TYPE EXAMINATION CERTIFICATE

46 24 03

PLUS+1 Development tools, version 10.0.X

Issued to

Danfoss Power Solutions AB,

Teknikgatan 1, SE-34334 ÄLMHULT, Sweden

Product name and description

The PLUS+1 development tools, version 10.0.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 10.0.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 10.0 are fulfilled for graphic code, GUIDE C-code, Structured Text, Function Block Diagram, Ladder Logic Diagram code, Instruction lists, Sequential function chart but not for externally developed C-code
- IEC 61508 tool requirements for Service Tool version 10.0 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 RISE report 8P01100:A supplemented with a separate evaluation of the PLUS+1 Development tools described in RISE report 8P01100:B and the user documentation in the currently valid revision. The external C-compilers that are fully verified to be used with PLUS+1 GUIDE 10.0 are listed in RISE reports 8P01100:B and 8P01100:C.

Marking

Each sample that conforms in all respects with the original item certified may display the text "Type-examined by RISE". 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 2021-06-27.

Miscellaneous

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

Martin Tillander

Jan Jacobson

REPORT

Contact person RISE	Date	Reference	Page
Johan Hedberg Electronics +46 10 516 50 71 johan.hedberg@ri.se	2018-09-11	8P01100:C	1 (9)

Danfoss Power Solutions AB
Teknikgatan
S-343 34 ÄLMHULT
SWEDEN

PLUS+1 10.0 Safety Evaluation Overview

Test object

The test object is PLUS+1 tools GUIDE version 10.0 and Service Tool version 10.0 developed by Danfoss Power Solutions AB.

Summary

The conclusion is that Danfoss PLUS+1 tools GUIDE version 10.0 and Service Tool version 10.0 is certified according to IEC 61508:2010 under certain conditions.

RISE Research Institutes of Sweden AB
Electronics - Dependable Systems

Examined by

Johan Hedberg Signed by: Johan Hedberg
Reason: I am the author of this document

Johan Hedberg

Examined by

Innehåll

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 [1]. This document is an extract of “RISE report PLUS+1 10.0 Safety Evaluation, 8P01100:B, 2018-03-21” and is intended for users as initial information when considering Danfoss Power Solutions AB PLUS+1 tools [2].

The PLUS+1 Development tools are two, namely:

- GUIDE tool, that handles the translation of graphic symbols to executable code [3].
- Service Tool, that handles the download of the executable code to hardware [4].

These are certified according to IEC 61508:2010, but under certain circumstances.

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 10.0.X (where X is an integer ≥ 1), however there could be coming versions that may have effects on this document. Check with Danfoss if uncertainties.

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 10.0, which are defined by the referenced documents as given below.

The test object was delivered to RISE Electronics 2017-12-08.

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”, “Instruction List” and “Sequential Function Chart” 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”, “Instruction List” or “Sequential Function Chart” as defined in IEC 61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
IEC 61508	IEC 61508:2010 part 1-7
IL	“Instruction List” programming language defined in IEC61131-3 Second edition 2003-01, Programmable controllers – Part 3:Programming languages
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
SFC	“Sequential Function Chart” programming language defined in IEC61131-3 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 Johan Hedberg and Ted Strandberg, RISE Electronics, during the period from February 2018 to March 2018.

Results apply to the test object only.

PLUS+1 Overview

The Danfoss Power Solutions AB PLUS+1 tools are used to create applications, typically for controlling heavy, powerful, and mobile off-road equipment such as tractors, cranes, and harvesters.

The PLUS+1 tools consists of GUIDE which is a graphical programming environment and Service Tool which is a tool for downloading applications or parameters to a controller.

GUIDE contains a drawing area where graphical components could be “dragged and dropped”. The graphic components creates a clear separation of application and infrastructure/hardware and has the advantage that non-programmers can understand and create programs.

The software to components containing controllable logic can be developed in GUIDE using different programming languages. GUIDE supports the Danfoss graphic language, GUIDE C-code, FBD, LD, IL, ST and SFC [3]. GUIDE also supports standard C-code since there could be cases when it is necessary to incorporate externally developed C-code. The purpose of including all the languages is primarily for making it easy to include already written code.

Each of the application languages is entered in separate code editors. The application code is translated into C-code and compiled into a compiled code package CCP, linked and packed into a LHX-file containing the binaries. As shown in Figure 1, the same compiler is used for all the application languages. Each of the languages is handled separately, compiled separately and then linked.

The Service Tool can connect to a target computer and download an LHX-file. The Service Tool can also retrieve the binaries from a target computer, as well as configure parameters on the target.

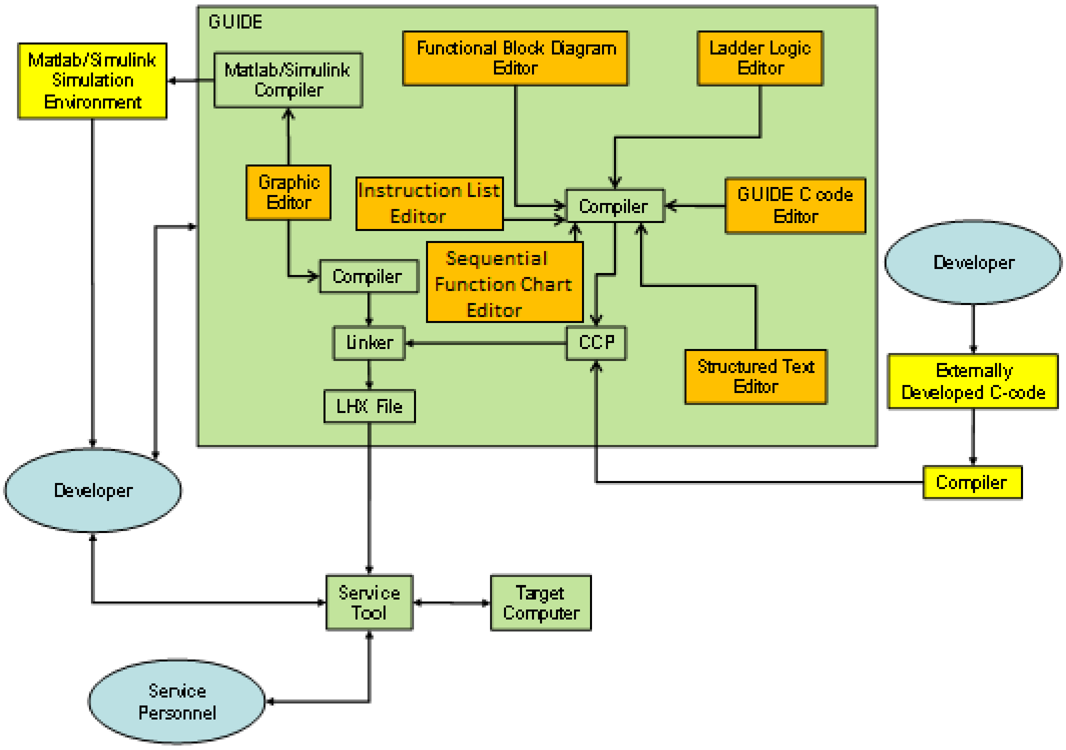

Figure 1: Plus+1 development environment.

61508 Classification of support tools

Software support tools can, according to 61508, be classified as either **software on-line support tools** or **software off-line support tools.** The on-line tools can directly influence the safety-related system during its run-time, while the off-line tools cannot.

The **software on-line support tools** are considered as part of the safety function and must fulfil 61508 requirements like any other software element.

The **software off-line support tools** must fulfil the requirements for off-line support tools in 61508, clause 7.4.4 and be categorized according to the following classes:

– T1
generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system, e.g. a text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools.

– T2

supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software, e.g. a test harness generator; a test coverage measurement tool; a static analysis tool.

– T3
generates outputs which can directly or indirectly contribute to the executable code of the safety related system, e.g. an optimising compiler where the relationship between the source code program
and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code.

GUIDE

GUIDE is classified as a **software off-line support tool** since it cannot directly influence the safety related system during its runtime. GUIDE includes text editors, test tools, debuggers, compilers/translators and is used as a development tool during application development. Thus, GUIDE can be categorized as all the subclasses **T1, T2** and **T3**, but it is enough to consider the highest category; **T3**.

Service Tool

The classification of the Service tool is somehow more complex. It can be used both as a **software on-line support tool** and as a **software off-line support tool.**

In GUIDE the parameters ‘ServiceTool.DisableWrite’, ‘ServiceTool.DisableRead’ and ‘ServiceTool.DisableDownload’ can be used in the projects when developing an application. The disable parameters determine the ability of Service Tool to influence the application during runtime. If ‘ServiceTool.DisableWrite’ and ‘ServiceTool.DisableDownload’ is set, Service Tool cannot change any parameter and Service Tool is then to be classified as a **software off-line support tool.**

If ‘ServiceTool.DisableWrite’ and ‘ServiceTool.DisableDownload’ is not set, Service Tool is classified as a **software on-line support tool.**

This means that the classification of Service Tool is indirectly controlled by GUIDE, since the disable parameters are set by the developer when developing the software for a controllable component. Thus, the aspect of changeable parameters and 61508 fulfilment of off-line support tool needs to be considered already in GUIDE during the application development.

If Service Tool is used as a **software off-line support tool**, it is categorized as subclass **T2** since it is seen as a test tool used during application development but not contributing to the executable code.

If Service tool is used as a **software on-line support tool**, it is considered as part of the safety function, and must fulfil 61508 requirements like any other software element.

Protection from unauthorized use

The means for protection against unauthorized use are application access control, licenses and passwords.

The disable parameters described in previous section can be used to control if the Service Tool can access the target during runtime or not.

Access to components can be limited by access levels. There are 10 different access levels (0-9) where 9 has the least access rights, and 0 has the most rights. The access levels can be applied on different categories as for example read, write, diagnostic data, error data and other data where each have its own access level.

To protect the application against unauthorized use a lock between target computer and P1D file is used. This locking is achieved by Service Tool using Tool Key. Without Tool Key protection, there is an increased risk that unauthorized personnel could use Service Tool to view and change your application’s operating parameters.

License is checked at start of both GUIDE and Service Tool. The data of the license file is both encrypted and provided with a checksum.

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

SIL application development

It is possible to use the GUIDE to develop SIL classified components. For SIL classified components all included application parts are treated as SIL and needs to fulfil the requirements for that SIL level. Thus, there is no mixture of parts with different SIL levels.

To be able to compile a SIL application the following needs to be fulfilled:

- The hardware must have a released version of an HWD that is certified according to IEC 61508. Such HWD tells the PLUS+1 GUIDE by a flag if it supports the 'COMPILE SIL2'.
- A market released and certified according to IEC 61508 version of PLUS+1 GUIDE must be used. There are built-in checks in GUIDE to make sure that it is a market released version. The user needs to check that the concerned version is certified by looking at Danfoss homepage.
- The developer must manually acknowledge SIL requirements in GUIDE via dialogues during development phase.
- When creating SIL components, the SIL components must be developed using Strict Mode which means that compiler warnings are treated as errors. Normally the developer can choose how warnings should be treated in the compiler settings, but when compiling SIL-applications the code is always compiled in Strict Mode. The Strict Mode applies for GUIDE C-code, FBD, LD, ST, IL and SFC.
- Extern C-code is not allowed.

If all conditions are fulfilled for a SIL application, the 'COMPILE SIL2' button will become visible in the GUIDE menu bar and compilation is possible.

The String data type is as of now not allowed in SIL classified units; however, it is still possible to perform a 'COMPILE SIL2' with Strings included since there is today no automatic control excluding Strings in the tool set. Thus, the application developer must make sure that no Strings are included in the project before compiling SIL2 applications.

The SIL application must be downloaded to target by a market released and certified according to IEC 61508 version of Service Tool. Service Tool makes sure that it is a market released version by internal checks, but the user needs to check that the concerned version is certified by looking at Danfoss homepage.

Languages

The code should follow a coding guideline, and for GUIDE C-code this means MISRA C coding guideline[6]. Each of the IEC 61131 languages FBD, LD, ST, IL and SFC have their own coding guideline which are defined in the PLC Open Coding Guidelines [5].

It is also possible for a developer to handle externally developed C-code. The code is compiled into a CCP and can be linked with other code. 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.

Since the Danfoss handling of externally developed C-code does not fulfil all requirements in IEC 61508 the externally developed C-code shall not be used within SIL applications unless the application developer is able to prove that the implementation fulfils the requirements of IEC 61508. Danfoss does not take any responsibility for including externally generated C-code, this is completely up to the application developer to handle.

Compilers

The following C-compilers are fully verified to be used with PLUS+1 GUIDE 10.0.

Compiler	**Flags**	**PLUS+1 GUIDE naming**
GNU ARM Embedded Toolchain 4.7-2013-q2	-c -fno-inline-small-functions -mthumb -mcpu=cortex-m3 -O2 -fwrapv -fsigned-char -mlittle-endian -Wall -Wno-main	ARM v4.7-2013q2
Sourcery G++ ARM EABI 2006q1-3	-g -c -mcpu=arm7tdmi-s -w -O2	arm-elf v410
Sourcery G++ Lite ARM EABI Sourcery G++ Lite 2009q3-68	-c -fno-inline-small-functions -mthumb -mcpu=cortex-m3 -O1 -fsigned-char -mlittle-endian -Wall -Wno-main	Sourcery G++ Lite arm-2009q3-68
Texas Instruments C2000 Code Generation Tools v5.2.5	-pm -o3 -q -g -pdv -pden -pdw -pdse225 -d"LARGE_MODEL" -ml -v28 -pdf -me	TI v525
Texas Instruments C2000 Code Generation Tools v6.4.9	-pm -o3 -q -g -pdv -pden -pdw -pdse225 -d"LARGE_MODEL" -ml -v28 -pdf -me	TI v649

References

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

[2] Danfoss PLUS1 10.0 Safety Evaluation, 8P01100:B, 2018-02-13

[3] PLUS+1 GUIDE User Manual, 10100824 · Rev 1503 April 2017

[4] PLUS+1 GUIDE Service Tool User Manual, L1307770 • Rev 0401 March 2017

[5] PLCopen Coding Guidelines 2016-04-21
http://www.plcopen.org/pages/pc2_training/index.htm

[6] MISRA C:2012 Coding Guidelines
https://www.misra.org.uk/Buyonline/tabid/58/Default.aspx