TYPE EXAMINATION CERTIFICATE

46 24 03

PLUS+1 Development tools, version 9.0.X

Issued to

Danfoss Power Solutions AB,

Teknikgatan 1, SE-34334 ÄLMHULT, Sweden

Product name and description

The PLUS+1 development tools, version 9.0.X are support tools used for code generation, where high level graphical symbols are transferred to source code and in addition supports the assembling, linking and downloading of the source code to the hardware and reading/writing of information from/to the hardware. The PLUS+1 Development tools, version 9.0.X, consists of two main parts, namely:

- GUIDE tool, that handles the translation of graphical symbols to executable code
- Service Tool, that handles the download of executable code to the hardware and reading/writing of information from/to the hardware

Certification

The product described above fulfils the requirements placed on support tools for use in the development of application software according to the standard IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 and 3 within the following limitations:

- IEC 61508 tool requirements for GUIDE version 9.0 are fulfilled for graphic code, GUIDE C-code, Structured Text, Function Block Diagram, Ladder Logic Diagram code but not for externally developed C-code
- IEC 61508 tool requirements for Service Tool version 9.0 are fulfilled as long as it is not used as a software on-line support tool as defined by IEC 61508

The certification is based on a functional safety assessment according to IEC 61508:2010 described in SP report 7P02281:A supplemented with a separate evaluation of the PLUS+1 Development tools described in SP report 7P02281:B and the user documentation in the currently valid revision.

Certificate No. 462403 | issue 3 | 2017-08-24

RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
Phone: +46 10-516 50 00
certifiering@ri.se| www.ri.se

This document may not be reproduced other than in full, except with the prior written approval by RISE Certification.

Marking

Each sample that conforms in all respects with the original item certified may display the text "Type-examined by SP". In addition, manuals and marking shall also show the number of the standard, the reached SIL (Safety Integrity Level) of the item, the number of this certificate and the serial number or equivalent of the item.

Validity

This certificate is valid until not later than 27th June 2021.

Miscellaneous

Other terms and conditions are set out in RISE certification rules for type-examination, SPCR 123.

Lennart Månsson

Lennart Aronsson

This document may not be reproduced other than in full, except with the prior written approval by RISE Certification.

REPORT

Contact person RISE
Lars Strandén
Electronics
+46 10 516 55 52
lars.stranden@ri.se

Date	Reference	Page
2017-06-30	7P02281:C	1 (8)

Danfoss Power Solutions AB
Teknikgatan
S-343 34 ÄLMHULT
SWEDEN

PLUS+1 9.0 Safety Evaluation Overview

Test object

The test object is PLUS+1 tools GUIDE version 9.0 and Service Tool version 9.0 developed by Danfoss Power Solutions AB.

RISE Research Institutes of Sweden AB
Electronics - Dependable Systems

Performed by

Signed by: Lars Strandén
Reason: I am the author of this document
Date & Time: 2017-06-20 07:56:57 +02:00

Lars Strandén

Examined by

Signed by: Johan Hedberg
Reason: I have reviewed this document
Date & Time: 2017-06-28 13:43:54 +02:00

Johan Hedberg

This document may not be reproduced other than in full, except with the prior written approval of RISE.

Summary

This document is public and focusses on the Danfoss Power Solutions AB PLUS+1 tools from a safety perspective according to IEC 61508:2010. This document is an extract of "RISE report PLUS+1 9.0 Evaluation, 7P02281:B, 2017-06-30" and is intended for users and as initial information when considering Danfoss Power Solutions AB PLUS+1 tools.

The PLUS+1 Development tools are two, namely:

- GUIDE tool, that handles the translation of graphic symbols to executable code.
- Service Tool, that handles the download of the executable code to hardware.

These are certified according to IEC 61508:2010 under certain conditions.

Commission

This document is public and gives an overview of the Danfoss Power Solutions AB PLUS+1 tools from a safety perspective according to IEC 61508:2010. The document is assumed to match PLUS+1 version 9.0.X (where X is an integer ≥ 1) however there could be coming versions that may have effects on this document. This has to be checked by Danfoss Power Solutions AB.

The purpose is to give an overview of the possible quality of a product developed using the PLUS+1 environment. In this document a product is a safety function or a part of a safety function according to IEC 61508:2010.

Client

Danfoss Power Solutions AB
Teknikgatan 1
S-343 34 ÄLMHULT

Contact person: Johan Karlsson

Test object

Introduction

The test object is the pair of tools GUIDE and Service Tool both of version 9.0 which are defined by the referenced documents as given below.

The test object was delivered to RISE Electronics 2017-01-13 and 2017-05-09.

Terminology

Term	Description
CCP	Compiled Code Package used for making it possible to merge external C-code, “Function Block Diagram”, “Ladder Logic Diagram”, “Structured Text” code with graphic code.
Danfoss	Danfoss Power Solutions AB. Danfoss is here considered as a development environment provider not as a safety function provider.
Danfoss graphic language	The Danfoss language including graphic symbols and connections between them.
FBD	“Function Block Diagram” programming language defined in IEC61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
Function Block	Application independent function created using graphic symbols. License may be needed.
GUIDE C-code	Programming language C supported by GUIDE
HWD file	HardWare Description file
IEC 61131 language	One of “Function Block Diagram”, “Ladder Logic Diagram”, “Structured Text” as defined in IEC 61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
IEC 61508	IEC 61508:2010 part 1-7
LD	“Ladder Logic Diagram” programming language defined in IEC61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
LHX file	Downloadable protected file
NV memory	Non Volatile memory
P1D file	Diagnostic file to be used with the Service Tool to connect to the system
POU	Program Organization Unit, used for IEC 61131 languages defined in IEC 61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
SIL application	An application according to IEC 61508 SIL i.e. a safety critical application (safety function or part of it).
ST	“Structured Text” programming language defined in IEC61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages

Performance and result

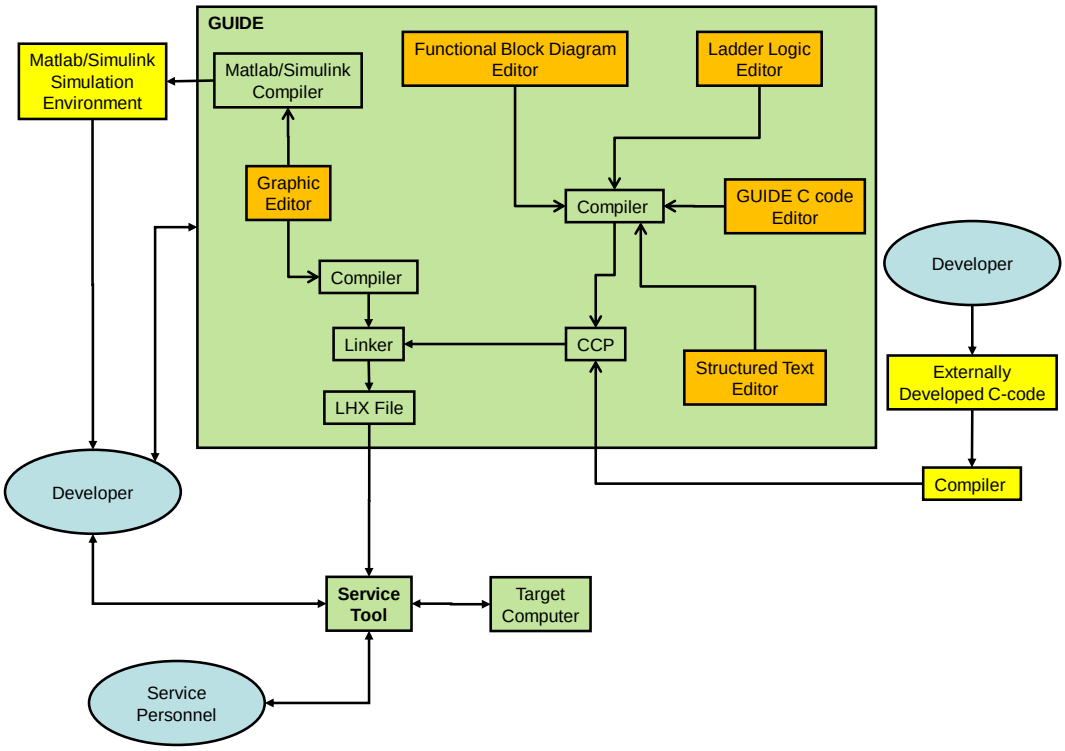
General

Evaluation was carried out by Lars Strandén, RISE Electronics, during the period from May 2017 to June 2017.

Results apply to the test object only.

PLUS+1 Overview

The PLUS+1 development environment is shown in the figure below.



GUIDE supports the Danfoss graphic language and GUIDE C-code, FBD, LD and ST. Each can be edited, connected and compiled in the GUIDE environment. The purpose of including GUIDE C-code, FBD, LD and ST is primarily for including already written code. However, there could be cases where adaptation is needed in order to incorporate GUIDE C-code, FBD, LD and ST code into GUIDE. As shown in the figure the same compiler is used for the application languages GUIDE C-code, FBD, LD and ST. The compiler takes the source code and generates C-code which is packed into CCP and linked. Separate application editor is used for each of GUIDE C-code, FBD, LD and ST.

A call is always made from the graphic GUIDE component to subroutine defined using GUIDE C-code, FBD, LD or ST. Since IEC 61508 considers a single programming language at a time each of GUIDE C-code, FBD, LD and ST is handled separately. For example, each needs a coding guidelines. Special conditions must be fulfilled if part of the application is implemented in GUIDE C-code, FBD, LD or ST. In order to use more than one language each is compiled separately and linked together.

It is possible to simulate behaviour using Matlab/Simulink and by loading S-Functions created from graphic code. Thus the original is always the graphic code.

It is also possible for a developer to handle externally developed C-code and to create a CCP to be linked with other code. However, in this case the responsibility is completely up to the developer and Danfoss does not give any support. Also, the compiler used to create a CCP needs to match the compiler defined by the HWD file in the project where it is used. This has to be checked manually i.e. without tool support.

Generally, responsibility is shared between Danfoss and the safety function developer when creating safety related applications. In case of doubt, however, the final responsibility always rests with the safety function developer.

Safety measure examples

Parameters

Parameters can be used for supporting variants and also allowing different behaviour. Special care is needed in order to not create inconsistent sets of parameters.

In order to improve safety, read only parameters are recommended but this is up to the application developer to handle. A graphic symbol is used for specifying read only parameters. The application decides how to handle valid and non-valid read only parameters. Read only parameters are stored in NV memory and they are downloaded to the target computer.

The application is able to limit changes of read / write parameters by using the signal “ServiceTool.DisableWrite”. To fulfil the requirements of off-line support tool (see below) this signal has to be used when the machine is in operation.

Notice that, due to HW, the number of writes for NV memory is limited. After the limit has been passed the memory content may become corrupted.

Protection from unauthorized use

The means for protection against unauthorized use are licenses, passwords and application controlled access to the application at runtime.

A lock between target computer and P1D file is needed in order to ensure that only the intended P1D file can be used to access the target computer.

The application itself can decide access to the application at runtime and handle its own password protection.

License is checked for verifying information at start of GUIDE, Service Tool and internal GUIDE executables. License can also be used for Function Blocks and can be decided for each Function Block individually. The data of the license file is both checksummed and encrypted.

Since user identity is stored for several actions it is possible to trace responsible person.

SIL application

For the scope of this report the following applies for a SIL application:

- In the HWD file a flag is set indicating support of SIL application.
- Activity Log is included.
- Only a SIL version of Service Tool can be used for SIL application.

A SIL flag is set in the LHX file if all conditions are fulfilled for a SIL application i.e.

- SIL version of HWD file. Connection is made to specific hardware since information in system file specifies hardware with specific part number.
- SIL version of GUIDE
- COMPILE SIL2 has been used
- Manual acknowledge via dialogues. Application developer user identity is included in LHX file.

Programming languages

Graphic code

The graphic code has the following advantages:

- Non-programmers can understand and create programs
- Clear separation of application and infrastructure/hardware.
- Exhaustive test of graphic symbols is possible since there is a limited number of possible code blocks (one per graphic symbol). This makes it also possible to fully verify an external C-compiler with respect to the code generated by the graphic symbols.

Each application has a top level graphic page. A page may consist of modules, sub-pages and symbols. At each cycle, the execution takes place as a strict sequence from left to right.

Development guidelines exist for use of graphic code.

The application can check its own safety level (SIL or not SIL). It shall be used for stopping the whole SIL application if not all conditions for SIL are fulfilled.

There are many different error messages that could be set as a result from erroneous graphic input.

If the result of a calculation made by a symbol is outside the range of the output type, the output value is undefined. If capped symbols are used the output value is limited to the range of the output type and an overflow output is set active. In any case no warning or error is given. Thus special care is needed.

Before application is started the first time outputs are set to predefined values. Special care is then needed in order to not create a dangerous situation at start up. This is up to the application to handle.

IEC 61131 languages

Each IEC 61131 language has its own definition of strict mode (language subset).

It is not possible to read or write parameter values using an IEC 61131 language.

Coding guidelines exist for each IEC 61131 language.

A graphic component is used for accessing IEC 61131 language code.

An IEC 61131 language subroutine can generate different types of error. Checks are made automatically (by GUIDE at compile time and by runtime support at runtime).

In case deadline is passed when executing IEC 61131 language code the error is propagated back to first called IEC 61131 language subroutine and then to the graphic code where it is handled in the normal way.

C (externally developed)

Since the Danfoss handling of externally developed C-code does not fulfil all requirements in IEC 61508 it means that externally developed C-code shall not be used in SIL applications unless the application developer is able to prove that the implementation fulfills the requirements of IEC 61508.

A graphic component is used for accessing externally developed C-code.

Danfoss does not take any responsibility for including externally generated C-code, this is completely up to the application developer to handle. No guidance is given by Danfoss.

GUIDE C-code

Strict mode is supported.

It is not possible to read or write parameter values directly using GUIDE C-code.

Coding guidelines exist for GUIDE C-code.

A graphic component is used for accessing GUIDE C-code.

GUIDE C-code subroutine can generate different types of error. Checks are made automatically (by GUIDE at compile time and by runtime support at runtime).

In case deadline is passed when executing GUIDE C-code the error is propagated back to first called GUIDE C-code subroutine and then to the graphic code where it is handled in the normal way.

Tools

Classification

In IEC 61508 tools are classified as T1, T2 or T3. T1 concerns e.g. administrative tools, T2 concerns test tools while T3 concerns tools that could affect the behaviour at runtime. The following is a possible classification of Danfoss tools:

1. Software off-line support tool, T2 (Service Tool). Service Tool in combination with P1D file can be used as a test tool during application development.
2. Software off-line support tool, T3 (GUIDE). GUIDE is a compiler/translator and used as a development tool during application development. Test Tool and debugger are included.
3. Software on-line support tool - Not affecting behaviour (Service Tool and P1D file). Even though not explicitly stated in IEC 61508 this case could be seen as matching T2. It is up to the developer to guarantee that the behaviour is not affected when using Service Tool and P1D file at runtime (this is set up in the application). For example, Service Tool changing CAN ID or sending CAN messages in general must, if allowed, be guaranteed not affecting behaviour.
4. Software on-line support tool - Software element according to IEC 61508 (Service Tool). In this case the Service Tool and P1D file combination can affect behaviour at runtime (decided by the application) and is thus considered a part of the safety function (like any other Software Element). This case is complicated since much effort is necessary and Danfoss details are needed.

Compatibility and suitability of other tools used together with Danfoss tools is up to the application developer. Danfoss is responsible for GUIDE and Service Tool working together.

GUIDE

There are several internal checks e.g. detection of corrupt file.

An error, by definition, stops the creation of an executable.

For a SIL application all included application parts are treated as SIL. Everything is compiled from graphics to linkable objects files since the directive COMPILE SIL2 is used. Thus there is no mixture of parts with different SILs. The following conditions apply for fulfilling COMPILE SIL2:

- A market released and certified according to IEC 61508 version of PLUS+1 GUIDE (there are built-in checks if this is the case).
- A released version of an HWD that is certified according to IEC 61508. Such HWD tells the PLUS+1 GUIDE if it supports the "COMPILE SIL2".
- Manual acknowledge via dialogues.

In the HWD file a flag is set indicating support of SIL application.

COMPILE SIL2 enforce Strict Mode for GUIDE C-code, FBD, LD and ST.

A specific Test Tool is included making it possible to verify a complete page including sub-pages and CAN messages, module calls and calls to GUIDE C-code, FBD, LD and ST.

FBD, LD and ST. Graphic code can be compiled to S-Functions which can be verified by executing them in the Matlab/Simulink environment. Thus GUIDE addresses additional tools (T2 tool according to IEC 61508) available for verification and thus improving quality.

Service Tool

As described above the Service Tool in combination with P1D file can have different roles. Especially important is to be aware of the roles at runtime. For not affecting behaviour at runtime an analysis has to be made concerning the application handling this situation.

There are several internal checks e.g. detection of corrupt file.

To download a "Compile SIL2" application the following conditions apply:

- A market released and certified according to IEC 61508 version of Service Tool (there are built-in checks if this is the case).
- Only a SIL version of Service Tool can be used for SIL application.

The Service Tool reads back a checksum of the downloaded data, calculated by the boot loader of the hardware after the download is completed.

Service Tool blocks download if error is detected.

Service Tool can handle different nodes in a CAN network e.g. it is possible to set parameters via CAN (if a valid P1D file is available and the application allows parameter setting).

A USB/CAN gateway makes it possible to connect external tools via USB interface in order to get access to CAN bus used for communication between target computers.

References

[1] IEC 61508:2010, parts 1-7

[2] PLUS+1 9.0 Evaluation, 7P02281:B, 2017-06-30