EKS Light *FSA* on Siemens S7-300 – operation mode selection with touchscreen

Contents

Components/modules used

EUCHNER

Description	Order no./item designation
EKS Light *FSA* compact	112207 / EKS-A-IPLA-G01-ST05/04
or	
EKS Light *FSA* modular	113645 / EKS-A-APRA-G08
EKS FHM	106585 / EKS-A-SFH-G30-2000
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.com. 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 light *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 flag words
HMI	The human-machine interface comprising a screen with touch-sensitive surface or softkeys.
MW	Flag 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

Operation mode selection is to be realized on a machine using the EKS light *FSA* as an access system. The operation 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 operation mode are realized via a safe programmable logic controller (F-PLC). With the aid of the EKS light FSA, five authorization levels for access to the operation mode selection can be defined. Which operation modes the owner of the related Electronic-Key can select depends on the authorization level.

Electronic-Key structure

The data on the Electronic-Key are structured as follows.

Byte no.	Description	Type	Length	Explanation
109	Operating state	Byte	1 byte	State of the EKS light *FSA*
110 – 111	Authorization level	Word	2 bytes	Authorization level for access to the machine's operation mode.
112 – 113	Access code	Word	2 bytes	Restriction of the machine or installation group (10 bits)
114 – 115	KEYCRC	CRC	2 bytes	Checksum over a certain part of the Electronic-Key as copy protection.
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.

For this application the value 6 or 7 must be set on the EKS light *FSA* as the operating state. With this value the EKS light *FSA* will operate in the operating state that is necessary for the selection of the operation mode via a touchscreen or softkeys. The same value must also be saved on the Electronic-Key.

In operating state 6 a comparison is made with the access code as to whether the Electronic-Key has the same value as is set on the DIP switches in the device. The Electronic-Key is only accepted if they match fully.

In operating state 7 a comparison is made with the access code as to whether the bit on the Electronic-Key in the same position as the bit that is set on the DIP switches has the value 1. Only if both the Electronic-Key and the DIP switch have a 1 in this bit is the Electronic-Key accepted.

One of the five values from Table 2 for MW01 or ReadAuthorization must be saved in the authorization level field; this value permits the selection of one or more operation modes. The outputs A to D as well as STR are set to suit this field. Each of the 5 outputs represents an allowed authorization level. Only one output is ever set. The safety PLC must check this aspect and, as soon as more than one output is set simultaneously, branch to the fault mode. The assignment of the data words to the outputs is described in Table 2.

A checksum calculated in the EKS light is entered automatically in the KEYCRC field by the EKM light administration program. Only if the checksum calculation produces the same value as that saved on the Electronic-Key are the outputs on the EKS light switched on.

Set of values for the authorization levels for 5 operation 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 corruption of the Electronic-Key. The value zero must not be used. This value is necessary to recognize a removed Electronic-Key. As data transfer between the various systems via the bus must be ensured, the codes for operation mode selection must be selected according to the set of values. Therefore, these data words must also be used within the program.

Definition of the data words for the operation-mode level

To avoid errors due to overwriting of the memory in the PLC, the meaning of operation mode selection **must** change the value in the various memory locations used. For this purpose, Table 2 defines the meaning of operation mode selection in the respective variable or in the data word. This is undertaken by means of constants.

Variable or data word	Definition Operation 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	Output A set. Mode of Safe Operation 0: Manual mode
	RE_MSO_1	0FF0H	Output B set. Mode of Safe Operation 1: Automatic mode
	RE_MSO_2	3333H	Output C set. Mode of Safe Operation 2: Setup mode
	RE_MSO_3	33CCH	Output D set. Mode of Safe Operation 3: Automatic mode with manual intervention
	RE_MSO_4	3C3CH	Output STR set. Mode of Safe Operation Service: Operation 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: Operation 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: Operation 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: Operation 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. For example, with the access authorization MSO3 the outputs LA and C are switched on. All others remain switched off.

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

Block diagram and description

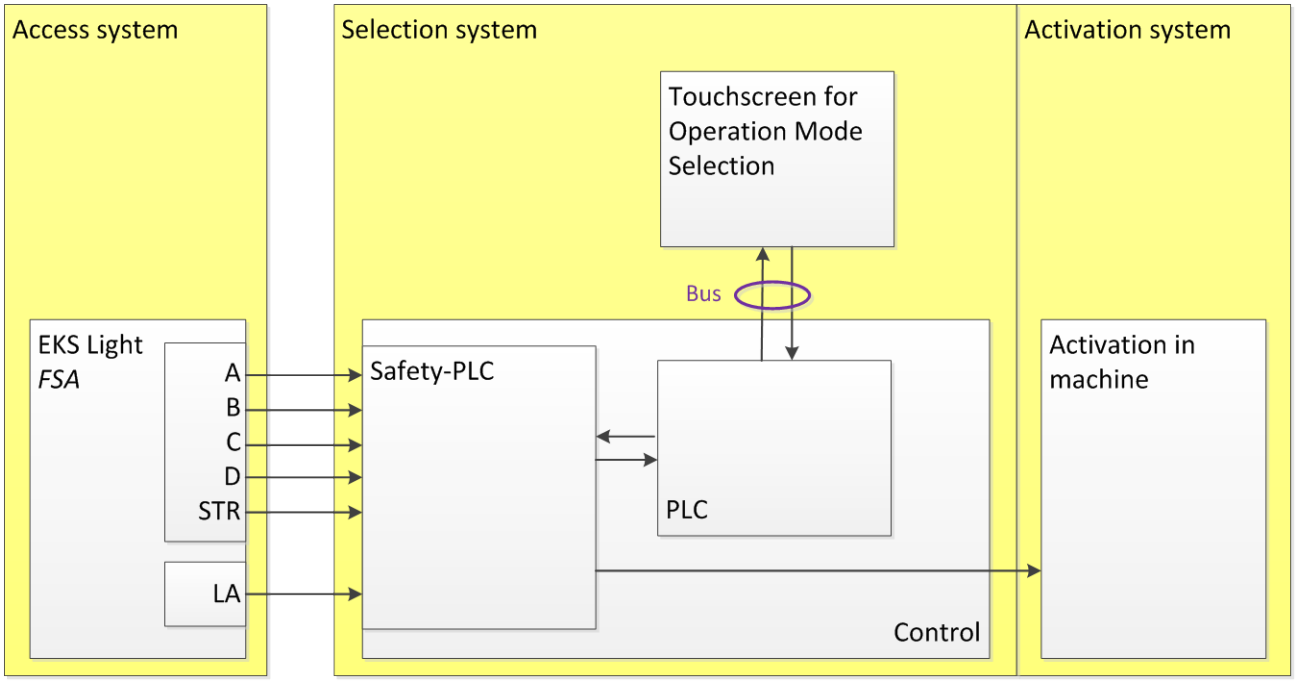


Figure 1

The switching outputs A to D as well as STR on the EKS Light FSA are connected to safe inputs on the F-PLC. The F-PLC internally forwards the data to the PLC via flag words (MW..). Any form of communication with the HMI is permissible, typically via a bus. Switching channel LA on the EKS FSA is connected to a further safe input on the F-PLC. FI1 is used in the example. The safe PLC is responsible for switching the operation mode. This could be internal signals to the PLC. First and foremost, however, the safety equipment for the selected operation mode is also switched on via outputs. It must be noted that this part of operation mode selection is also relevant to safety and therefore must fulfill the required Performance Level (PL_r) for the operation mode selection.

General notes about programming

The sequences in the 4 different devices are structured so that the F-PLC detects as many errors as possible automatically based on the data generated and forwarded by the various devices.

The sequences given below must be programmed in the devices PLC, HMI and F-PLC. During this process the programming principles required in EN ISO 13849-1:2008 section 4.6 are to be followed. All sequences relevant for safety are programmed in the F-PLC. The PLC is only used to forward data between the HMI and F-PLC.

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 undertaken such 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 9 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 initial status if the Electronic-Key is pulled out during program execution, for example. These checks prior to each step monitor that all elements of the control system operate in parallel and that the system switches back from a possible error once the portions of the software are executed correctly again.

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

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.

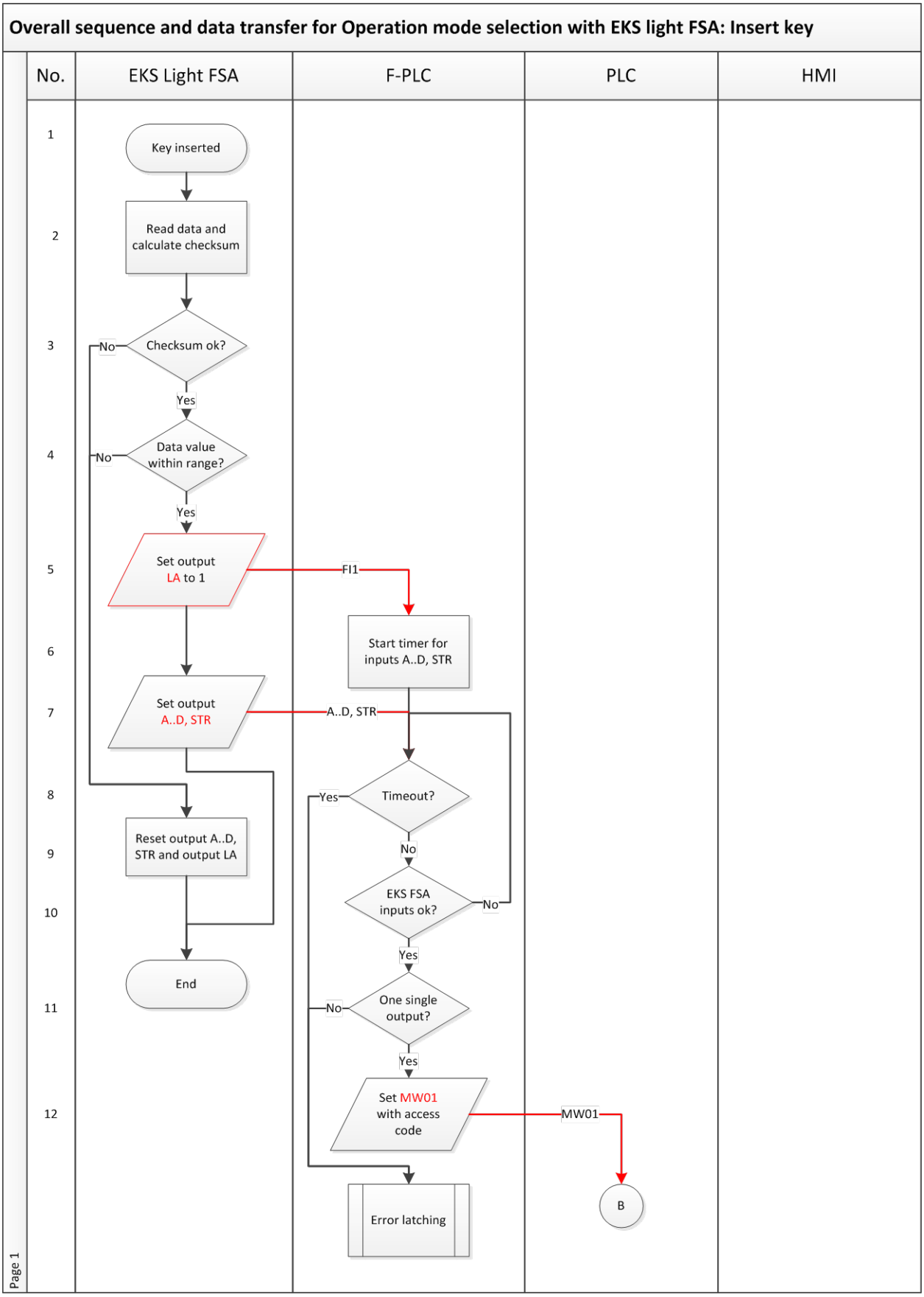


Figure 2.1

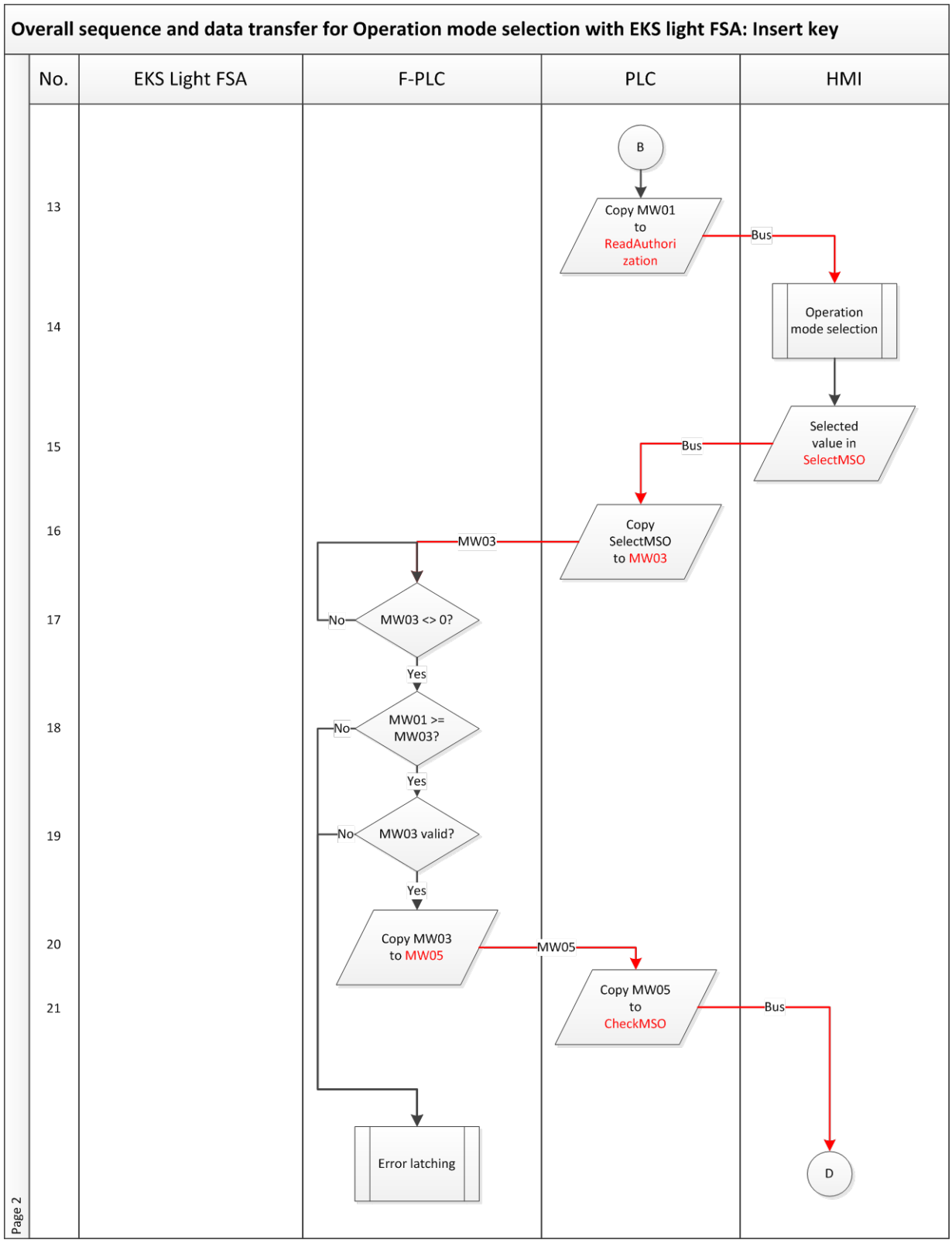


Figure 2.2

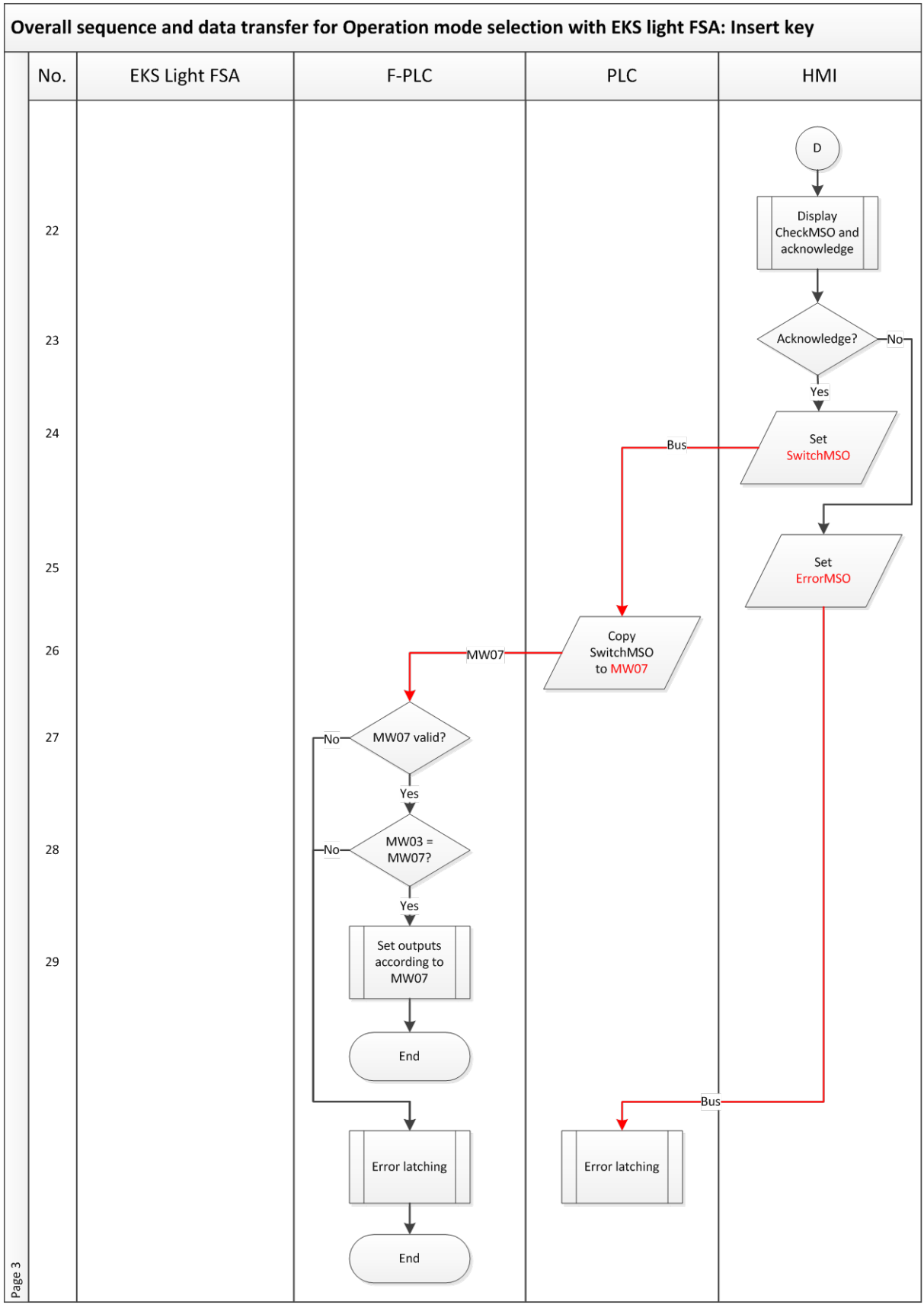


Figure 2.3

Step	System	Description
1	EKS light *FSA*	A user inserts an Electronic-Key.
2	EKS light *FSA*	Channels A and B on the EKS Light *FSA* read the data from the Electronic-Key and calculate the checksum for the content of the Electronic-Key.
3	EKS light *FSA*	It is checked whether the checksum for the Electronic-Key is correct. If the checksum is incorrect, the outputs A..D or STR and LA are reset.
4	EKS light *FSA*	In the EKS Light *FSA* it is checked whether valid data from the value range for MW01 and ReadAuthorization and the Electronic-Key content from Table 2 are present.
5	EKS light *FSA*	When an Electronic-Key is inserted, output LA is set to 1 if the Electronic-Key is a valid Electronic-Key.
6	F-PLC	A timeout (approx. 1 s) is started in the safe PLC by the end of which at least one of the outputs A..D or STR must also be set after setting the safe input FI1.
7	EKS light *FSA*	One of the outputs A..D or STR is set to suit the content of the Electronic-Key.
8	F-PLC	Check on whether the time has elapsed. In this way it is monitored whether the EKS is operating correctly and the Electronic-Key is valid.
9	EKS light *FSA*	The outputs A..D and STR as well as LA are set to 0. In this way it is signaled that there is an error.
10	F-PLC	To test all outputs, a pulse of short duration is first set on all outputs by the EKS light *FSA*. Then a single output is set that represents the maximum operation mode allowed for the Electronic-Key inserted. Figure 4 contains a sequence that describes this step in detail.
11	F-PLC	Only one of the outputs A..D or STR is allowed to be switched on (1 of N selection). If more than one input is set to 1, there is an error in the EKS.
12	F-PLC	Corresponding to the state of the inputs, the code corresponding to the EKS outputs A..D or STR for the maximum operation mode allowed is entered in flag word MW01. It must be borne in mind here that the definition of the value range for MW01 and the ReadAuthorization from Table 2 must be used.
13	PLC	The access code from the flag word MW01 is sent unchanged to the HMI via ReadAuthorization.
14	HMI	A screen in which the operation mode can be selected is generated or made accessible in the HMI. An operation mode is selected via a touchscreen or via softkeys. The highest operation mode that can be input must not exceed the access authorization on the EKS Electronic-Key corresponding to MW01 or ReadAuthorization.
15	HMI	The HMI sends the operation mode selected over the bus. It must be borne in mind here that the definition of the value range for MW03 and SelectMSO from Table 2 must be used.
16	PLC	The selected operation mode is copied from the input range of the bus connection to flag word MW03 to transfer it to the F-PLC.
17	F-PLC	It is checked whether new data have arrived from the PLC. This is identified by any value other than 0 appearing in flag word MW03.
18	F-PLC	The selected operation 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 must be used. Figure 5 contains a sequence that describes this step in detail.
19	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 must be used. Figure 6 contains a sequence that describes this step in detail.
20	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 6 contains a sequence that describes this step in detail.
21	PLC	The selected code from the flag word MW05 is sent unchanged to the HMI via CheckMSO.

22	HMI	The operation 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 operation 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 operation mode from step 13. The acknowledgment must not be at the same place on the touchscreen where the selected operation mode was confirmed.
23	HMI	The user must accept the data displayed by pressing a button.
24	HMI	Once the operation mode has been acknowledged, the value for the selected operation 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 must be used.
25	HMI	As negative acknowledgment, the HMI identifies that an error occurred. This information is sent via the bus.
26	PLC	The selected operation mode is copied from the input range of the bus connection to flag word MW07 to transfer it to the F-PLC.
27	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 Select-MSO from Table 2 must be used. Figure 7 contains a sequence that describes this step in detail.
28	F-PLC	A comparison is performed to determine whether the originally selected operation mode MW03 corresponds to the acknowledged operation mode MW07. Figure 7 contains a sequence that describes this step in detail.
29	F-PLC	If it corresponds, switchover to the new operation mode from MW07 takes place.

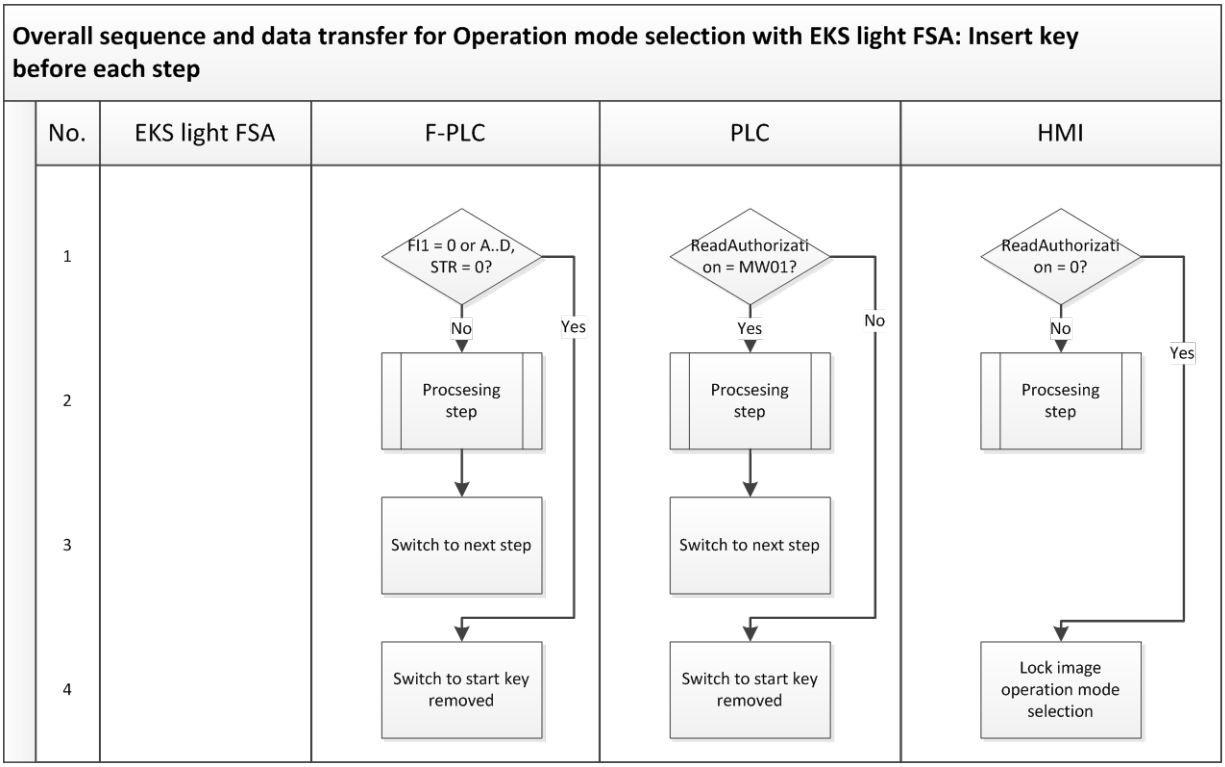


Figure 3

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

Step	System	Description
1	PLC	It is checked whether ReadAuthorization is still the same as MW01. It must be borne in mind here that the definition of MW01 and the ReadAuthorization from Table 2 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 enable for the “Operation mode input” screen is still present.
1	F-PLC	It is checked whether the EKS light *FSA* is still indicating that an Electronic-Key is inserted. For this purpose the output LA and also the outputs A .. D and STR are checked. If LA 0 is indicated or none of the outputs is 1, the Electronic-Key has been removed.
2	PLC HMI F-PLC	The step to be run from the flow chart in Figure 2 is executed.
3	PLC F-PLC	Switch in the status to the next step from the flow chart in Figure 2.
4	PLC	Switch to the start of the “Electronic-Key is removed” routine.
4	HMI	Access to the operation mode selection screen is inhibited.
4	F-PLC	Switch to the start of the “Electronic-Key is removed” routine.

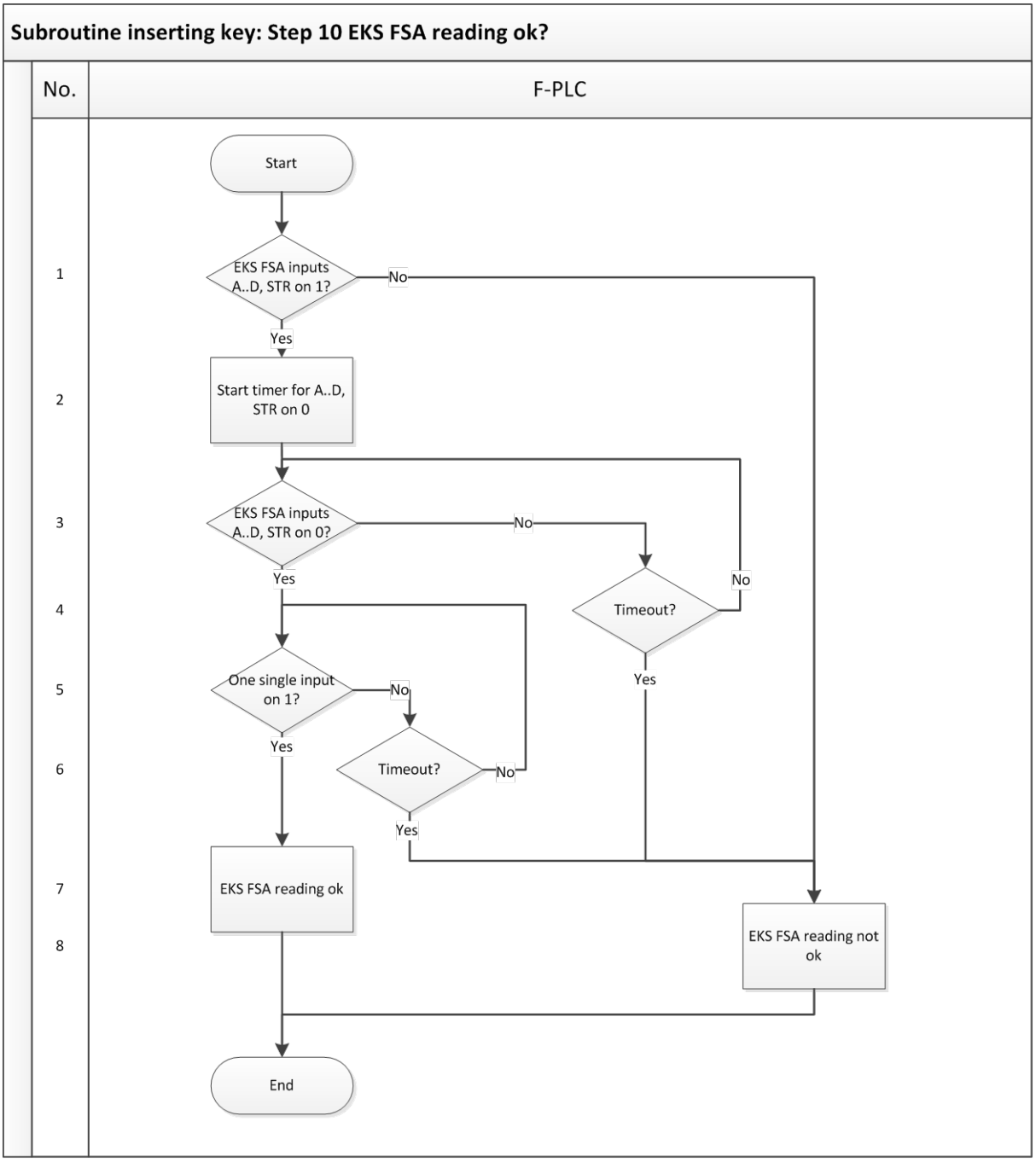

Subroutine inserting key: Step 10 EKS FSA reading ok?
No.
F-PLC
Start
1
EKS FSA inputs A..D, STR on 1?
No
Yes
2
Start timer for A..D, STR on 0
3
EKS FSA inputs A..D, STR on 0?
No
Yes
4
Timeout?
No
Yes
5
One single input on 1?
No
Yes
6
Timeout?
No
Yes
7
EKS FSA reading ok
8
EKS FSA reading not ok
End

Figure 4

Step	System	Description
1	F-PLC	It is checked whether all outputs on the EKS Light *FSA* are set to 1. This is used as a start signal. By setting all outputs to 1 and then back to 0, before the actual value is applied, tampering is prevented and all outputs on the EKS light *FSA* are checked for correct function by the F-PLC.
2	F-PLC	After all outputs on the EKS light *FSA* have been set to 1, these go to 0 again after 200 ms. The timer is set to a value of 1000 ms.
3	F-PLC	It is checked whether all outputs on the EKS Light *FSA* are set to 0 again. This state is also reached after 200 ms. This step is also monitored by the timeout.
4	F-PLC	It is checked whether the time has elapsed. If it has not elapsed, waiting continues. If the time has elapsed, it is reported that a valid value has not be read from the EKS light *FSA*.
5	F-PLC	After all outputs on the EKS light *FSA* have reached both the state 1 and also the state 0, only one output is set that represents the highest operation mode allowed for the Electronic-Key inserted.
6	F-PLC	It is checked whether the time has elapsed. If it has not elapsed, waiting continues. If the time has elapsed, it is reported that a valid value has not be read from the EKS light *FSA*.
7	F-PLC	It is reported that one output is set and the sequence was ok.
8	F-PLC	It is reported that a valid result has been signaled by the EKS light *FSA*.

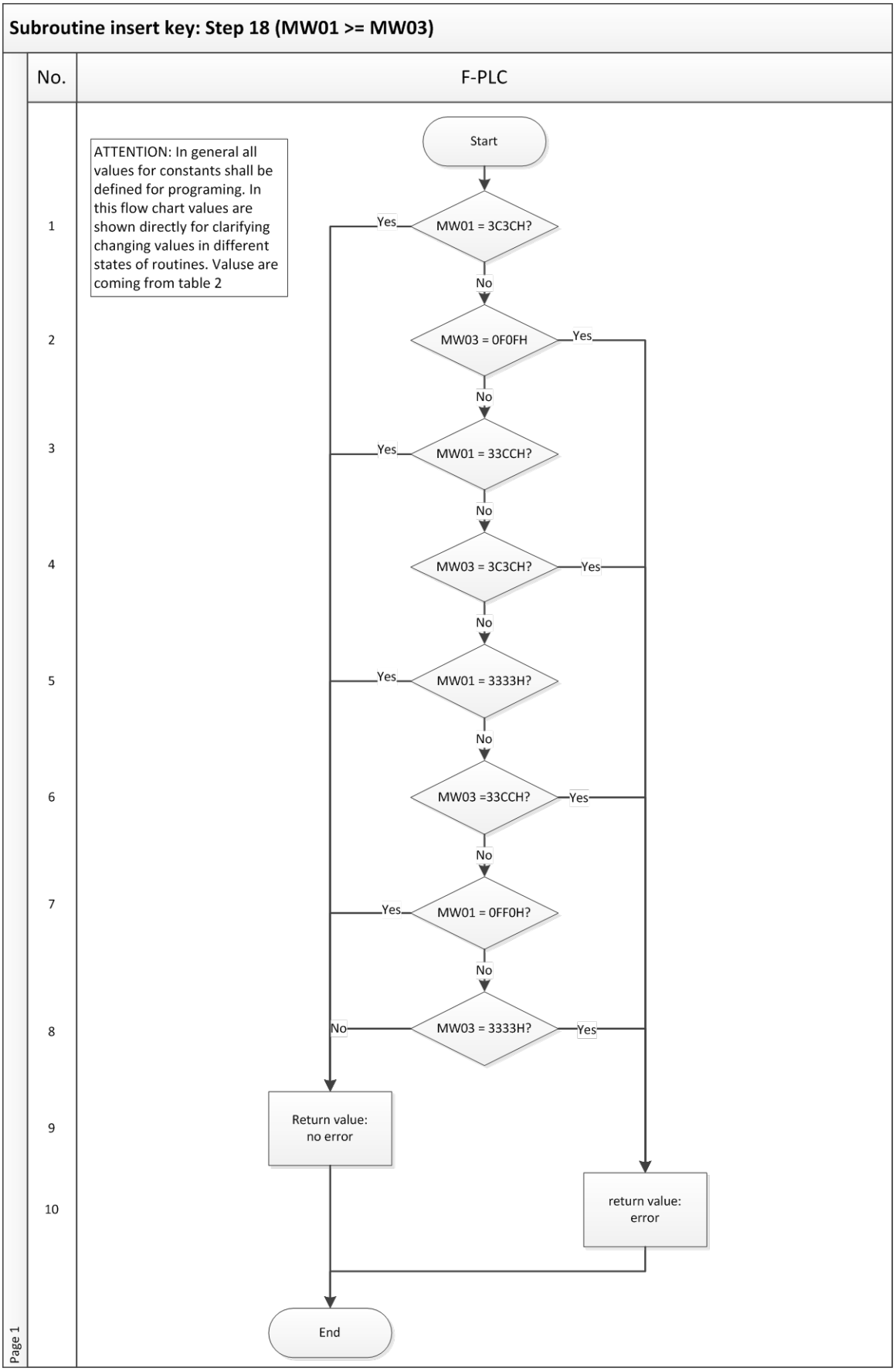

Subroutine insert key: Step 18 (MW01 >= MW03)
No.
F-PLC
ATTENTION: In general all values for constants shall be defined for programing. In this flow chart values are shown directly for clarifying changing values in different states of routines. Valuse are coming from table 2
Start
MW01 = 3C3CH?
Yes
No
MW03 = 0F0FH
Yes
No
MW01 = 33CCH?
Yes
No
MW03 = 3C3CH?
Yes
No
MW01 = 3333H?
Yes
No
MW03 =33CCH?
Yes
No
MW01 = 0FF0H?
Yes
No
MW03 = 3333H?
Yes
No
Return value: no error
return value: error
End
1
2
3
4
5
6
7
8
9
10
Page 1

Figure 5

Step	System	Description
1	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW01 (permissible operation mode). In MW01, this is indicated by the value 3C3CH. If YES, every selected operation 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 operation mode). In MW03, this is indicated by the value 0F0FH. If YES, an impermissible operation mode was selected, because there is no authorization for this operation mode in MW01.
3	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW01 (permissible operation mode). In MW01, this is indicated by the value 33CCH. If YES, every selected operation 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 operation mode). In MW03, this is indicated by the value 3C3CH. If YES, an impermissible operation mode was selected, because there is no authorization for this operation mode in MW01.
5	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW01 (permissible operation mode). In MW01, this is indicated by the value 3333H. If YES, every selected operation 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 operation mode). In MW03, this is indicated by the value 33CCH. If YES, an impermissible operation mode was selected, because there is no authorization for this operation mode in MW01.
7	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW01 (permissible operation mode). In MW01, this is indicated by the value 0FF0H. If YES, every selected operation 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 operation mode). In MW03, this is indicated by the value 3333H. If YES, an impermissible operation mode was selected, because there is no authorization for this operation mode in MW01.
9	F-PLC	It is reported that no error occurred.
10	F-PLC	It is reported that an error occurred.

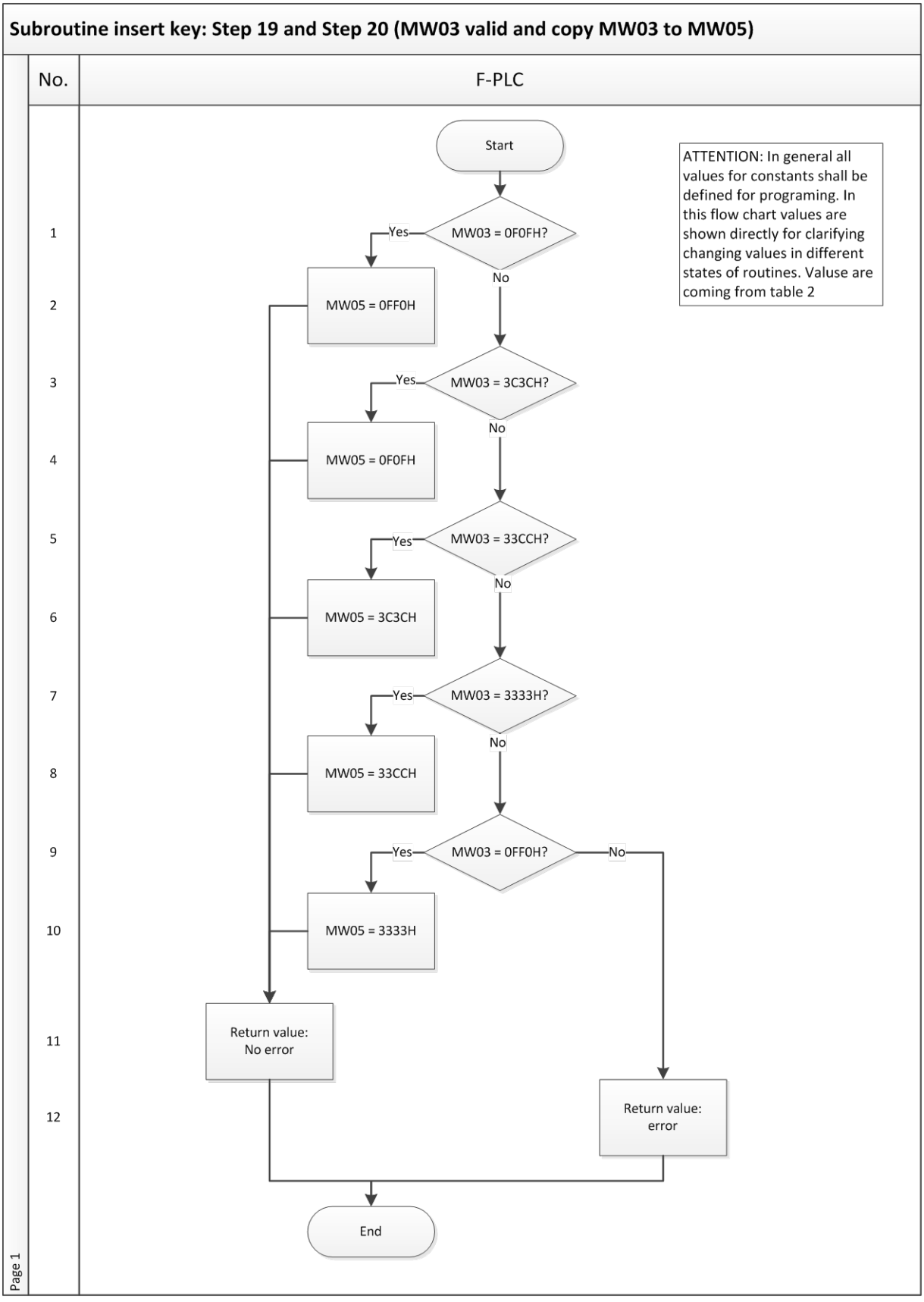


Figure 6

Step	System	Description

1	F-PLC	It is checked whether authorization level MSO 4 is stored in MW03 (selected operation 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 (operation 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 operation 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 (operation 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 operation 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 (operation 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 operation 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 (operation 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 operation 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 (operation 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.

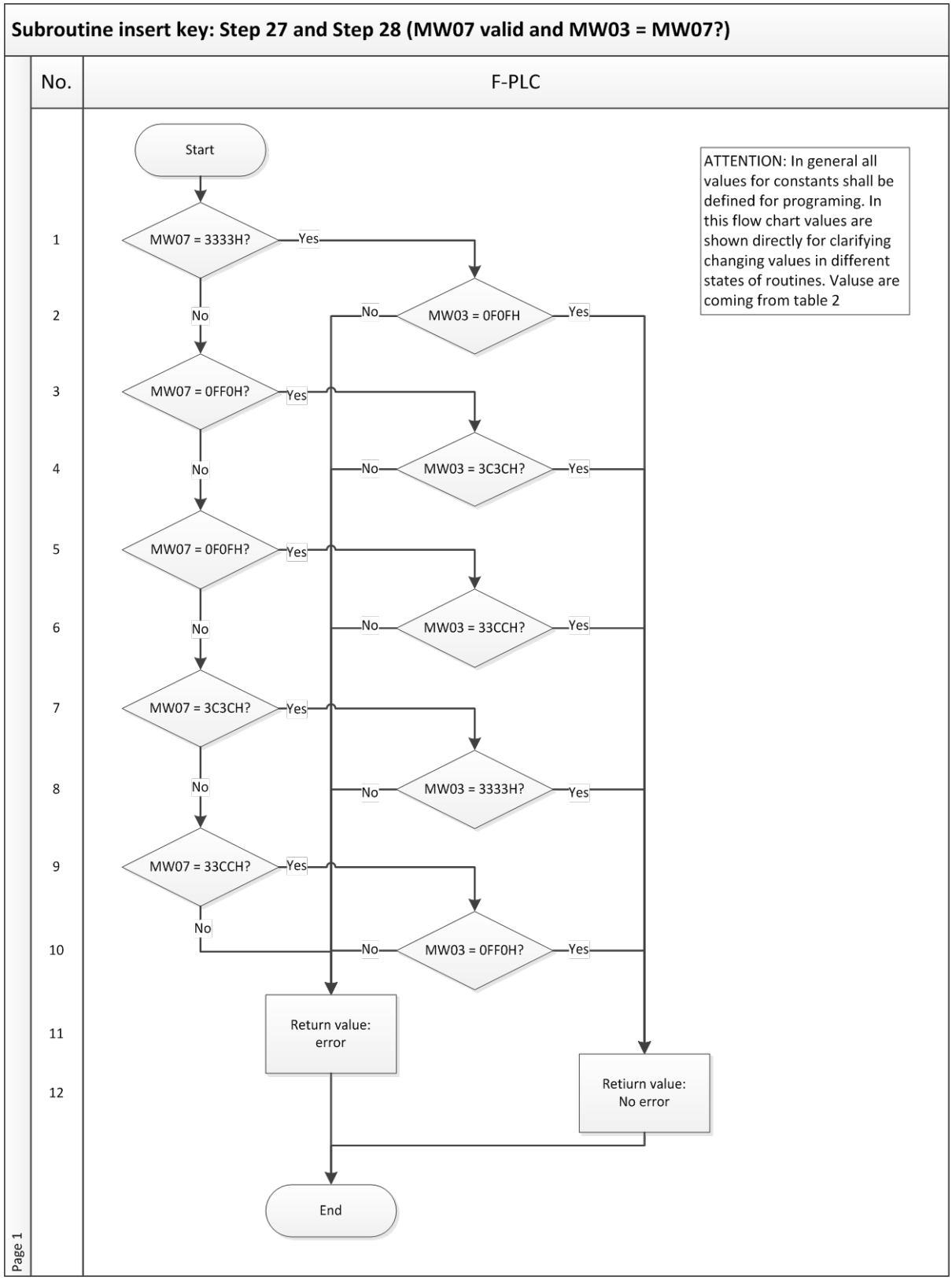

Subroutine insert key: Step 27 and Step 28 (MW07 valid and MW03 = MW07?)
No.
F-PLC
Start
ATTENTION: In general all values for constants shall be defined for programing. In this flow chart values are shown directly for clarifying changing values in different states of routines. Valuse are coming from table 2
1
MW07 = 3333H?
Yes
2
No
MW03 = 0F0FH
No
Yes
3
MW07 = 0FF0H?
Yes
4
No
MW03 = 3C3CH?
No
Yes
5
MW07 = 0F0FH?
Yes
6
No
MW03 = 33CCH?
No
Yes
7
MW07 = 3C3CH?
Yes
8
No
MW03 = 3333H?
No
Yes
9
MW07 = 33CCH?
Yes
10
No
MW03 = 0FF0H?
No
Yes
11
Return value:
error
12
Retiurn value:
No error
End
Page 1

Figure 7

Step	System	Description
1	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW07 (acknowledged operation mode). In MW07, this is indicated by the value 3333H. If YES, it can be checked whether this is also the previously selected operation mode.
2	F-PLC	It is checked whether the highest authorization level (MSO 4) is stored in MW03 (selected operation mode). In MW03, this is indicated by the value 0F0FH. If YES, switchover to this operation mode can take place.
3	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW07 (acknowledged operation mode). In MW07, this is indicated by the value 0FF0H. If YES, it can be checked whether this is also the previously selected operation mode.
4	F-PLC	It is checked whether the second-highest authorization level (MSO 3) is stored in MW03 (selected operation mode). In MW03, this is indicated by the value 3C3CH. If YES, switchover to this operation mode can take place.
5	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW07 (acknowledged operation mode). In MW07, this is indicated by the value 0FF0H. If YES, it can be checked whether this is also the previously selected operation mode.
6	F-PLC	It is checked whether the third-highest authorization level (MSO 2) is stored in MW03 (selected operation mode). In MW03, this is indicated by the value 33CCH. If YES, switchover to this operation mode can take place.
7	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW07 (acknowledged operation mode). In MW07, this is indicated by the value 3C3CH. If YES, it can be checked whether this is also the previously selected operation mode.
8	F-PLC	It is checked whether the next-to-last authorization level (MSO 1) is stored in MW03 (selected operation mode). In MW03, this is indicated by the value 3333H. If YES, switchover to this operation mode can take place.
9	F-PLC	It is checked whether the last authorization level (MSO 0) is stored in MW07 (acknowledged operation mode). In MW07, this is indicated by the value 33CCH. If YES, it can be checked whether this is also the previously selected operation mode.
10	F-PLC	It is checked whether the last authorization level (MSO 0) is stored in MW03 (selected operation mode). In MW03, this is indicated by the value 0FF0H. If YES, switchover to this operation 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 flow charts in Figures 8.1 and 8.2. Transfer variables are shown in red.

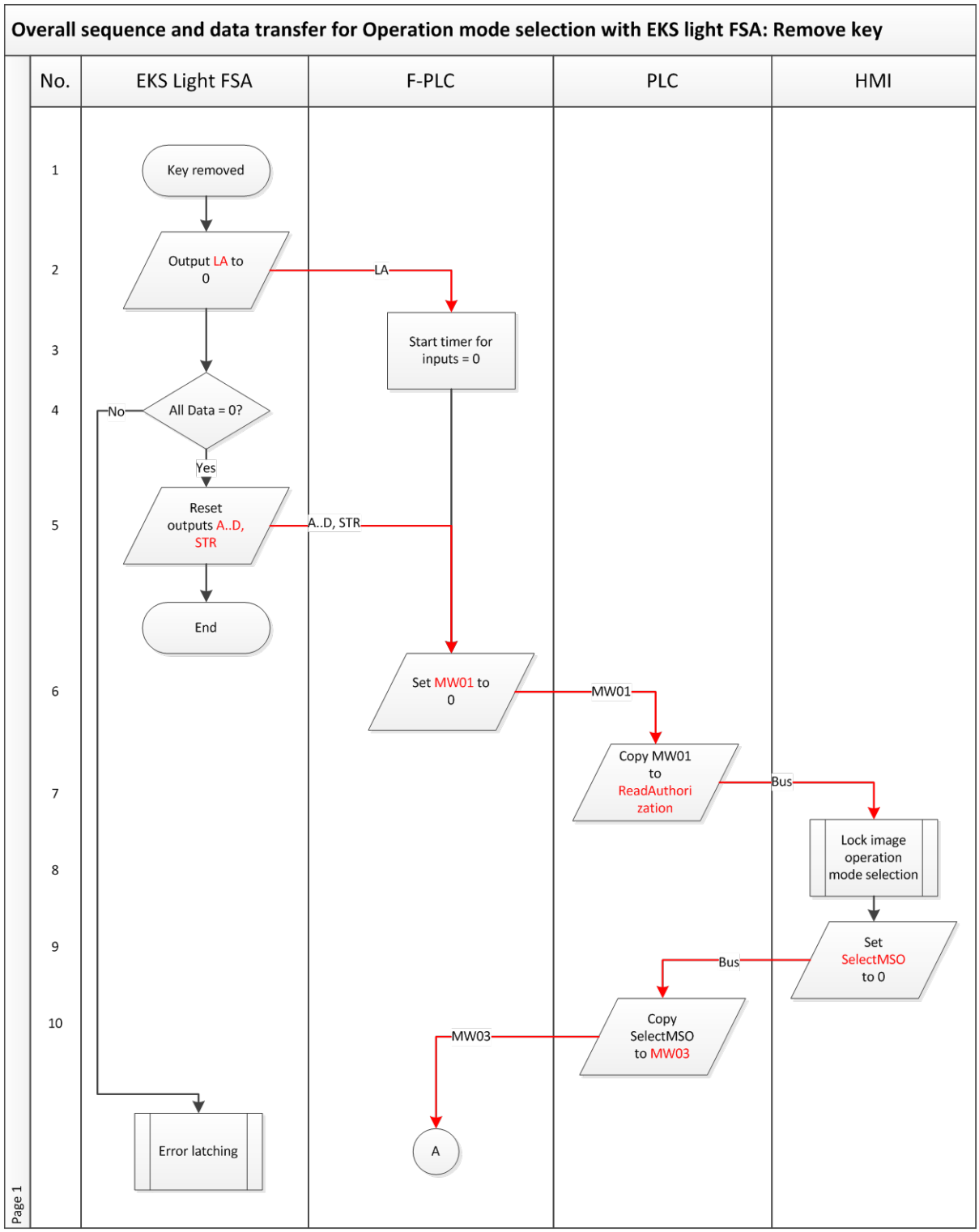


Figure 8.1

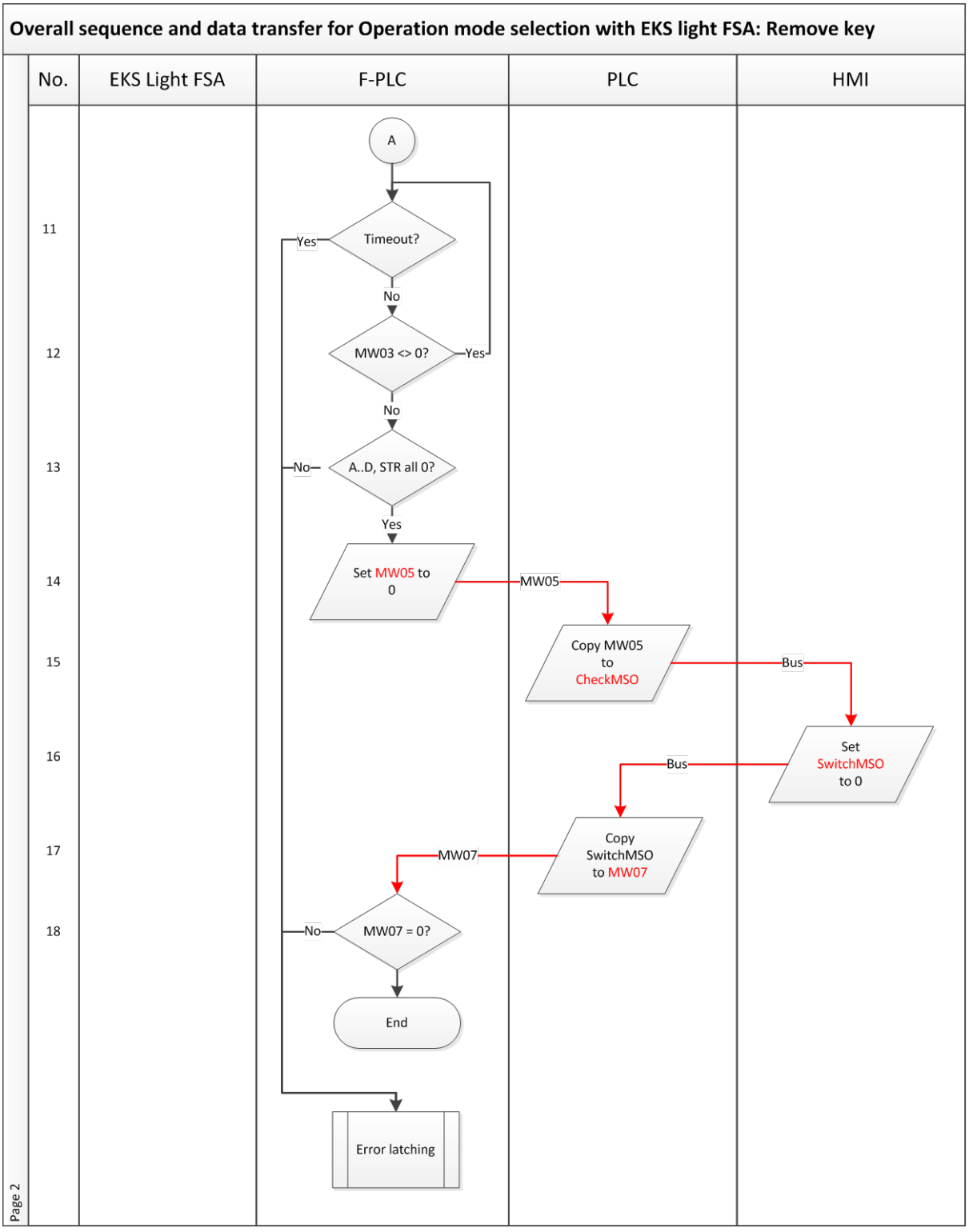

Overall sequence and data transfer for Operation mode selection with EKS light FSA: Remove key
No.
EKS Light FSA
F-PLC
PLC
HMI
11
12
13
14
15
16
17
18
A
Timeout?
Yes
No
MW03 <> 0?
Yes
No
A..D, STR all 0?
No
Yes
Set MW05 to 0
MW05
Copy MW05 to CheckMSO
Bus
Set SwitchMSO to 0
Bus
Copy SwitchMSO to MW07
MW07
MW07 = 0?
No
End
Error latching
Page 2

Figure 8.2

Step	System	Description
1	EKS light *FSA*	A user removes an Electronic-Key.
2	EKS light *FSA*	When an Electronic-Key is removed, output LA is set to 0.
3	F-PLC	A timeout is started in the safe PLC until the outputs A..D and STR as well as the data in the PLC and HMI also go to 0 after setting the safe input FI1.
4	EKS light *FSA*	In EKS channel B it is checked whether all internal data are 0, incl. registers for outputs. If not, an internal fault is detected and latched to fault.
5	EKS light *FSA*	The outputs A..D and STR are set to zero.
6	F-PLC	The F-PLC saves the value zero in the flag word MW01 so that the passage of the data through the HMI and PLC can be tested.
7	PLC	The PLC sends the content of ReadAuthorization to the HMI via the bus system.
8	HMI	Owing to the lack of access authorization, the HMI must inhibit the operation mode selection screen to prevent any more changes. The currently selected operation mode remains active and must continue to be displayed.
9	HMI	As feedback, the HMI returns the zero as the newly selected operation mode.
10	PLC	The PLC saves the value from SelectMSO in flag word MW03. It must be zero.
11	F-PLC	Max. the set time is waited.
12	F-PLC	The flag word MW03 must have been returned by the HMI as zero. If not, waiting continues.
13	F-PLC	It is checked all outputs have been set to zero by the EKS light *FSA*.
14	F-PLC	It is checked whether zeros are sent as data in flag word MW03 by the HMI and PLC. This checks the correct sequence through the PLC and the HMI.
15	PLC	The PLC sends the content of CheckMSO to the HMI via the bus system.
16	HMI	As feedback, the HMI returns the confirmed operation mode as zero.
17	PLC	The data from the HMI are copied over to flag word MW07 so that they are accessible for the F-PLC.
18	F-PLC	The F-PLC checks whether the zero was also returned in flag word MW07.

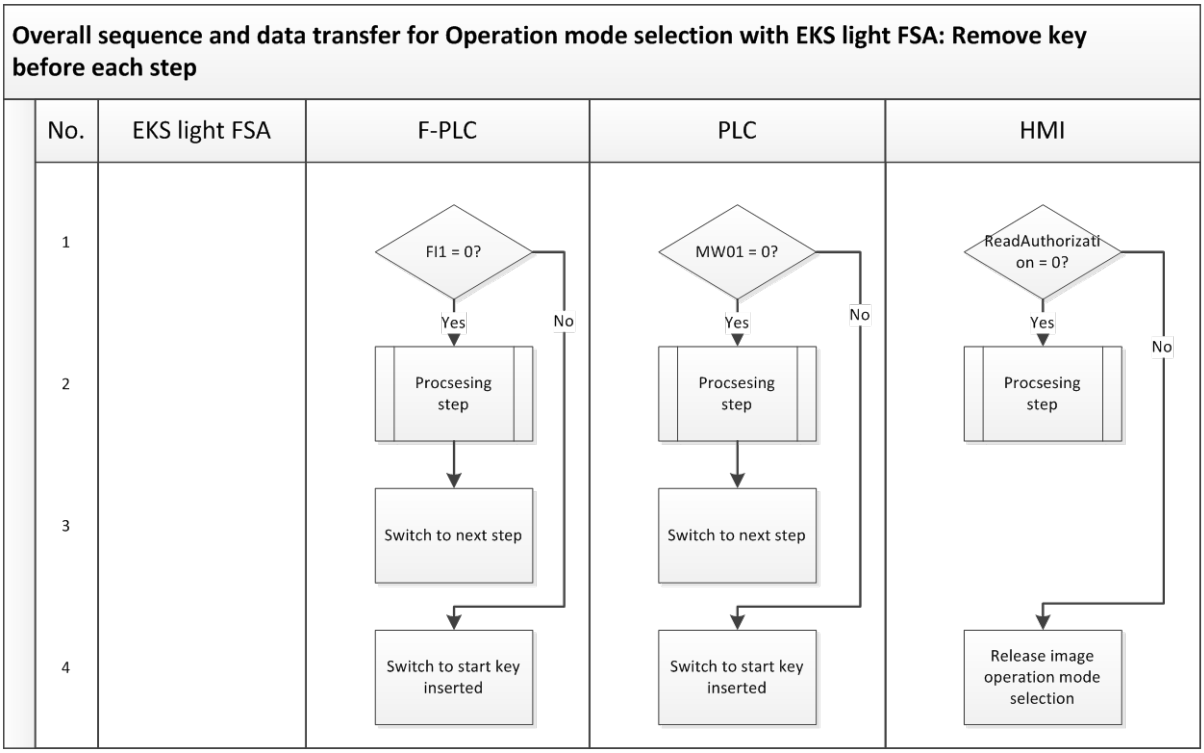


Figure 9

The synchronous sequence in the PLC, HMI and F-PLC systems can detect differences in the systems (channels). This represents error detection as defined in EN ISO 13849-1. For this reason, the sequence from Figure 9 must be programmed or called before every individual step in the flow chart from Figures 8.
These sequence steps must also be executed prior to the error routine. This ensures that system recovery is possible if a fault is not permanent (e.g. initiated by the user).

Step	System	Description
1	PLC	It is checked whether MW01 is still zero.
1	HMI	It is checked whether a PLC inhibit for the “Operation mode input” screen still exists.
1	F-PLC	It is checked whether the EKS light *FSA* is still indicating that no Electronic-Key is inserted.
2	PLC HMI F-PLC	The step to be run from the flow chart in Figure 2 is processed.
3	PLC F-PLC	Switch in the status to the next step from the flow chart in Figure 2.
4	PLC	Switch to the start of the “Electronic-Key is inserted” routine.
4	HMI	Access to the operation mode selection screen is enabled.
4	F-PLC	Switch to the start of the “Electronic-Key is inserted” routine.

Principle circuit diagram

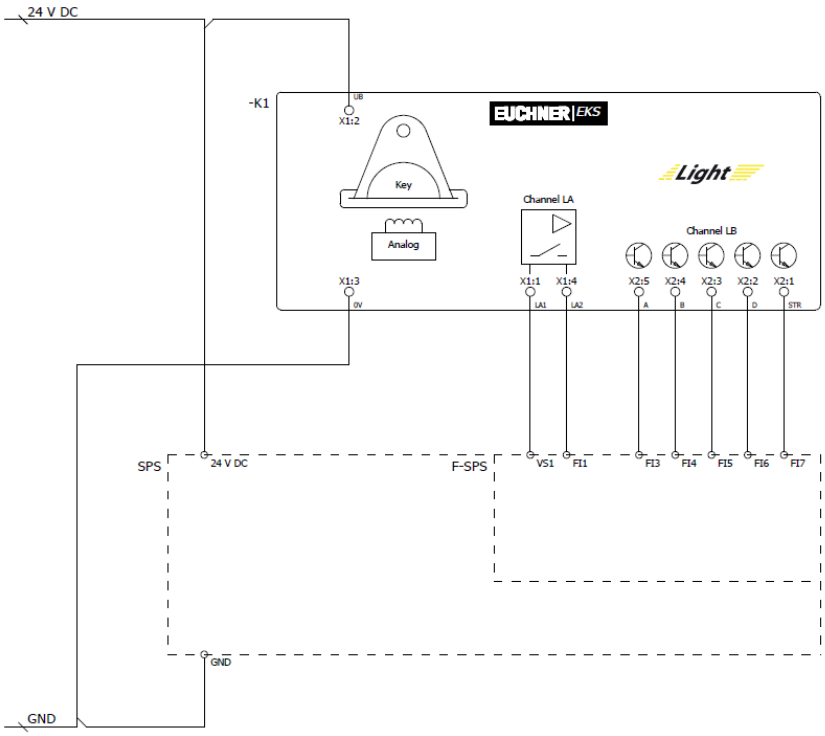


Figure 10

Safety description

EKS Light FSA

In the first channel on the EKS light *FSA*, the data and thus the access authorization are read from the Electronic-Key inserted. The result is signaled to the F-PLC via the outputs A..D.

In the second channel on the EKS light *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 F-PLC permits switchover of the operation mode only if this input is switched on and in this way can check whether switchover is permissible at all.

When the Electronic-Key is removed, the EKS light *FSA* outputs zeros on all outputs A..D. The authorization level is thereby also set to 0. This is transmitted to the F-PLC. The output for the second channel on the EKS light *FSA* is also reset. The F-PLC can then check whether the outputs A..D have actually adopted the zero state. In addition, the check to ensure the zero can be sent to all parts of the control system is started.
Data corruption is possible on the transmission links (bus systems) or in the memory of the various systems. According to GS-ET-26, the codes selected with a data word with 16 bits and a Hamming distance of 8 result in a residual error probability of:

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

This low residual error probability ensures that no incorrect operation mode can be selected through the EKS light *FSA*. This residual error probability is not included in the calculation to determine the PFH_d of the overall system. The EKS light *FSA* serves only as an access system for operation 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 operation mode selection takes place only when authorization is present ~~on the inputs~~ from the EKS light *FSA*.
Only those touchscreen buttons that can be selected according to the inserted Electronic-Key are enabled.
The selected operation mode is transmitted to the PLC and from there to the safe PLC. The safe PLC returns an acknowledgment with the selected operation mode, which must be displayed. This must be acknowledged by the user. The procedure corresponds to safe parameter entry according to 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 on all data in the F-PLC
- Control of data corruption due to the large Hamming distance
- Plausibility checks on sequences to detect errors in the hardware and software
- Change in the meaning of the data words in the various selection levels to prevent overwriting of the memory or incorrect storage of data

The operation 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 entry corresponding to the procedure specified by EN ISO 13849-1.

F-PLC

In the F-PLC, operation mode selection is realized as a 1 of N system (only one operation 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 on writing the software. Refer to the next section for more information on this aspect.
The F-PLC is used to detect errors in all devices and components involved. The procedure for selecting the operation mode must be implemented in the F-PLC.
The failure probability of the F-PLC is included as the actual operation mode switchover in the calculation of the PL.

Summary

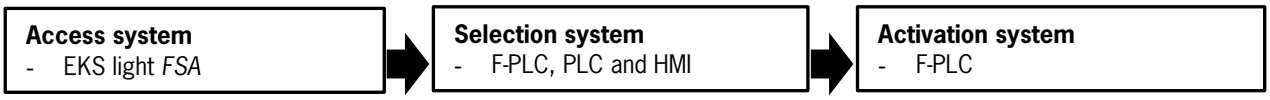
Software

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 write and assess the software in the F-PLC. The software must be validated according to section 9.5 of EN ISO 13849-2:2013.

The software in the PLC and HMI must be written according 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 operation mode selection comprises three blocks:



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

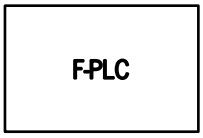
The access system is used to meet the requirements of the Machinery Directive for restricting access to certain groups of people. The selection system is the selection of the required operation mode by the user. In this example, user input is via the touchscreen. The activation system activates or deactivates the safety sensors and actuators according to the selected operation 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 operation modes can be found in DGUV Information FB HM-073.

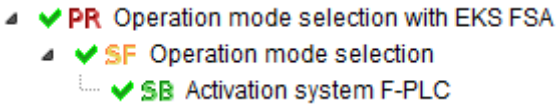
The access system does not have to be evaluated with a PL, but it is part of the safety system. Access restriction must be at least equivalent to that of a mechanical key. This security is achieved through the coding of the Electronic-Key and the dual-channel structure. Moreover, the EKS light *FSA* 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 light *FSA* is to trigger error checking in the F-PLC to monitor the EKS light *FSA*, the PLC and the HMI for correct function.

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 operation mode selection corresponding to this application, the operation mode selection system can be regarded as equivalent to a key-operated rotary switch in terms of safety. A PL cannot be assigned to the selection system in this example because operation mode selection is a parameter assignment based on software measures according to section 4.6.4 of EN ISO 13849-1:2008 (software-based parameterization).
The activation system must comply with the PL_r from the risk assessment of the machine for operation 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 written 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 downstream of the F-PLC (e.g. contactors and valves) are also involved in the operation 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 operation mode” to be designed with a Performance Level of up to PL e.

Safety block diagram:





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 has the obligation to assess the safety technology him/herself. 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.