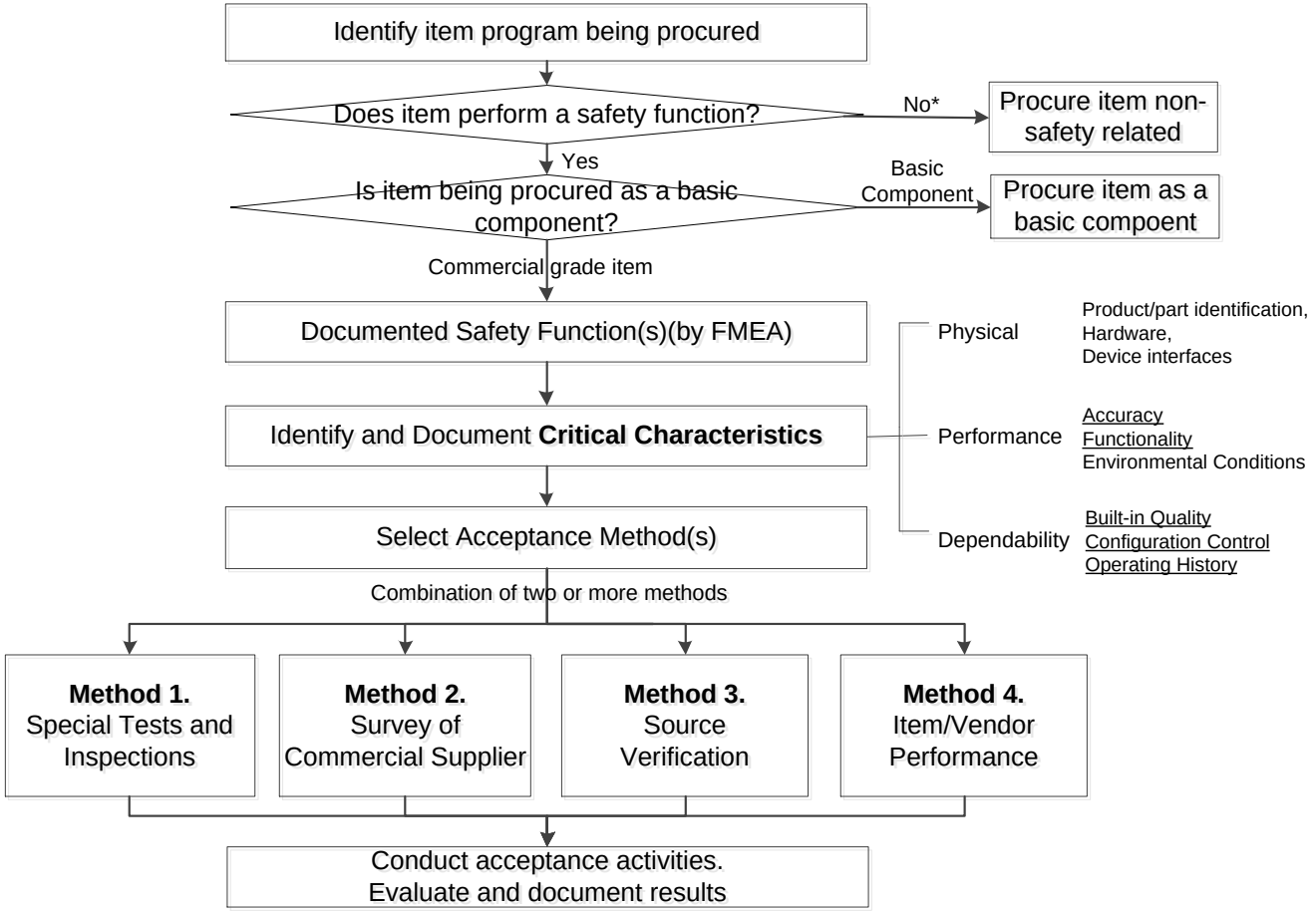
COTS SW Dedication

Introduction and Concept

정세진
Dependable Software Laboratory
Konkuk Univ.

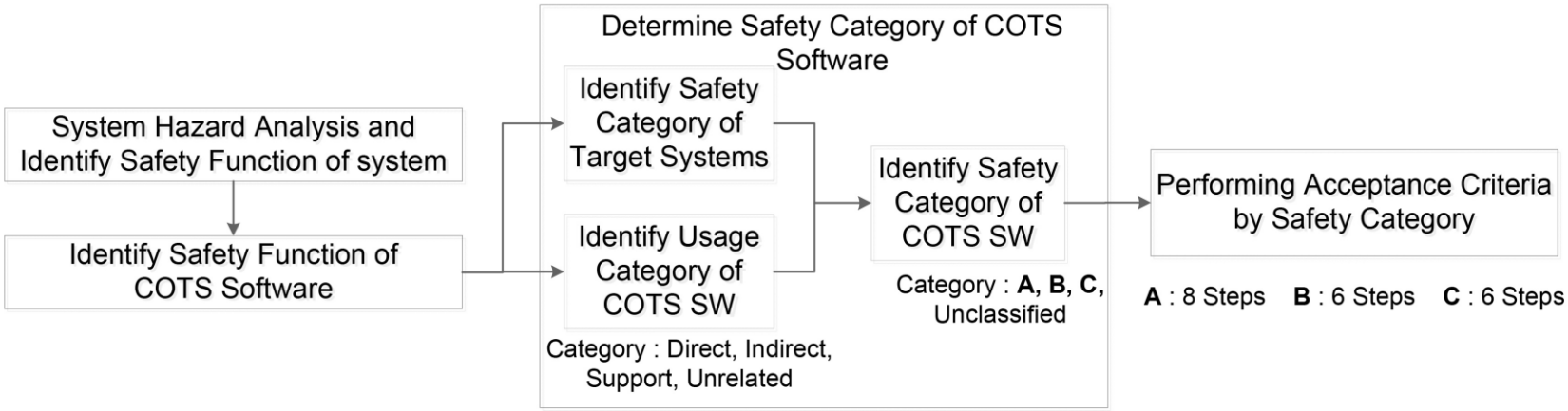
NP-5652/TR-106439

- **The process overview of NP-5652**
  - **Performing combination of 4 methods to dedicate**
  - **Targeting direct items**



NUREG/CR-6421 process overview

- **The overview of NUREG/CR-6421 process**
  - **Preliminary phase of criteria**
    - **Identify safety function of SW**
    - **Determine safety category of target COTS SW**
  - **Detailed acceptance criteria**
    - **Apply acceptance criteria accordance with safety category**



LINTING

Linting

- **Linter program checks static errors or potential errors and coding style guideline violations**
  - **variables being used before being set**
  - **division by zero**
  - **conditions that are constant**
  - **calculations whose result is likely to be outside the range of values representable in the type used**
  - **Mixed lananguage**
  - **Coding style check**
  - **Etc**

- **일반적으로 FPGA 개발에서는 RTL design에 적용됨**

RTL Linting

- RTL linting is kinds of static analyzer for RTL design + rule checking
- There are several linting tools
  - Leda of Synopsys
  - SpyGlass lint of atrenta in synopsys
  - Ascent Lint of Real Intent
  - VHDL rule checker of Sigasi
  - HAL of cadence => Cadence Circuit Design Tools 에서 사용할 수 있음
- They checks with their own rules and user defined rules also
- Ascent Lint of Real Intent
  - FSM state reachability and coding issues
  - Legal but dubious modeling indicating probable errors
  - Differences between simulation and synthesis semantics
  - Naming and RTL coding conventions
  - Subset restrictions to enforce modeling clarity and reduce complexity
  - Opportunities to improve simulation performance
  - Operations with hidden or expensive implementation costs
  - Downstream tool flow issues
  - Network and connectivity checks for clocks, resets, and tri-state-driven signals
  - Module partitioning rules
  - Design testability

RTL Linting Rules

- 상용 도구들의 자세한 규칙에 대한 내용은 접근 불가
- Functional safety standard에 의한 safety lifecycle 에서 verification phase 에 static analysis포함
- ModelSim 에서는 몇몇 규칙에 대해서 optional 하게 제공
  - when Module ports are NULL.
  - when assigning to an input port
  - when referencing undeclared variables/nets in an instantiation
- Microsemi Libero SoC 11.5, Synopsys Synplify Pro에서 linting 혹은 static analysis를 수행한다는 것을 data sheet, white paper, guideline 에서 찾아 볼 수 없었음

NUREG/CR-7006

- NUREG/CR-7006 is the “Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems”
- It is design practice and guidelines for developing FPGA based NPP safety systems
- Providing design practice guidelines for improving safety of FPGA
  - Explain FPGA design about potentially unsafe
  - It contains board-level (Hardware) design issue and HDL (Verilog, VHDL) design issues
- NUREG/CR-7006 uses framework of NUREG/CR-6463
  - Reliability
  - Robustness
  - Traceability
  - Maintainability

NUREG/CR-7006 Design Entry Example

- Reliability
- If and Case Statements
  - All of branches in if, case statements should be specified explicitly

- Maintainability
- Vendor-Specific Intellectual Property Cores
  - Using IP Core library is able to reduce development cost and improve efficiency
  - However, using in safety critical system should be avoided, because it makes hard to verify the system

Structural Analysis about FBD for safety critical software

- NUREG/CR-6463기반의 Guideline 및 Rule Checker
  - Reliability
    - Correct Control Flow
    - Correct Variables and Functions
    - Type Conversion
  - Maintainability
    - Drawing Diagram
    - Defining Variables
    - Abstraction

- Verilog/VHDL 등에 없는 keyword 사용에 대해 추가적인 제약사항 필요
  - Data type에서도 없는 keyword가 존재 (e.g. ANY_DURATION – TIME, LTIME)

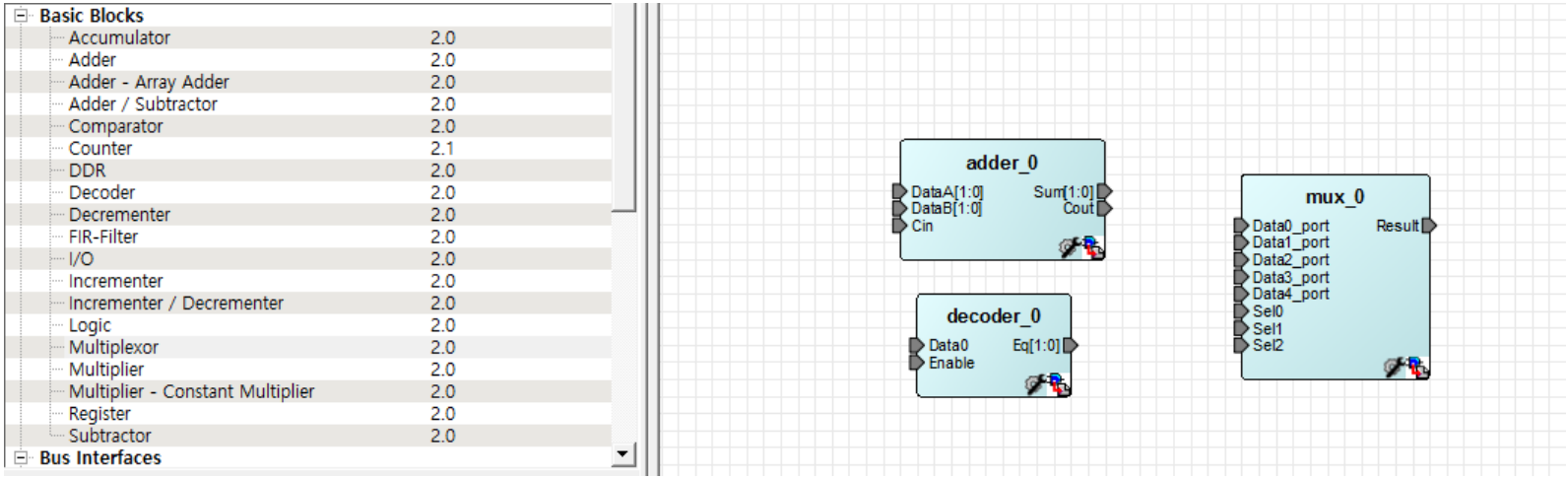
- NuDE 환경에서 FBD Rule checker를 FPGA 에 사용 할 때의 영향
  - HDL 에 존재하지 않는 KEYWORD (Data type 등) 사용 제약 추가 필요
  - 변환기에서 7006 의 내용 적용이 필요

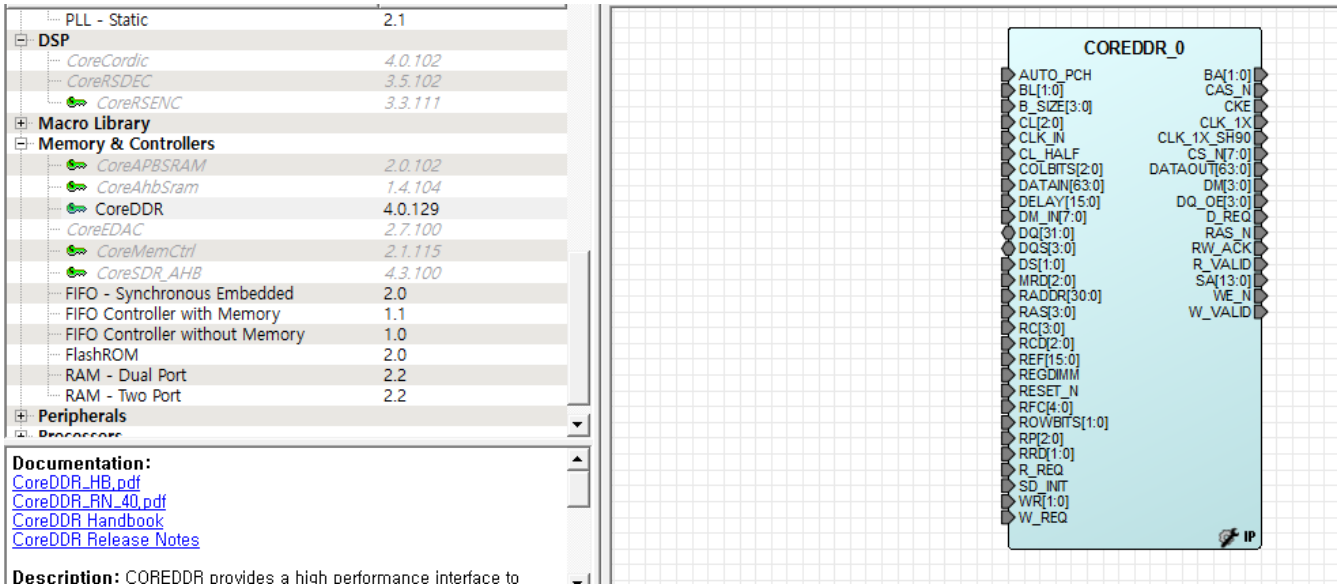
IP CORE LIBRARY

IP Core Library

- IP (Intellectual Property) Core in FPGA
  - Design, cell, chip, logic 등 다시 사용 할 수 있는 것들
  - 복잡한 시스템의 설계를 간단히 하기 위해 미리 정의한 기능과 회로의 라이브러리
    - Vendor, 3rd party 등에서 제공
  - Microsemi 에서는 Libero SoC 안의 Smart Design tool 에서 IP Core 사용을 제공
    - RTL code도 이용 가능

IP Core using example in Smart Design

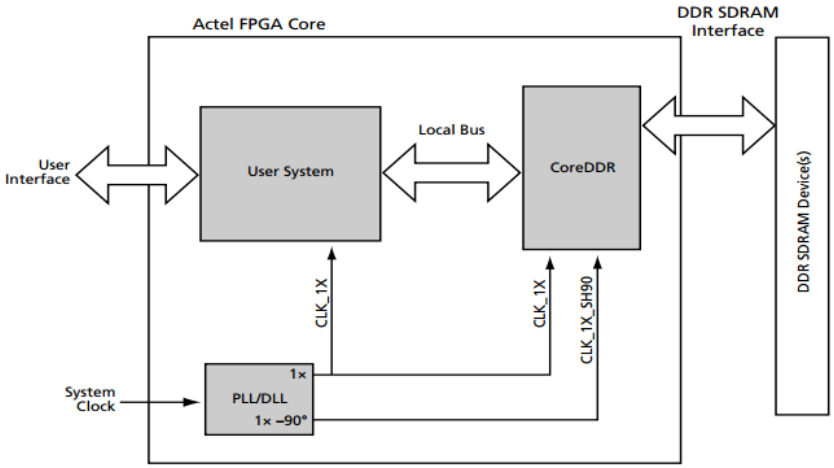




IP Core Library

- Generally, direct core is provided with release note, handbook, data sheet, V&V report, etc.

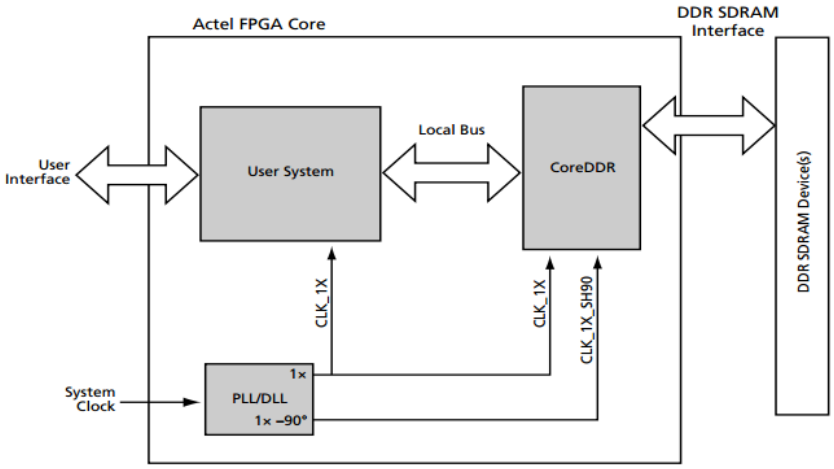
- CoreDDR is a high-performance SDRAM controller that is optimized for Microsemi FPGAs and designed to simplify system design while maximizing memory bandwidth and overall system performance



- Accordance with NUREG/CR-7006, IP core library is not recommended to use in safety systems
  - 만약 사용한다면, dedication 의 대상이라고 볼 수 있음
  - 검증된 IP Core library를 사용해야 함

IP Core Library

- 전체 시스템



IP Core Library

- **Library로 제공되는 controller**

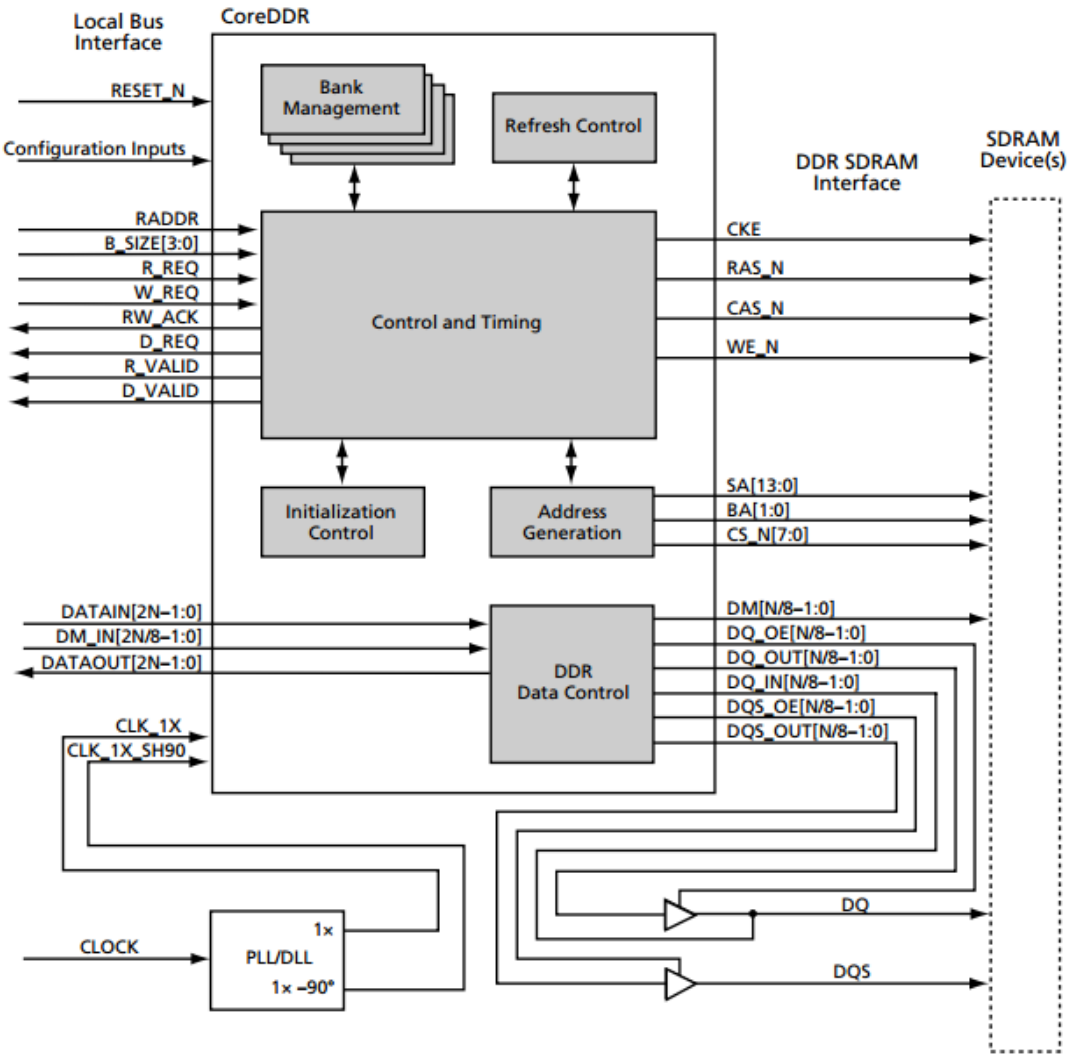
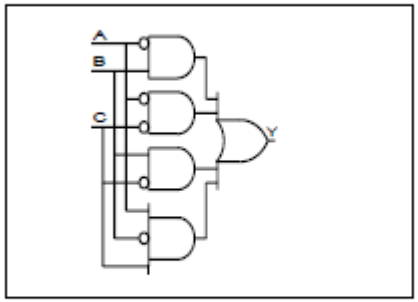


Figure 1-2 · DDR SDRAM Controller Block Diagram

Vendor (Chip) specific macro libraries

- 각 벤더 (chip) 별로 합성, P&R 등의 편의성을 이유로 macro libraries 를 지원
  - Dedication 대상 이라기 보다는 대상 vendor의 IDE나 Synthesis 도구의 V&V 과정에서 확인 되어야 할 대상으로 생각

AO12 — IGLOO, ProASIC3, SmartFusion, Fusion



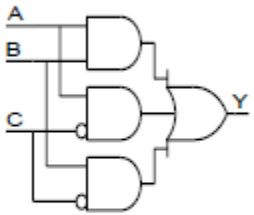
Function: 3-Input AND-OR

Truth Table

A	B	C	Y
0	0	0	1
1	0	0	0
0	1	0	1
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	0

Input: A, B, C — Output: Y

AO13 — IGLOO, ProASIC3, SmartFusion, Fusion



Function: 3-Input AND-OR

Truth Table

A	B	C	Y
0	0	0	0
1	0	0	1
0	1	0	1
1	1	0	1
0	0	1	0
1	0	1	0
0	1	1	0
1	1	1	1

Input: A, B, C — Output: Y

OTHER STANDARDS ABOUT DEDICATION

Other Standards

- In addition to, there are some standards about COTS dedication
- TR-107330 : “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants”, 1996
- TR-107339 : “Evaluating Commercial Digital Equipment for High Integrity Applications A Supplement to EPRI Report TR-106439”, 1997
  - 106439 보충
- TR-104159 : “Experience with the Use of Programmable Logic Controllers in Nuclear Safety Applications”
  - PLC를 대상으로 dedication 경험
- NP-7218 : “Guideline for Sampling in the Commercial Grade Item Acceptance Process”, 1992
- TR-017218 : “Guideline for Sampling in the Commercial-Grade Item Acceptance Process (Revision of NP-7218)”, 1999
  - Sampling guideline => 전자/전기 기기들을 대상으로 특별시험 적용시에 sampling 가이드라인

Other Standards

- **TR-103699 V1-2 : "Programmable Logic Controller Qualification Guidelines for Nuclear Applications", 1994**
  - **PLC qualification guideline : 106439의 기반?**

- **TR-1025243 : "Plant Engineering : Guidelines for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications", 2013**

- **NP-6406 : "Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants (NCIG-11), 1989**
- **TR-1008256 : "Plant Support Engineering : Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants (Revision of NP-6406)", 2006**
  - **NP-5652의 technical evaluation 부분에 대한 추가적인 가이드라인**

- **NP-6895 : "Guidelines for the Safety Classification of Systems Components, and Parts Used in Nuclear Power Plant Applications (NCIG-17)", 1991**

Other Standards

- **ASME NQA-1**
- **TR-112579 : “Critical Characteristics for Acceptance of Seismically Sensitive Items”, 2007**
  - **Seismically sensitive 한 제품들의 critical characteristics에 대해 설명**
- **TR-1016157 : “Plant Support Engineering: Information for Use in Conducting Audits of Supplier Commercial Grade Item Dedication Programs”**
- **NUREG-6294 : “Design Factors for Safety-Critical Software”, 1994**

However…

- Evaluation of Guidance for Tools Used to Develop Safety-Related Digital Instrumentation and Control Software for Nuclear Power Plants by NRC
  - ~~Task 1 Report : Survey of the State of Practice~~
    - Survey of concerning the use of software tools
  - Task 2 Report : Analysis of the State of Practice, 2014, 350 pages
    - 여러 산업 표준들에 대해 detailed analysis 수행,
  - Task 3 Report : Technical Basis for Regulatory Guidance, 2015, 80 pages
    - Technical basis for software tool regulatory guidance for review and acceptance of software tools

    Software tools: A computer program supporting or used in the design, development, testing, review, analysis, or maintenance of a PDD or its documentation. Examples include compilers, assemblers, linkers, comparators, cross-reference generators, decompilers, editors, flow charters, monitors, test case generators, integrated development environments, timing analyzers, simulators, and thermal-hydraulic analysis programs. (Adapted from IEEE Std. 7-4.3.2 [6])

  - 각종 산업 (auto, railway, nuclear, aerospace, aviation), 각종 기관 (NRC, IEEE, IEC, IAEA, EPRI, NIST, AECL, NASA, etc) 의 regulatory guideline, practice, experience, standard, TR을 통하여 safety-related or safety system 개발에 사용되는 software tool의 selection, evaluation, acceptance 등 the safety assessment of software tool 에 대한 내용 정리 및 분석, regulatory guidance를 위한 기초 제공 목적

- TR-1025243 : Plant Engineering : Guidelines for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications, 2014
  - Computer program의 dedication에 대해 내용 제공

Common Position

- **Licensing of safety critical software for nuclear reactors**
  - **It is *"Common position of international nuclear regulators and authorized technical support organisations"***
  - **Common technical positions on a set of important licensing issues**

- **Task force, which contains 7 countries, establish documents for licensing issues of safety critical software (Licensing issues of safety critical software for nuclear reactors)**
  - **Belgium, Germany, Canada, Spain, United Kingdom, Sweden, Finland**

- **In the later, the U.S. NRC has participated in the meetings of the task force**

This document should neither be considered as a standard, nor as a new set of European regulations, nor as a common subset of national regulations, nor as a replacement for national policies. It is the account, as complete as possible, of a common technical agreement among

- **National regulations may have additional requirements or different requirements, but hopefully in the end no essential divergence with the common positions.**

Common Position

- This documents consists of involved issues, common positions, recommended practices about each licensing issues

- It provides 23 issues about licensing
  - 1.1 Safety Demonstration
  - 1.2 System Classes, Function Categories and Graded Requirements for Software
  - 1.3 Reference Standards
  - 1.4 Pre-existing Software (PSW)
  - 1.5 Tools
  - 1.6 Organizational Requirements
  - 1.7 Software Quality Assurance Program and Plan
  - 1.8 Security
  - 1.9 Formal Methods
  - 1.10 Independent Assessment
  - 1.11 Graded Requirements for Safety Related Systems (New and Pre-existing Software)
  - 1.12 Software Design Diversity
  - 1.13 Software Reliability
  - 1.14 Use of Operating Experience
  - 1.15 Smart Sensors and Actuators

  - 2.1 Computer Based System Requirements
  - 2.2 Computer System Architecture and Design
  - 2.3 Software Requirements, Architecture and Design
  - 2.4 Software Implementation
  - 2.5 Verification
  - 2.6 Validation and Commissioning
  - 2.7 Change Control and Configuration Management
  - 2.8 Operational Requirements

The END

END

FUNCTIONAL SAFETY

IEC 61508 Functional Safety

- 전자, 전기 시스템의 기능 안전을 위한 표준
  - 특정 분야에 구애 받지 않은 전반적인 요구사항
  - E/E/PE safety-related system의 기능 안전성을 달성하기 위해 필요한 관리 및 기술적 활동을 명시
- Safety Life Cycle
  - 기능 안전 달성을 위한 활동을 체계적으로 관리하기 위해 제안 및 채택
  - 7.5 전체 안전 요구사항 : Hazard & Risk analysis를 통해 E/E/PE safety-related system, 기타 기술 안전 관련 시스템, 외부 리스크 감소 설비에 대하여 안전기능 요구사항 및 완전무결성 요구사항의 측면에서 전체 안전 요구사항에 대한 명세서를 개발함으로써 기능 안전성을 달성
    - 각 위험원에 대해 요구되는 기능안전성을 확보하기 위해서 필요한 안전기능들이 명시 되어야 함
    - 리스크 감소 측면에서, 안전무결성 요구사항 (SIL) 이 각 안전기능에 대해 명시되어야 한다

- 61508-3 requirements 중 소프트웨어 개발
  - 7.4.2.11 표준화된 소프트웨어 또는 기존에 개발된 소프트웨어가 설계단계에서 활용된다면, 해당 소프트웨어를 분명하게 파악해야 한다. 소프트웨어 안전 요구사항 명세를 만족하는데 대한 소프트웨어 적합성은 그 근거가 제시 되어야 한다.
  - 개발에 사용되는 언어, 컴파일러, 형상관리 도구, V&V 도구 세트는 SIL 에 따라 선택 되어야 한다
  - SIL 수준에 따라 확증 인증서를 보유한 번역기/컴파일러를 가져야 함
  - 충족되지 못하면 그 타당성을 문서화 되어야 함

  - 부록으로 정적분석의 몇몇 항목에 대해 표로 표시하고 있음

Functional Safety Certification

- **SIL(Safety Integrity Level) : 제품의 안전 기능에 요구되는 신뢰도 수준**
  - **Using Performance Measures, probability of the safety function operation**

Safety-Integrity Level (SIL)	High demand rate (dangerous failures/hr)	Low demand rate (Probability of failure on demand)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

Functional Safety Certification

- **Standards for providing the requirements for the functional safety system**
  - **IEC 61508 : functional safety of electrical, electronic, and programmable electronic equipment**
  - **IEC 61513 : for NPP system**
  - **IEC 60880 : for category A software**
  - **IEC 62138 : for category A software**
  - **ISO 26262 : for automotive**

- **This product receives IEC-61508 SIL2 certification**
  - 내압방폭 구조로서 폭발 위험지역에 설치하여 가연성, CO2, CO, N2O가스를 연속적으로 감지

적외선 타입 가스감지기

CERTIFICATE

CERTIFICATE NO FS/71/220/14/0030 PAGE 1/1

'LICENCE HOLDER'
GASTRON CO.,LTD
18-8, DOGEUMDANJI1(IL)-GIL, SANGROK-GU, ANSAN-SI, GYEONGGI-DO, KOREA

'MANUFACTURING PLANT'
GASTRON CO.,LTD
18-8, DOGEUMDANJI1(IL)-GIL, SANGROK-GU, ANSAN-SI, GYEONGGI-DO, KOREA

PROJECT NO/-ID	LICENSED TEST MARK	CERT. REPORT NO.
F1MW		F1MW0003

Tested according to	IEC 61508: 2010
Certified product(s)	Infrared Type Gas Detector
Model(s)	GIR-3000
Technical Data and Parameter	Type B device with HFT=0 for the particular Safety Functions : Suitable for safety related systems in low demand mode up to and including SIL 2
Specific Requirements	The certificate is for type approval and based on voluntary tests. Any changes to the design, materials, components or processing may require repetition of some of the qualification tests in order to retain type approval. The certification report is an integral part of this certificate. All requirements and constraints of the current valid revision of this report shall be met.

Certification Body
for Functional Safety
SGS-TÜV Saar GmbH

Munich, 2014-02-11

Marcus Rau

SafeTI™ 소프트웨어 개발 프로세스, ISO 26262 및 IEC 61508 "기능 안전" 표준에서 ASIL D 및 SIL 3 레벨 인증 취득

2015-02-12 오전 10:26:38 · 편집부

Hercules™ MCU 소프트웨어 컴포넌트를 위한 새로운 SafeTI 인증 지원 패키지로 "기능 안전성" 개발 및 인증 지원

TI(대표이사 켄트 전)는 자사의 SafeTI™ "기능 안전" 소프트웨어 개발 프로세스가 ISO 26262 및 IEC 61508 준수 소프트웨어 컴포넌트 개발에 적합하다고 인증 받았음을 발표했다. 이 프로세스는 품질 및 안정성 규격에 대한 적합성을 평가하는 국제 공인 독립 평가 기관인 TÜV NORD(독일기술검사협회)에서 심사하였다.

더불어 TI는 인증된 소프트웨어 개발 프로세서를 기반으로 새로운 SafeTI 인증 지원 패키지(CSP, Compliance Support Package)를 개발하였으며, 현재 Hercules™ 마이크로컨트롤러(MCU) 소프트웨어 컴포넌트에 사용되고 있다. CSP는 Hercules 소프트웨어를 이용하는 고객들이 자사의 최종 시스템의 "기능 안전성" 인증을 더욱 수월하게 달성할 수 있도록 하기 위해 개발되었다.

SafeTI CSP는 정적 및 동적 분석 테스트 결과, 규격 적합성에 대한 코드 추적가능성(code traceability to requirements), 코드 커버리지, 코드 품질 지수 등을 포함하고 있다. 고객들은 이 CSP를 이용함으로써 소프트웨어 검증 작업에 대한 수고를 줄이고, 최종 시스템의 "기능 안전성" 인증을 보다 쉽게 달성할 수 있다.

TI는 CSP 개발에 LDRA(Liverpool Data Research Associates) 소프트웨어 분석 툴 수트를 이용하고 있다. 또한, 이들 CSP는 LDRAunit®을 활용한 테스트 자동화 유닛(Test Automation Unit)을 포함하며 고객들은 그들의 환경에 이 유닛 레벨 테스트 사례를 채실행할 수 있다. 이들 CSP는 HALCoGen(Hardware Abstraction Layer Code Generator) 디바이스 드라이버와 Hercules MCU의 SafeTI 진단 라이브러리에 이용할 수 있다.

이러한 TÜV 인증 SafeTI "기능 안전" 소프트웨어 개발 프로세스와 이를 적용한 SafeTI CSP, 그리고 최근 출시된 인증 Hercules TMS57011x/12x 및 RM46x MCU는 향후 고객들이 기능 안전 애플리케이션을 간편하게 개발할 수 있도록 도와주는 포괄적인 SafeTI 설계 패키지로, TI의 고객 지원을 위한 노력을 잘 설명해주고 있다.

공급 시기

TI의 HALCoGen 디바이스 드라이버와 SafeTI Hercules 진단 라이브러리에 이 CSP를 이용함으로써 고객들은 제품의 출시 시간을 단축하고 검증 작업에 대한 수고를 줄이며, 소프트웨어 안전 작업을 간소화할 수 있다. 현재 이들 CSP 평가판 뿐만 아니라 1인용 또는 멀티용 정식 라이선스도 이용 가능하다.

IEC 60880 고려사항

- Software tool 선택은 (개발에 사용되는) 60880의 1~12 chapter의 요구사항을 만족하거나 15 chapter의 assessment를 만족해야 함 => dedication 관점과 비슷하게 사용됨
  - 60880의 전체적인 내용과 dedication에서 사용하고 있는 그런 critical characteristics를 통한 criteria와 잘 매핑을 시켜보면서 두개의 연관성에 대해 고려해 보고 생각 할 수 있을 것으로 판단됨

- 적용되어야 하는 assessment수준은 tool의 type에 따라 달라짐
  - 1. compiler, translator
  - 2. verification tools
  - 3. os
  - 4. development support systems (e.g. word processor?)
  - 5. version control tool (e.g. svn)
  - 각각의 분류에 따른 수준에 대한 언급 부족

- Compiler, translator의 optimization
  - Should be avoided
  - 사용 한다면, 컴파일 결과에 대해 test, verification, validation 반드시 수행

COMMON POSITION EXAMPLE

1.4 Pre-existing Software – Issues Involved

- **Issues involved**
  - **A set of issues about licensing**

- **Issues about 1.4 pre-existing software**
  - **The functional behavior and non-functional qualities of the PSW is often not clearly specified and documented**
  - **It is not certain that developing under safety life cycle like IEC 60880**
  - **The operational experience of the PSW are not often enough to compensate for the lack of knowledge on the PSW (information about product and development process)**

1.4 Pre-existing Software – Common Position

- **Common Position**
  - **A set of common positions on the basis for licensing and evidence which should be sought by task forces**

- **Common positions about 1.4 pre-existing software**
  - **The functions that have to be performed by PSW, shall be clearly and unambiguously specified**
  - **The code version of PSW shall be clearly identified**
  - **The interfaces (the user or other software) shall be clearly identified**
  - **The PSW shall have been developed and maintained according to QA standards and software development process**
  - **Documentation and source code shall be available if modification**
  - **Documents of quality assurance plan and development process shall be available**
  - **Conditions for accepting**
    - **Verify the functions performed by the PSW about requirements specification**
    - **The PSW functions shall be validated by testing**
  - **Defects which are found during validation shall be analyzed**

1.4 Pre-existing Software – Recommended Practices

- **Recommended Practices**
  - **Consensus on best design and licensing recommended practices by task forces**

- **Recommended Practices about 1.4 pre-existing software**
  - **Operational experience may be regarded as evidence to validation or verification**
  - Configuration of the PSW;
    - Functions used;
    - Types and characteristics of input signals, including the ranges and, if needed, rates of change;
    - User interfaces;
    - Number of systems.
  - Demand rate and operating time data should include:
    - Elapsed time since first start-up;
    - Elapsed time since last release of the PSW;
    - Elapsed time since last severe error (if any);
    - Elapsed time since last error report (if any);
    - Types and number of demands exercised on the PSW.
  - Error reports should include:
    - Descriptions and dates of errors, severity;
    - Descriptions of fixes.
  - Release history should include:
    - Dates and identifications of releases;
    - Descriptions of faults fixed, functional modifications or extensions;
    - Pending problems.

Example of Certification by IEC 61508

- **This product receives IEC-61508 SIL2 certification**
  - **내압방폭 구조로서 폭발 위험지역에 설치하여 가연성, CO2, CO, N2O가스를 연속적으로 감지**

적외선 타입 가스감지기

Prev

SGS TÜV SAAR

CERTIFICATE NO FS/71/220/14/0030 **PAGE 1/1**

LICENCE HOLDER
GASTRON CO.,LTD
18-8, DOGEUMDANJI1(IL)-GIL,
SANGROK-GU, ANSAN-SI,
GYEONGGI-DO, KOREA

MANUFACTURING PLANT
GASTRON CO.,LTD
18-8, DOGEUMDANJI1(IL)-GIL,
SANGROK-GU, ANSAN-SI,
GYEONGGI-DO, KOREA

PROJECT NO/-ID	LICENSED TEST MARK	CERT. REPORT NO.
F1MW	SGS TÜV SAAR FUNKTIONALE SICHERHEIT GEPRÜFT FUNCTIONAL SAFETY APPROVED	F1MW0003

Tested according to	IEC 61508: 2010
Certified product(s)	Infrared Type Gas Detector
Model(s)	GIR-3000
Technical Data and Parameter	Type B device with HFT=0 for the particular Safety Functions Suitable for safety related systems in low demand mode up to and including **SIL 2**
Specific Requirements	The certificate is for type approval and based on voluntary tests. Any changes to the design, materials, components or processing may require repetition of some of the qualification tests in order to retain type approval. The certification report is an integral part of this certificate. All requirements and constraints of the current valid revision of this report shall be met.

Certification Body
for Functional Safety
SGS-TÜV Saar GmbH

Munich, 2014-02-11

Marcus Rau

CERTIFICATE

TI development process

- **SafeTI software development process receive functional safety ceritification**

SafeTI™ 소프트웨어 개발 프로세스, ISO 26262 및 IEC 61508 "기능 안전" 표준에서 ASIL D 및 SIL 3 레벨 인증 취득

2015-02-12 오전 10:26:38 편집부

Hercules™ MCU 소프트웨어 컴포넌트를 위한 새로운 SafeTI 인증 지원 패키지로 "기능 안전성" 개발 및 인증 지원

TI(대표이사 켄트 전)는 자사의 SafeTI™ "기능 안전" 소프트웨어 개발 프로세스가 ISO 26262 및 IEC 61508 준수 소프트웨어 컴포넌트 개발에 적합하다고 인증 받았음을 발표했다. 이 프로세스는 품질 및 안정성 규격에 대한 적합성을 평가하는 국제 공인 독립 평가 기관인 TÜV NORD(독일기술검사협회)에서 심사하였다.

더불어 TI는 인증된 소프트웨어 개발 프로세서를 기반으로 새로운 SafeTI 인증 지원 패키지(CSP, Compliance Support Package)를 개발하였으며, 현재 Hercules™ 마이크로컨트롤러(MCU) 소프트웨어 컴포넌트에 사용되고 있다. CSP는 Hercules 소프트웨어를 이용하는 고객들이 자사의 최종 시스템의 "기능 안전성" 인증을 더욱 수월하게 달성할 수 있도록 하기 위해 개발되었다.

SafeTI CSP는 정적 및 동적 분석 테스트 결과, 규격 적합성에 대한 코드 추적가능성(code traceability to requirements), 코드 커버리지, 코드 품질 지수 등을 포함하고 있다. 고객들은 이 CSP를 이용함으로써 소프트웨어 검증 작업에 대한 수고를 줄이고, 최종 시스템의 "기능 안전성" 인증을 보다 쉽게 달성할 수 있다.

TI는 CSP 개발에 LDRA(Liverpool Data Research Associates) 소프트웨어 분석 툴 수트를 이용하고 있다. 또한, 이들 CSP는 LDRAunit®을 활용한 테스트 자동화 유닛(Test Automation Unit)을 포함하며 고객들은 그들의 환경에 이 유닛 레벨 테스트 사례를 재실행할 수 있다. 이들 CSP는 HALCoGen(Hardware Abstraction Layer Code Generator) 디바이스 드라이버와 Hercules MCU의 SafeTI 진단 라이브러리에 이용할 수 있다.

이러한 TÜV 인증 SafeTI "기능 안전" 소프트웨어 개발 프로세스와 이를 적용한 SafeTI CSP, 그리고 최근 출시된 인증 Hercules TMS57011x/12x 및 RM46x MCU는 향후 고객들이 기능 안전 애플리케이션을 간편하게 개발할 수 있도록 도와주는 포괄적인 SafeTI 설계 패키지로, TI의 고객 지원을 위한 노력을 잘 설명해주고 있다.

공급 시기

TI의 HALCoGen 디바이스 드라이버와 SafeTI Hercules 진단 라이브러리에 이 CSP를 이용함으로써 고객들은 제품의 출시 시간을 단축하고 검증 작업에 대한 수고를 줄이며, 소프트웨어 인증 작업을 간소화할 수 있다. 현재 이들 CSP 평가판 뿐만 아니라 1인용 또는 멀티용 정식 라이선스도 이용 가능하다.