S7 Program for the Detection of Changes in the User Program and Hardware Configuration

SIMATIC S7-300/400 CPU

FAQ · July 2011

Service & Support

Answers for industry.

SIEMENS

Question

How can you detect a change in the S7 user program?

Answer

Follow the instructions and notes listed in this document for a detailed answer to the above question.

Contents

1 Introduction

In many technical applications there may be a need to document changes in the program and in the configuration of the controller which is used.

The sample program available in this FAQ as a download registers a change in the checksums which are located in the system status list (SSL). This procedure is used to detect the manipulations below:

- Changes in the hardware configuration
- Changes in the existing program code
- Deletion or addition of program parts or blocks

A change which is detected in the checksums is documented in the form of a user-definable entry in the diagnostic buffer of the CPU.

2 The S7 Program

2.1 Structure of the S7 Program

The S7 program contained in this S7 possesses the following blocks.

Figure 2-1: Program structure

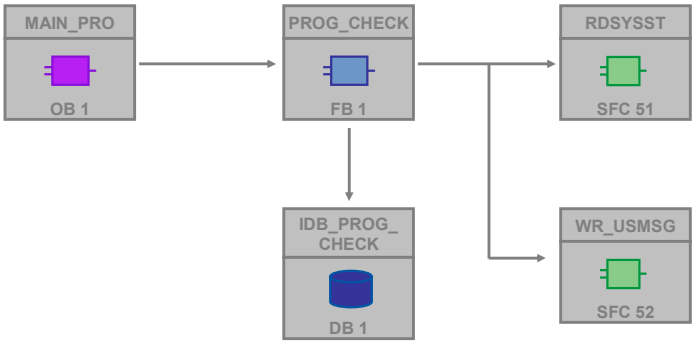


Table 2-1: Function blocks of the S7 program

Block	Function
FB 1 "PROG_CHECK"	Comparison between checksums and generation of the diagnostic message

Table 2-2: Data blocks of the S7 program

Block	Function
DB 1 "IDB_PROG_CHECK"	Instance DB of the FB 1

Table 2-3: System functions of the S7 program

Block	Function
SFC 51 "RDSYSST"	Reading out the system status list
SFC 52 "WR_USMSG"	Generation of diagnostic messages

2.2 The "PROG_CHECK" Function Block

The "PROG_CHECK" function block (FB 1) determines the checksum from the appropriate system status list with the aid of the "RDSYSST" system function (SFC 51).
When changes are made to the checksums, an entry is created in the diagnostic buffer of the CPU by FB 1 with the aid of the "WR_USMSG" system function (SFC 52).

The "PROG_CHECK" function block is called in the organization block OB1 and possesses the following interface.

Figure 2-2: "PROG_CHECK" FB call

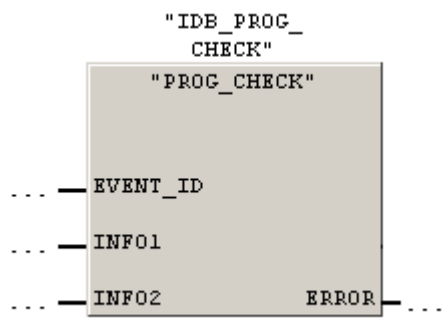


Table 2-4: "PROG_CHECK" FB parameters

Name	Type	Data type	Description
EVENT_ID	INPUT	WORD	Event ID for the diagnostic message
INFO1	INPUT	WORD	Additional information 1 for the diagnostic event
INFO2	INPUT	DWORD	Additional information 2 for the diagnostic event
ERROR	OUTPUT	BOOL	Error message

Input parameters

The input parameters "EVENT_ID", "INFO1" and "INFO2" serve to specify the diagnostic buffer entries (also refer to section 3.2).

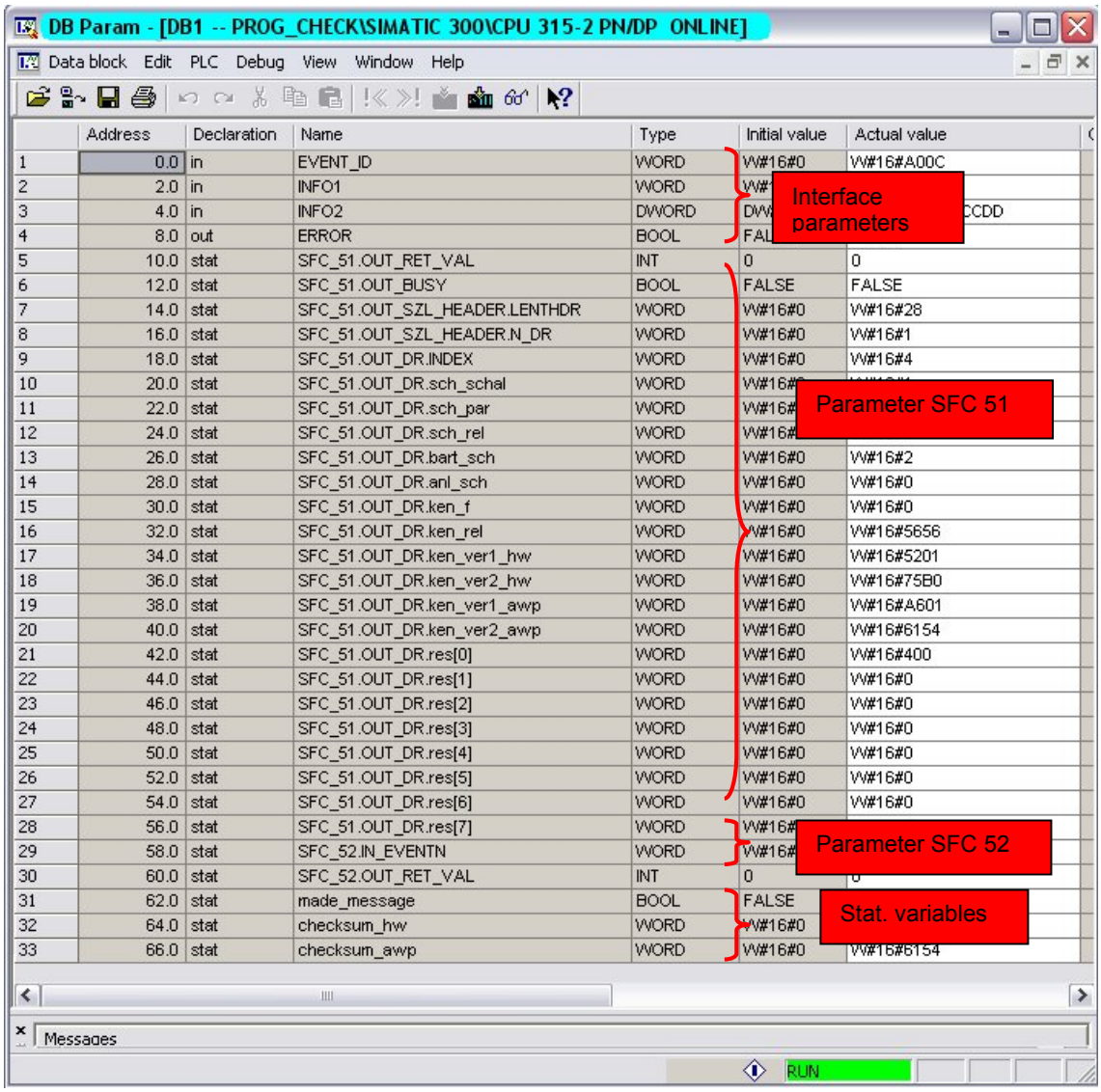
Error message

Error information is displayed via the output variable "ERROR". This leads to a high signal if one of the system functions used reports an error.

2.3 The "IDB_PROG_CHECK" Instance Data Block

The "IDB_PROG_CHECK" instance data block (DB1) contains all the information that is required to operate the "PROG_CHECK" function block. DB1 also acts as a data store for the WRDSYSST" and "WR_USMSG" system functions.

Figure 2-3: Structure of the "IDB_PROG_CHECK" instance data block



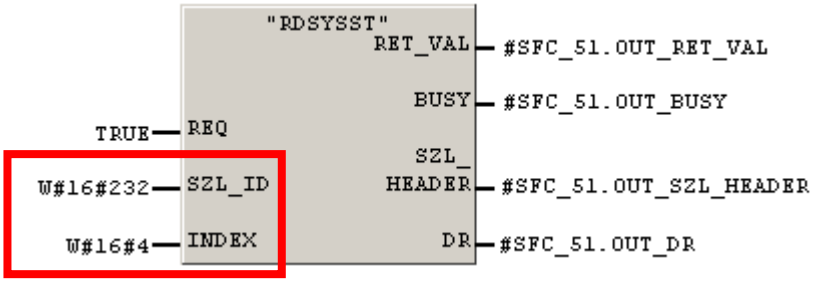
	Address	Declaration	Name	Type	Initial value	Actual value
1	0.0	in	EVENT_ID	WORD	W#16#0	W#16#A00C
2	2.0	in	INFO1	WORD	W#	
3	4.0	in	INFO2	DWORD	DW	CDD
4	8.0	out	ERROR	BOOL	FAL	
5	10.0	stat	SFC_51.OUT_RET_VAL	INT	0	0
6	12.0	stat	SFC_51.OUT_BUSY	BOOL	FALSE	FALSE
7	14.0	stat	SFC_51.OUT_SZL_HEADER.LENTHDR	WORD	W#16#0	W#16#28
8	16.0	stat	SFC_51.OUT_SZL_HEADER.N_DR	WORD	W#16#0	W#16#1
9	18.0	stat	SFC_51.OUT_DR.INDEX	WORD	W#16#0	W#16#4
10	20.0	stat	SFC_51.OUT_DR.sch_schal	WORD	W#16#	
11	22.0	stat	SFC_51.OUT_DR.sch_par	WORD	W#16#	
12	24.0	stat	SFC_51.OUT_DR.sch_rel	WORD	W#16#	
13	26.0	stat	SFC_51.OUT_DR.bart_sch	WORD	W#16#0	W#16#2
14	28.0	stat	SFC_51.OUT_DR.anl_sch	WORD	W#16#0	W#16#0
15	30.0	stat	SFC_51.OUT_DR.ken_f	WORD	W#16#0	W#16#0
16	32.0	stat	SFC_51.OUT_DR.ken_rel	WORD	W#16#0	W#16#5656
17	34.0	stat	SFC_51.OUT_DR.ken_ver1_hw	WORD	W#16#0	W#16#5201
18	36.0	stat	SFC_51.OUT_DR.ken_ver2_hw	WORD	W#16#0	W#16#75B0
19	38.0	stat	SFC_51.OUT_DR.ken_ver1_awp	WORD	W#16#0	W#16#A601
20	40.0	stat	SFC_51.OUT_DR.ken_ver2_awp	WORD	W#16#0	W#16#6154
21	42.0	stat	SFC_51.OUT_DR.res[0]	WORD	W#16#0	W#16#400
22	44.0	stat	SFC_51.OUT_DR.res[1]	WORD	W#16#0	W#16#0
23	46.0	stat	SFC_51.OUT_DR.res[2]	WORD	W#16#0	W#16#0
24	48.0	stat	SFC_51.OUT_DR.res[3]	WORD	W#16#0	W#16#0
25	50.0	stat	SFC_51.OUT_DR.res[4]	WORD	W#16#0	W#16#0
26	52.0	stat	SFC_51.OUT_DR.res[5]	WORD	W#16#0	W#16#0
27	54.0	stat	SFC_51.OUT_DR.res[6]	WORD	W#16#0	W#16#0
28	56.0	stat	SFC_51.OUT_DR.res[7]	WORD	W#16#	
29	58.0	stat	SFC_52.IN_EVENTN	WORD	W#16#	
30	60.0	stat	SFC_52.OUT_RET_VAL	INT	0	0
31	62.0	stat	made_message	BOOL	FALSE	
32	64.0	stat	checksum_hw	WORD	W#16#0	
33	66.0	stat	checksum_awp	WORD	W#16#0	W#16#6154

2.4 The System Functions Used

2.4.1 The SFC 51 "RDSYSST" System Function

The SFC 51 system function enables a parts list or an excerpt of a parts list to be read out from the system status list (SSL).

Figure 2-4: SFC 51 "RDSYSST" call



The parts-list excerpt with the SSL ID W#16#232 and the index W#16#4 contains the following information:

- CPU protection level
- Position of the operating switch for the CPU
- Checksum of the hardware configuration
- Checksum of the user program

This parts excerpt from the system status list is shown with the following parameters in the "IDB_PROG_CHECK" instance data block.

Table 2-5: Structure of the parts excerpt

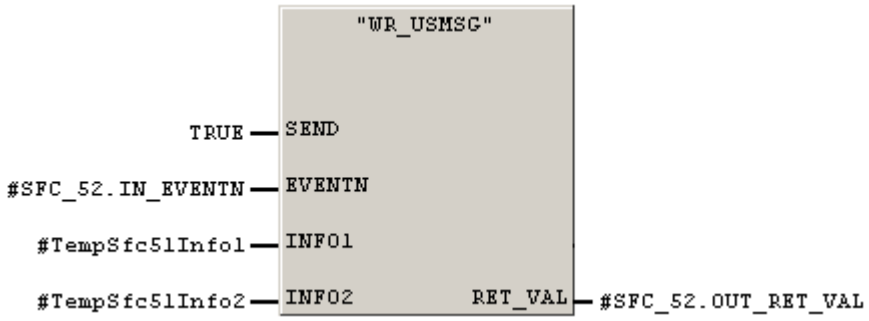
Name	Meaning
SFC_51.OUT_DR.INDEX	Index information from the parts excerpt
SFC_51.OUT_DR.sch_schal	Protection level set by the operating mode switch
SFC_51.OUT_DR.sch_par	Parameterized protection level
SFC_51.OUT_DR.sch_rel	Valid CPU protection level
SFC_51.OUT_DR.bart_sch	Position of the operating mode switch
SFC_51.OUT_DR.anl_sch	Position of the startup mode switch
SFC_51.OUT_DR.ken_f	Reserved
SFC_51.OUT_DR.ken_rel	Identifier for the validity of the following four checksums
SFC_51.OUT_DR.ken_ver1_hw	Checksum 1 of the hardware configuration
SFC_51.OUT_DR.ken_ver2_hw	Checksum 2 of the hardware configuration
SFC_51.OUT_DR.ken_ver1_awp	Checksum 1 of the user program
SFC_51.OUT_DR.ken_ver2_awp	Checksum 2 of the user program

Note Further information about the SFC 51 system function can be found in the SIMATIC S7 Online Help.

2.4.2 The SFC 52 "WR_USMSG" System Function

The SFC 52 system function enables entries to be written to the diagnostic buffer of the CPU.

Figure 2-5: SFC 52 "WR_USMSG" call



The input variables "EVENTN", "INFO1" and "INFO2" are supplied from the input variables of FB1.

Note A precise description and a sample program for the SFC 52 system function can be found in the download "Writing user-specific information to the diagnostic buffer of a CPU" (Entry ID 15166942).

3 How the S7 Program Works

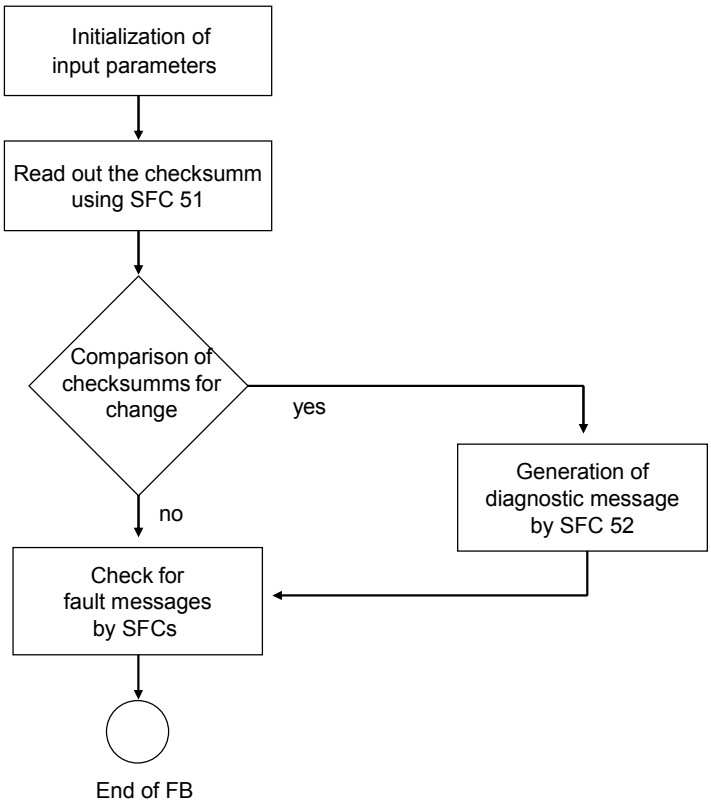
The "PROG_CHECK" function block (FB1) checks the following checksums:

- Checksum 2 of the hardware configuration:
  Exclusive OR operation via the checksums of all the system data blocks
- Checksum 2 of the user program:
  Exclusive OR operation via the checksums of the following blocks: OBs, DBs, FBs and FCs

3.1 Sequence Structure

The checksums are verified every time FB1 is called. Here, the current checksums are read out with the aid of the SFC 51 system function and are compared with the checksums which applied at the time of the previous FB1 call.

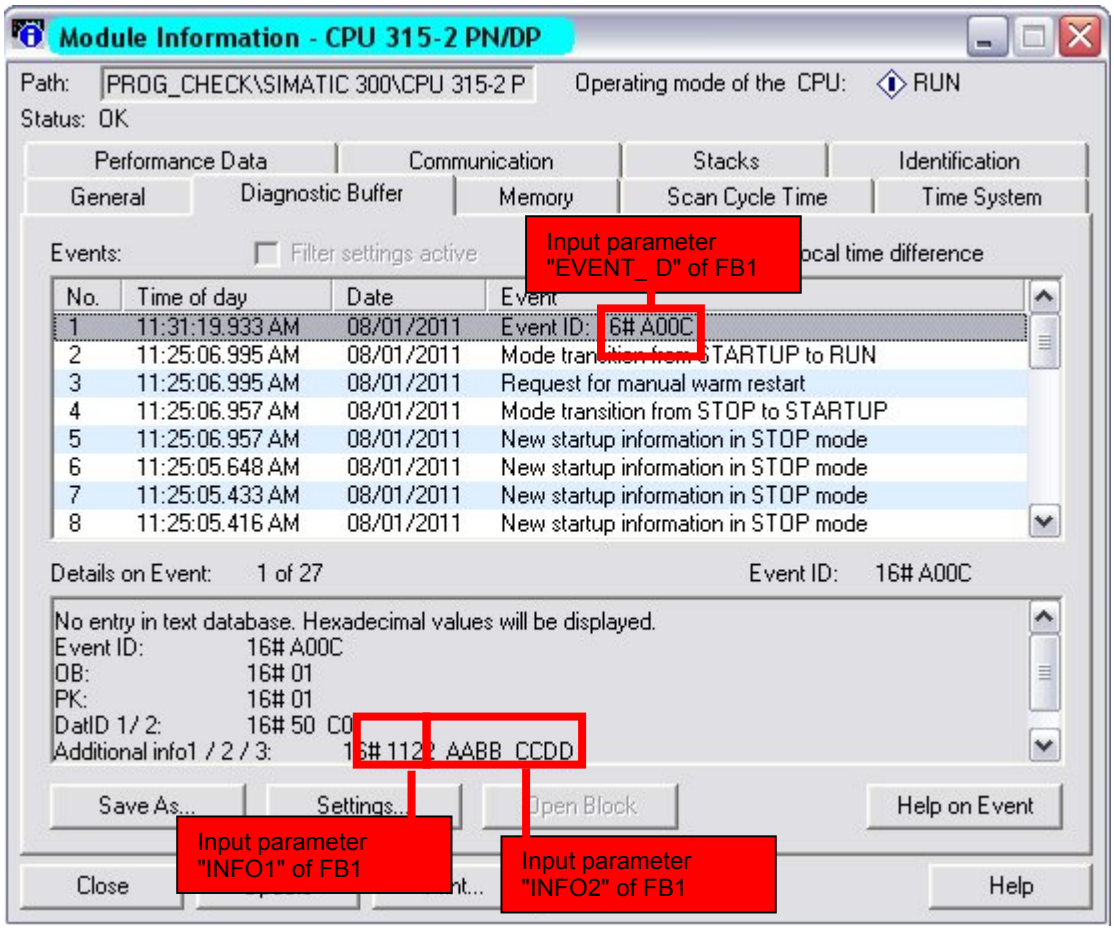
Figure 3-1: Sequence structure of the FB1 function block



3.2 Diagnostic Buffer Entry

If a change is detected when the checksums are verified, an entry is made in the diagnostic buffer of the CPU. This entry is implemented with a call for the SFC 52 system function.

Figure 3-2: Diagnostic buffer of the CPU



The event ID and the additional information relating to the diagnostic buffer entry can be defined with the aid of the input parameters "EVENT_ID", "INFO1" and "INFO2" of the FB1 function block.

4 Bibliography

This list is by no means complete and is only a selection of relevant literature.

Table 4-1: Bibliography

	Subject area	Title
/1/	STEP 7	Automation with STEP7 in STL and SCL Hans Berger Publicis MCD Verlag ISBN 3-89578-113-4

5 History

Table 5-1: History

Version	Date	Change
V1.0	07/2011	First edition
V1.0	03/2015	Correction of Fig. 3-1