

Data sheet

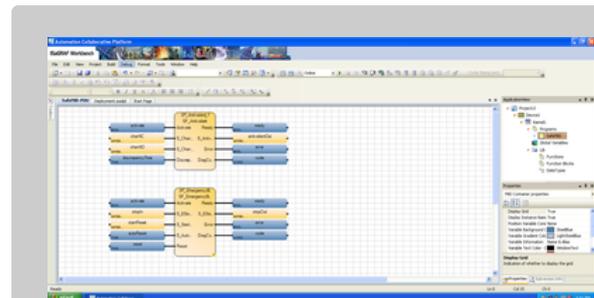
FlexiSafe®

FlexiSafe® is based on ISaGRAF technology. It is designed to facilitate the IEC 61508 SIL or the ISO 13849 certification of an OEM industrial automation product. It provides the fundamental elements required for certification:

- ISaGRAF has SC3 certification (Systematic Capability of 3)
- Evidence of the rigorous development environment and procedures at ISaGRAF
- Firmware technology that can be ported to any safety operating system, including a suite of validation and verification tools
- 100% test reports on the various TIC instructions, executed by an independent organisation
- Application code verification tool (diverse compiler)
- Other tools to help certify the end-user safety functions, depending on application safety concept (PLC Open safety function blocks, Cause and Effect diagram, static checker, version source control, cross-reference browser, dependency tree,...)

FlexiSafe® Safety Concept:

- Ability to reuse the technology and leverage the certification effort across multiple hardware platforms
- Simplify the design and certification of end-user applications
- Fail-Safe certification



FlexiSafe®

FlexiSafe® Certification Approach:

- Port the certified runtime to the target hardware platform and OS (taking into account the FlexiSafe® and OS safety manuals)
- Several safety measures are already included in the runtime
- Service of validation of porting using rigorous system layer and overall coverage testing suite
- No requirement for 100% testing of the end-user application (functional tests only)
- End-user application can take advantage of all IEC 61131-3 languages, including SFC
- No restrictions on the use of function blocks
- Integrated safety management and application life

Kernel Validation:

- Proven in use – 850,000 runtimes, 14 years of use in safety and critical control industry

- Encapsulation of safety functions; wrappers around functionality to validate correct and safe operation; program sequence validation
- Portable test harness to ensure correct functionality and no side effects; combination of black-box and white-box tests; covers overall kernel operation (I/O, online updates, ...) and every single TIC instruction

Compiler verification:

- Ensure compiler output is correct, matches source code input, and contains only essential elements of the input
- Uses both a diverse compiler and a de-compiler to generate language-neutral graphs
- XML graph comparison covers structure, flow, variables, and parameters
- Works with all IEC 61131-3 languages (ST, IL, LD, FBD, SFC)

Dependency trees:

- Forward dependencies to show variables derived from root
- Backward dependencies to show variables contributing to root
- Used by static analysers for impact analysis and SIL verification

Your benefit:

FlexiSafe® offers several benefits to the customer:

- SIL-certified firmware and configuration: This product fulfills requirements of the SC 3 and can be used in applications requiring SIL3. This also applies to ISO 13849 PLe.
- Reduced time to market
- Standardised and fully compatible with IEC 61131 standard
- Unlimited use of any of the IEC 61131 elements
- Standardised and fully compatible with PLC Open safety function blocks
- Flexible, adaptable to most hardware platforms using an O/S that fulfills SC3 requirements

To achieve this, FlexiSafe® focuses on providing a system that supports distributed applications, mixed safety and non-safety functionality, extensive safety management, and application life cycle tools. The FlexiSafe® solution targets any automation vendor seeking to develop a safety system requiring SIL 1, SIL 2, SIL 3 or PLe certification.

All hardware and software names used are brand names and/or trademarks of their respective holders.

© 2014, infoteam Software AG.

Right of modifications reserved.

Contact

Phone: +49 (0) 9131 / 78 00 - 0 infoteam Software AG
Fax: +49 (0) 9131 / 78 00 - 50 Am Bauhof 9
info@infoteam.de D-91088 Bubenreuth