe Byte 0
+15.0	ReadAuthorization_01	BYTE	B#16#0	Berechtigungsstufe Byte 1
+16.0	ReadDepartment	BYTE	B#16#0	Abteilungsnummer
+17.0	ReadKeyID_00	BYTE	B#16#0	KeyID Byte 0
+18.0	ReadKeyID_01	BYTE	B#16#0	KeyID Byte 1
+19.0	ReadKeyID_02	BYTE	B#16#0	KeyID Byte 2
+20.0	ReadKeyID_03	BYTE	B#16#0	KeyID Byte 3
+21.0	ReadKeyID_04	BYTE	B#16#0	KeyID Byte 4
+22.0	ReadKeyID_05	BYTE	B#16#0	KeyID Byte 5
+23.0	ReadKeyID_06	BYTE	B#16#0	KeyID Byte 6
+24.0	ReadKeyID_07	BYTE	B#16#0	KeyID Byte 7
+26.0	Buffer	ARRAY[0..5]		Empfangspuffer auf 32 Byte füllen
*1.0		BYTE		
=32.0		END_STRUCT		

Figure 10

Safety description

EKS FSA

In the first channel of the EKS *FSA,* the data – and thus the access authorization – are read from the inserted Electronic-Key. The result is reported as access authorization to the PLC via the bus. The PLC forwards the data unchanged to the safe PLC and to the HMI. It is thereby checked in the HMI that an operating mode is selected only within the value range, and it is checked in the safe PLC whether the value range was observed.

In the second channel of the EKS *FSA*, it is checked whether a valid Electronic-Key is inserted. The result is issued on output LA, which is connected to the F-PLC. The output of the second channel is switched on only if a valid Electronic-Key is detected in the first channel as well. The F-PLC permits switchover of the operating mode only if this input is switched on, and it checks whether switchover is even permissible.

When the Electronic-Key is removed, the EKS *FSA* sends only zeros as data. The authorization level is thereby also set to 0. This is sent to the HMI so that the HMI switches off operating mode selection. As acknowledgment, the return value from the HMI is also set to 0. This is transmitted to the F-PLC. The output of the second channel of the EKS *FSA* is also reset. This way, the F-PLC checks whether the zero was transmitted to all control systems involved.
Data falsification is possible on the transmission links (bus systems) or in the memory of the various systems. According to GS-ET-26, the selected codes with a data word with 16 bits and a Hamming distance of 8 results in a residual error probability of:

$$R(p) \approx 1{,}2 \cdot 10^{-12}$$

When an 8-bit code with a Hamming distance of 5 is used, the resulting residual error probability is:

$$R(p) \approx 5{,}43 \cdot 10^{-9}$$

This low residual error probability ensures that no incorrect operating mode can be selected through the EKS *FSA*. This residual error probability is not included in the calculation to determine the PFH_d of the overall system. The EKS *FSA* serves only as an access system for operating mode selection and therefore is not included in the calculation of the Performance Level.

PLC with touchscreen

In the HMI, switchover to the screen with operating mode selection takes place only when authorization is present at the EKS *FSA* inputs.
Only those touchscreen buttons that can be selected according to the inserted Electronic-Key are released.
The selected operating mode is transmitted to the PLC and from there to the safe PLC. The safe PLC returns an acknowledgment with the selected operating mode, which must be displayed. This must be acknowledged by the user. The procedure corresponds to safe parameter input in accordance with section 4.6.4 of EN ISO 13849-1:2008.
Several measures are implemented to ensure the integrity of the data that have to be exchanged for this purpose.

- Validity check of all data in the F-PLC
- Management of data falsification through the large Hamming distance
- Plausibility checks of sequences in order to reveal errors in the hardware and software
- Change in the meaning of the data words in the various selection levels in order to prevent overwriting of the memory or incorrect storage of data

The operating mode remains set when the Electronic-Key is removed and the corresponding screen in the HMI is no longer shown.
The failure probability of the HMI and PLC does not have to be included in the calculation of the failure probability of the safety function, because the HMI and PLC are used only for data input corresponding to the procedure specified by EN ISO 13849-1.

F-PLC

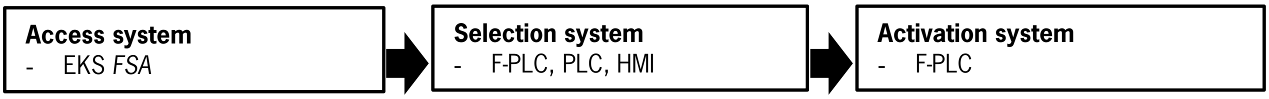
In the F-PLC, operating mode selection is realized as a 1 of N system (only one operating mode can be selected).
The F-PLC can fulfill the conditions of a PL e system according to EN ISO 13849-1, provided that this is permitted by the PL of the F-PLC and provided that all measures are observed during software creation. Refer to the next section for more information about this.
The F-PLC serves to reveal errors in all devices and components involved. The procedure for selecting the operating mode must be implemented in the F-PLC.
The failure probability of the F-PLC is included as the actual operating mode switchover in the calculation of the PL.

Software

The software in the F-PLC is relevant to safety. The methods and measures described in section 4.6.3 of EN ISO 13849-1:2008 for SRASW are to be used to create and asses the software in the F-PLC. The software must be validated according to section 9.5 of EN ISO 13849-2:2013.
Creation of the software in the PLC and HMI must correspond to section 4.6.4 of EN ISO 13849-1:2008. The methodology introduced in this application satisfies these requirements, but the programming must also be implemented accordingly. The software must be verified according to section 4.6.4.

Summary

The safety assessment of an operating mode comprises three blocks:



Access system
- EKS *FSA*

Selection system
- F-PLC, PLC, HMI

Activation system
- F-PLC

The safety function for operating mode selection means: activation of the safety functions required for the selected operating mode. Operating mode selection switches between different safety systems, for example: closed safety door in automatic mode and enabling switch together with limited speed with open safety door.

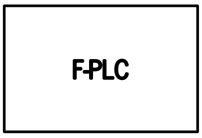
The access system serves to meet the requirements of the Machinery Directive for restricting access to certain groups of people.
The selection system is the selection of the required operating mode by the user. In this example, user input is via the touchscreen.
The activation system activates or deactivates the safety sensors and actuators according to the selected operating mode. Example: an enabling switch can be activated in setup mode, but certain feed movements can be disabled.
Tip: More detailed information about safety-related operating modes can be found in DGUV Information FB HM-073.

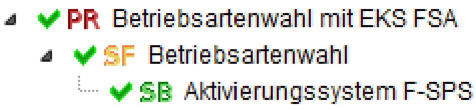
The access system does not have to be evaluated with a PL, but it is part of the safety system. Access restriction must be at least equivalent to that of a mechanical key. This security is achieved through the coding of the Electronic-Key and the two-channel structure. Moreover, the EKS *FSA* offers a personalization function because assignment of the Electronic-Key to a specific person is possible. A high level of protection against copying of an Electronic-Key is also provided.
In this application, one of the functions of the EKS *FSA* is to trigger error checking in the F-PLC in order to monitor the EKS *FSA*, the PLC and the HMI for proper functioning.

In this example, the system comprising the PLC, HMI and F-PLC forms the selection system to be assessed in terms of safety. In the implementation of operating mode selection in accordance with this application, the operating mode selection system can be regarded as being equivalent to a key-operated rotary switch in terms of safety. A PL cannot be assigned to the selection system in this example, because operating mode selection is a parameter assignment based on software measures according to section 4.6.4 of EN ISO 13849-1:2008 (software-based parameter assignment).
The activation system must comply with the PL_r from the risk assessment of the machine for operating mode switchover. With exclusive use of the F-PLC as the activation system, the resulting PL is the PL of the F-PLC (PL e). It must be noted that the software must be created according to section 4.6.3 of EN ISO 13849-1:2008 and validated according to section 9.5 of EN ISO 13849-2:2013. If other systems connected behind the F-PLC (e.g. contactors and valves) are also involved in the operating mode switchover, they must be included in the assessment of the PL.

This allows the safety function “Activation of the safety functions required for the selected operating mode” to be performed with a Performance Level of up to PL e.

Safety block diagram:





✓ PR Betriebsartenwahl mit EKS FSA
✓ SF Betriebsartenwahl
✓ SB Aktivierungssystem F-SPS

F-SPS	F-PLC
Betriebsartenanwahl mit EKS FSA	Operating mode selection with EKS FSA
Betriebsartenanwahl	Operating mode selection
Aktivierungssystem F-SPS	F-PLC activation system

Important note – please observe carefully!

This document is intended for a design engineer who possesses the requisite knowledge in safety engineering and knows the applicable standards, e.g. through training for qualification as a safety engineer. Only with the appropriate qualification is it possible to integrate the introduced example into a complete safety chain.

The example represents only part of a complete safety chain and does not fulfill any safety function on its own. In order to fulfill a safety function, the energy switch-off function for the hazard location and the software within the safety evaluation must also be considered, for example.

The introduced applications are only examples for solving certain safety tasks for protecting safety doors. The examples cannot be comprehensive due to the application-dependent and individual protection goals within a machine/installation.

If questions concerning this example remain open, please contact us directly.

In accordance with Machinery Directive 2006/42/EC, the design engineer of a machine or installation is obligated to perform a risk assessment and take measures to reduce the risk. When doing this, the engineer must comply with the applicable national and international standards. Standards generally represent the current state of the art. Therefore, the design engineer should continuously inform himself about changes in the standards and adapt his considerations to them. Relevant standards include EN ISO 13849 and EN 62061. This application must be regarded only as assistance for the considerations about safety measures.

The design engineer of a machine/installation is obligated to assess the safety technology itself. The examples must not be used for assessment, because only a small excerpt of a complete safety function was considered in terms of safety engineering here.

In order to be able to use the safety switch applications correctly on safety doors, it is indispensable to observe the standards EN ISO 13849-1, EN ISO 14119 and all relevant C-standards for the respective machine type. Under no circumstances does this document replace the engineer's own risk assessment, and it cannot serve as the basis for a fault assessment.

Particularly in case of fault exclusion, it must be noted that this can be performed only by the design engineer of a machine or installation and requires a reason. General fault exclusion is not possible. More information about fault exclusion can be found in EN ISO 13849-2.

Changes to products or within assemblies from third-party suppliers used in this example can lead to the function no longer being ensured or the safety assessment having to be adapted. In any event, the information in the operating instructions on the part of EUCHNER, as well as on the part of third-party suppliers, must be used as the basis before this application is integrated into an overall safety function. If contradictions should arise between the operating instructions and this document, please contact us directly.

Use of brand names and company names

All brand names and company names stated are the property of the related manufacturer. They are used only for the clear identification of compatible peripheral devices and operating environments in relation to our products.