

COTS SW Dedication

Introduction

정세진

Dependable Software Laboratory

Konkuk Univ.

2015.10.07

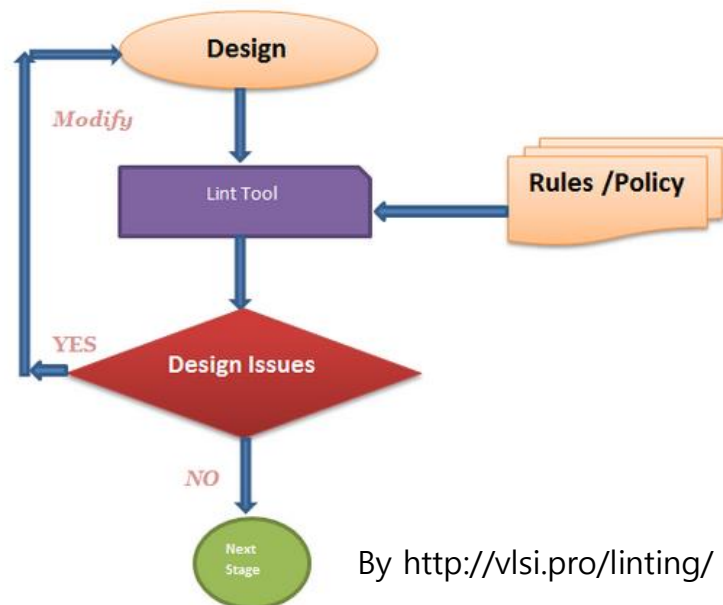
LINTING

Linting

- **Lint 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**
- **IEC 60880 같은 safety life cycle 에서 static analysis 때 적용**
 - 합성 도구와는 별개로 독립적으로 적용
 - 합성 도구에서 syntax check 는 수행

RTL Linting

- **Synthesis 이전에 Linting을 수행하면?**
 - Static error의 가능성을 발견하고, false alarm 이 존재할 가능성이 있지만 사용자가 미리 수정 할 수 있음
- **컴파일러 verification 의 간접 방법으로 사용?**
 - 합성 이전의 문제 발견을 위해 코드 체크하는 검증 방법으로 사용
- **상용 Linter program을 Safety-critical system 개발에 사용한다면**
 - 시뮬레이터와 같은 분석 도구 수준의 dedication이 필요할 것으로 생각 (TR-1025243)



By <http://vlsi.pro/linting/>

IP CORE LIBRARY

IP Core Library

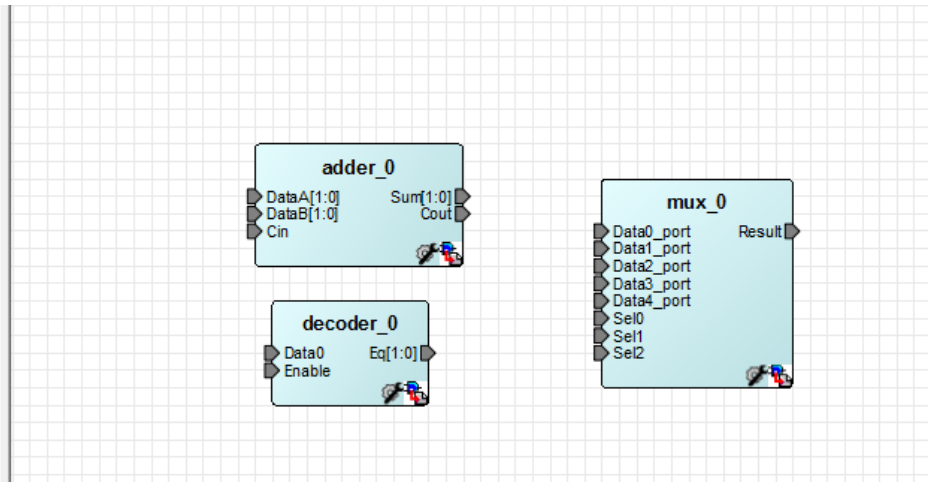
- **IP (Intellectual Property) Core in FPGA**
 - 복잡한 시스템의 설계를 간단히 하기 위해(편의성 및 효율성) 미리 정의한 기능과 회로의 라이브러리
 - Vendor, 3rd party 등에서 제공
 - Design, chip, cell, logic, etc
 - Microsemi 에서는 Libero SoC 안의 Smart Design tool 에서 IP Core 사용을 제공

IP Core using example in Smart Design

- Smart Design 에서의 IP Core 사용 example

Basic Blocks	
Accumulator	2.0
Adder	2.0
Adder - Array Adder	2.0
Adder / Subtractor	2.0
Comparator	2.0
Counter	2.1
DDR	2.0
Decoder	2.0
Decrementer	2.0
FIR-Filter	2.0
I/O	2.0
Incrementer	2.0
Incrementer / Decrementer	2.0
Logic	2.0
Multiplexor	2.0
Multiplier	2.0
Multiplier - Constant Multiplier	2.0
Register	2.0
Subtractor	2.0

Bus Interfaces	
PLL - Static	2.1

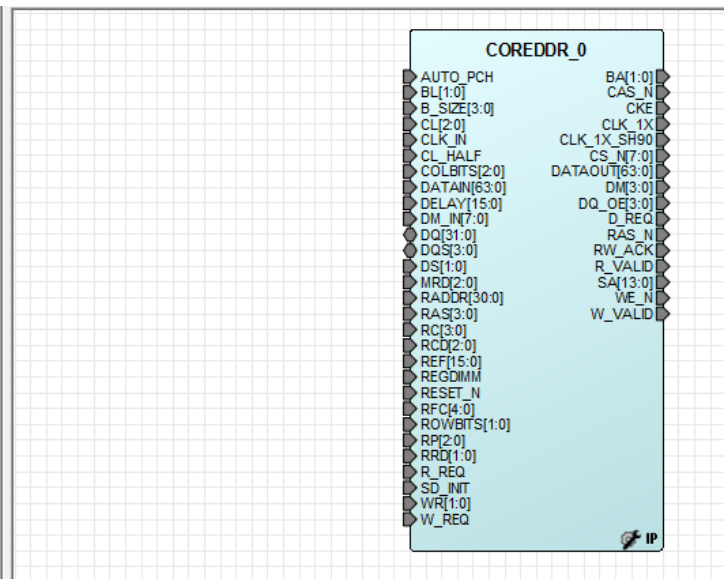


CoreCordic	4.0.102
CoreRSDEC	3.5.102
CoreRSENC	3.3.111

Macro Library	
Memory & Controllers	
CoreAPBSRAM	2.0.102
CoreAhbSram	1.4.104
CoreDDR	4.0.129
CoreEDAC	2.7.100
CoreMemCtrl	2.1.115
CoreSDR_AHB	4.3.100
FIFO - Synchronous Embedded	2.0
FIFO Controller with Memory	1.1
FIFO Controller without Memory	1.0
FlashROM	2.0
RAM - Dual Port	2.2
RAM - Two Port	2.2

Documentation:
[CoreDDR_HB.pdf](#)
[CoreDDR_RN_40.pdf](#)
[CoreDDR Handbook](#)
[CoreDDR Release Notes](#)

Description: COREDDR provides a high performance interface to



IP Core Library

- Library로 제공되는 controller spec

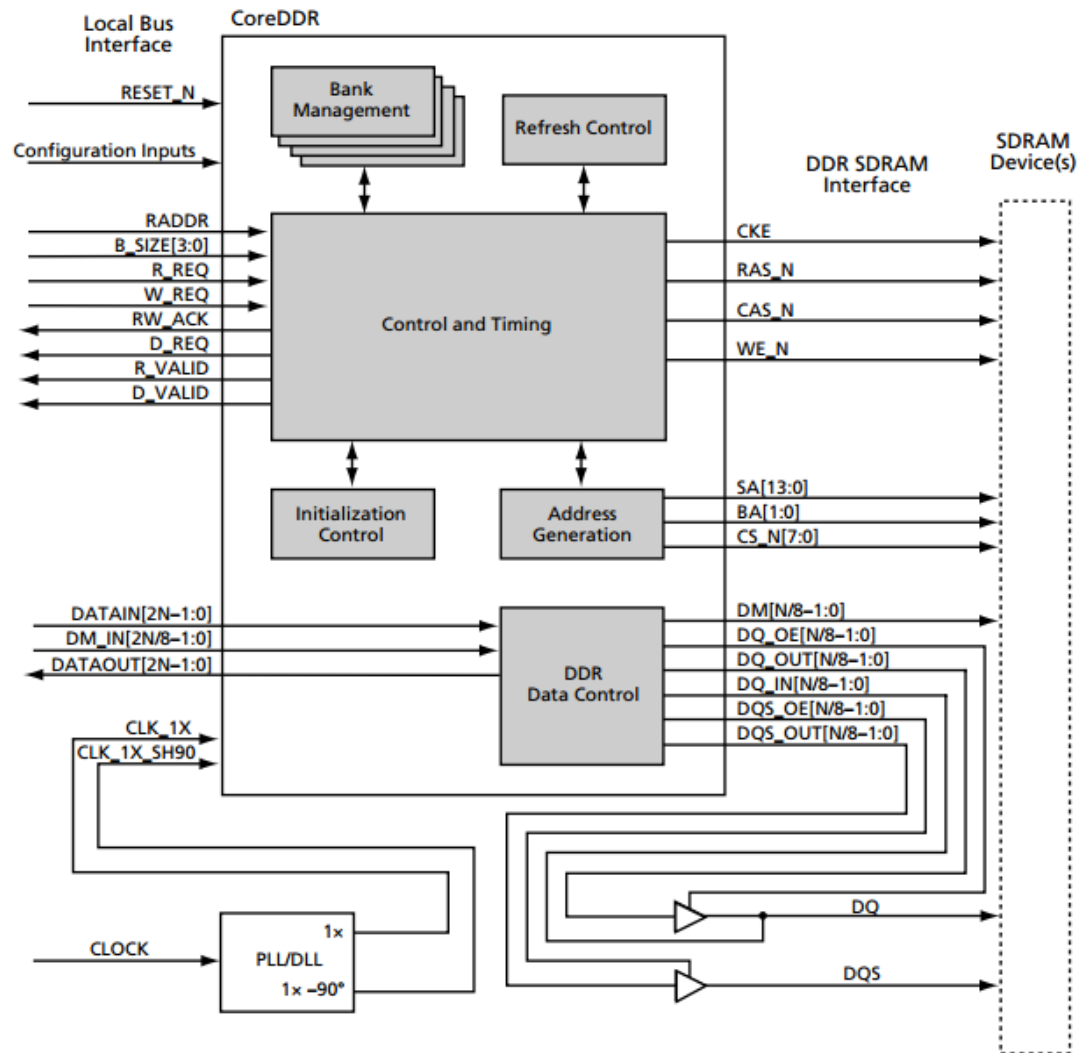


Figure 1-2 · DDR SDRAM Controller Block Diagram

IP Core Library

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

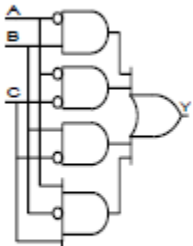
IP Core Library

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

Vendor (Chip) specific macro libraries

- 자주 사용하는 게이트 및 게이트 조합을 매크로화 시킨 라이브러리
 - Dedication 대상 이라기 보다는 대상 vendor의 IDE나 Synthesis 도구의 V&V 과정에서 확인 되어야 할 대상으로 생각
- Microsemi Libero SoC 11.5
 - Logic Synthesis 시 사용된 게이트에 따라 자동으로 Macro Library가 적용됨
 - 제공되는 Smart Design 도구에서도 같은 Macro library 사용

AO12 IGL00, ProASIC3, Smart



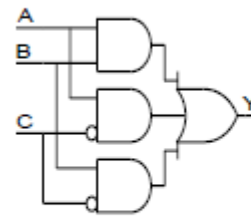
Function
3-Input AND-OR

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 IGL00, 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**

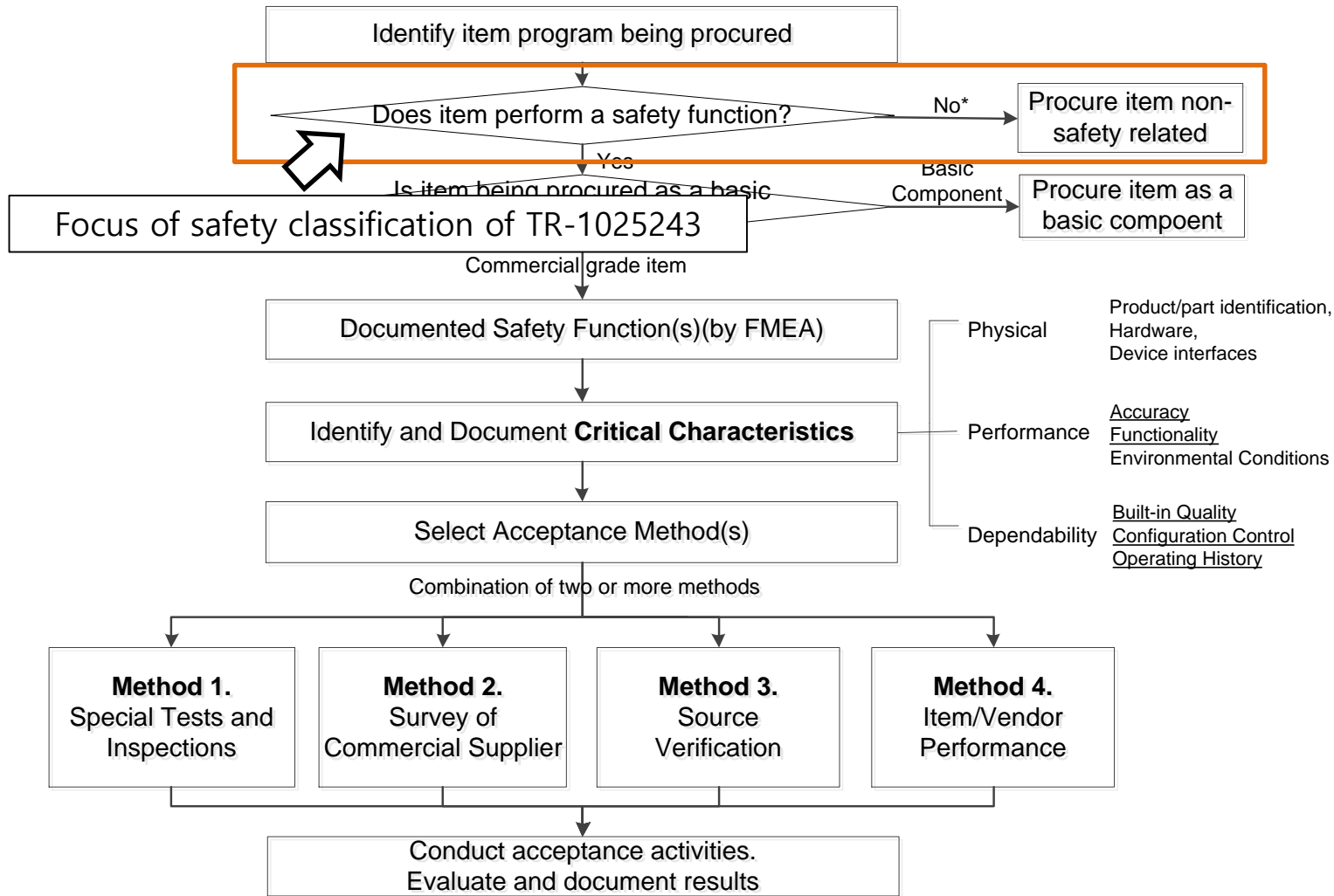
Software tools: A computer program supporting or used in the design, development, testing, review, analysis, or maintenance of a PDD or its documentation. Examples include compilers, assemblers, linkers, comparators, cross-reference generators, decompilers, editors, flow charters, monitors, test case 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, 아직 Regulatory Guide 로 제정까지는 아님

TR-1025243

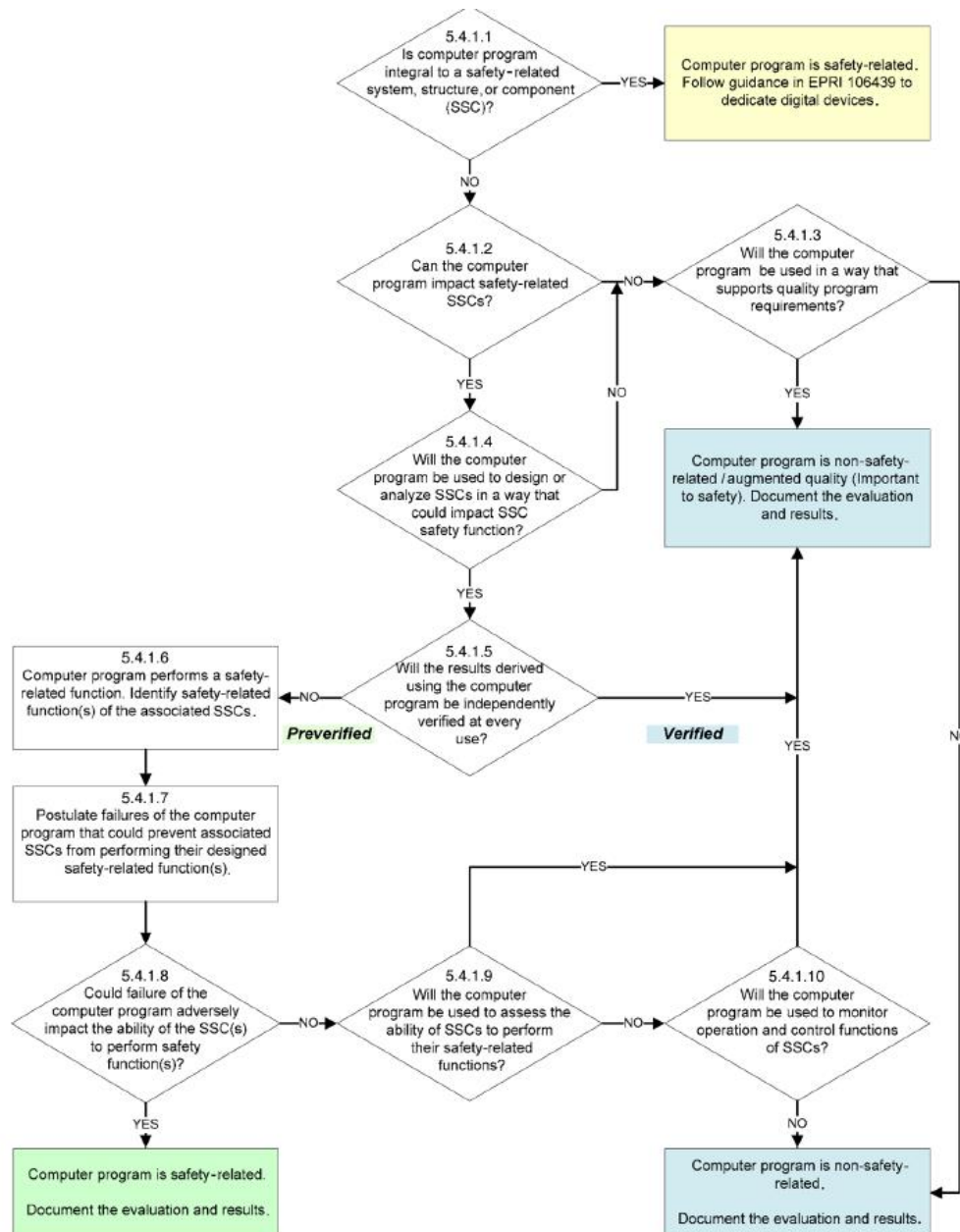
TR-1025243

- Commercial computer program (SW)의 acceptance guideline 제공
- NP-5652의 process 기반
 - Technical evaluation
 - Functional safety classification
 - FMEA
 - Identify Critical Characteristics
 - Documenting the results of technical evaluation
 - Acceptance process로 구성
- Functional Safety Classification
 - NP-5652/TR-106439와 다른 점
 - Computer program의 분류
 - Safety-related : dedication 수행
 - Non safety-related : dedication 수행 없이 사용
 - 2 가지 접근 방법이 존재
 - Failure mode and effects
 - Impact analysis

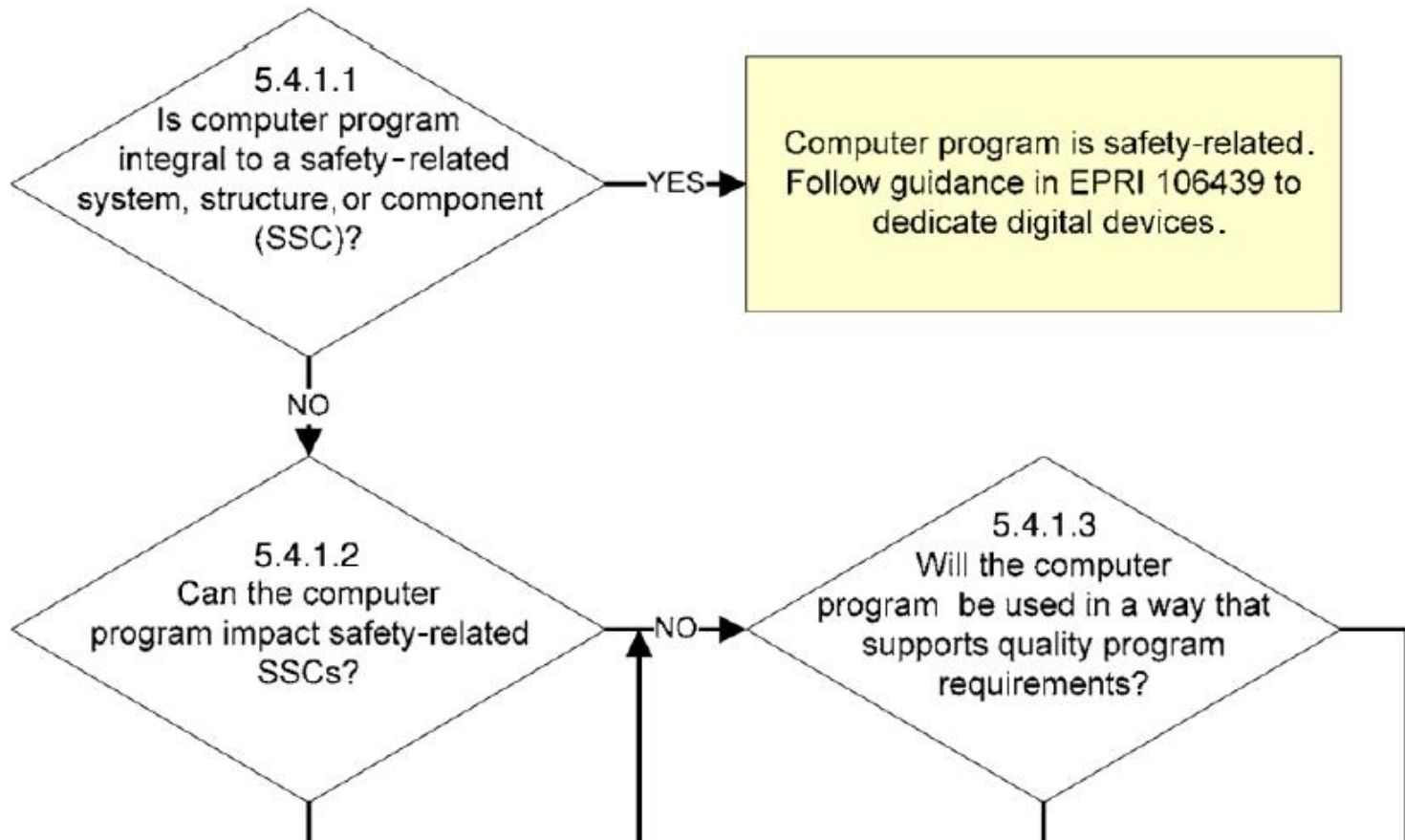
Acceptance Process of NP-5652



Safety Classification – FME



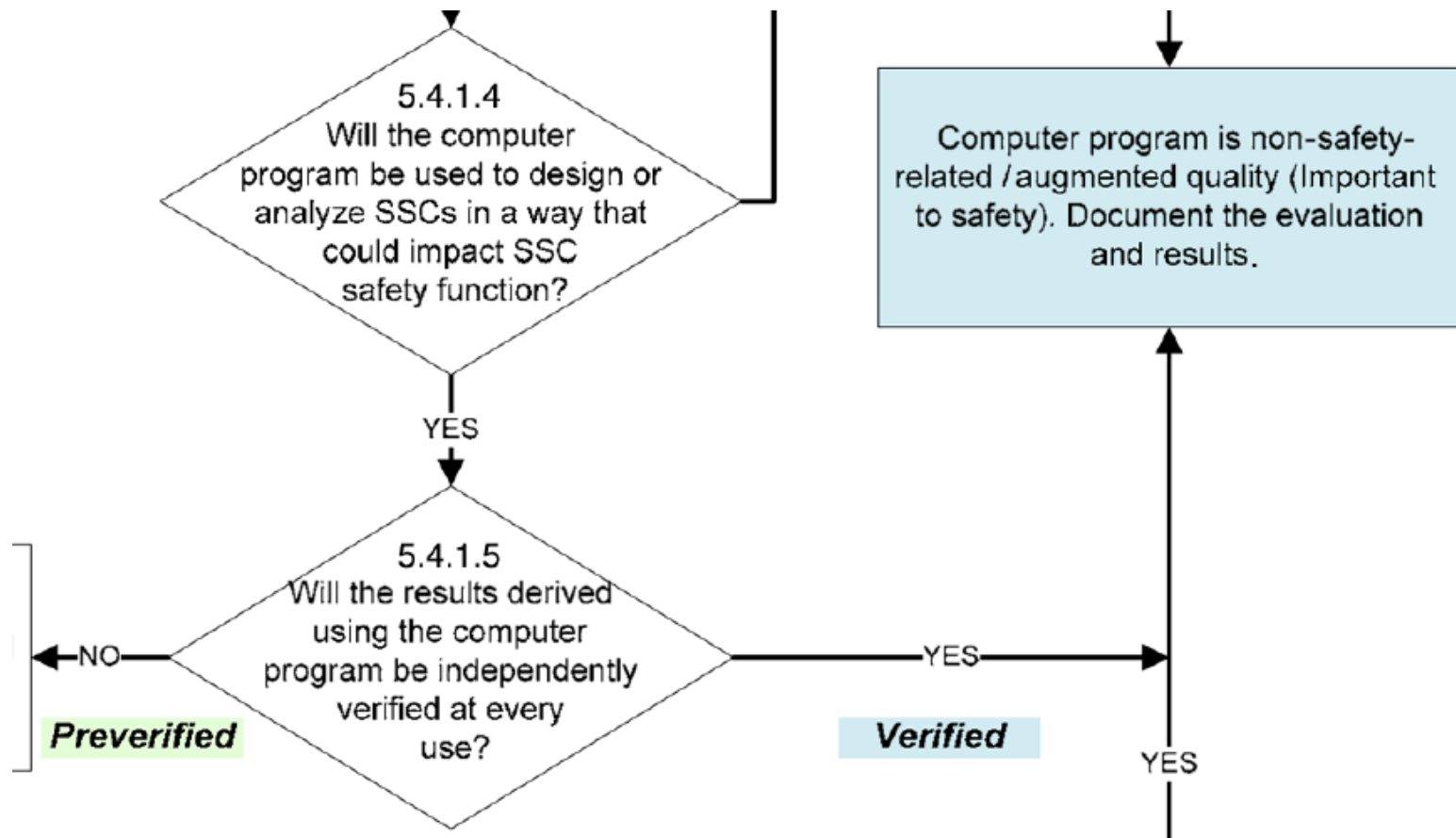
Safety Classification – FME



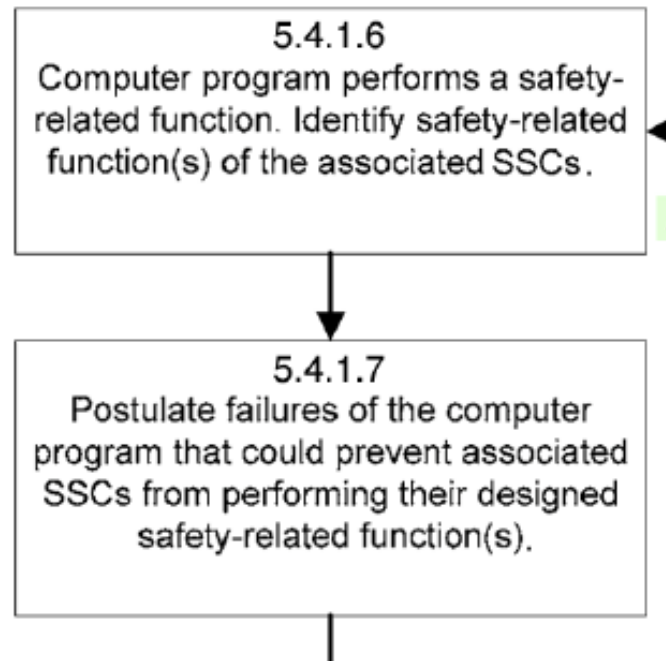
Safety Classification – FME

- 5.4.1.1
 - Safety related SSC (System, Structure, Component) 에 필수적인지 확인
 - E.g. PLC 에 바로 들어가서 원자력 I&C에 동작하는 computer program
 - TR-106439의 software based digital equipment dedication 수행
- 5.4.1.2
 - Computer program이 safety-related SSC에 연관이 있는가?
 - Used to facilitate **design**
 - Used to **analyze** how the safety-related SSC will function or design?
 - Used to **monitor** operation, control functions
- 5.4.1.3
 - Computer program이 quality program requirements 를 지원하는 용도로 사용되는가 확인
 - Supports quality program requirements
 - Document control or records management system
 - Dose management system
 - Tracking corrective actions
 - Maintain training records and transcripts
 - Emergency response preparedness
 - Non-safety-related but augmented quality

Safety Classification – FME



Safety Classification – FME



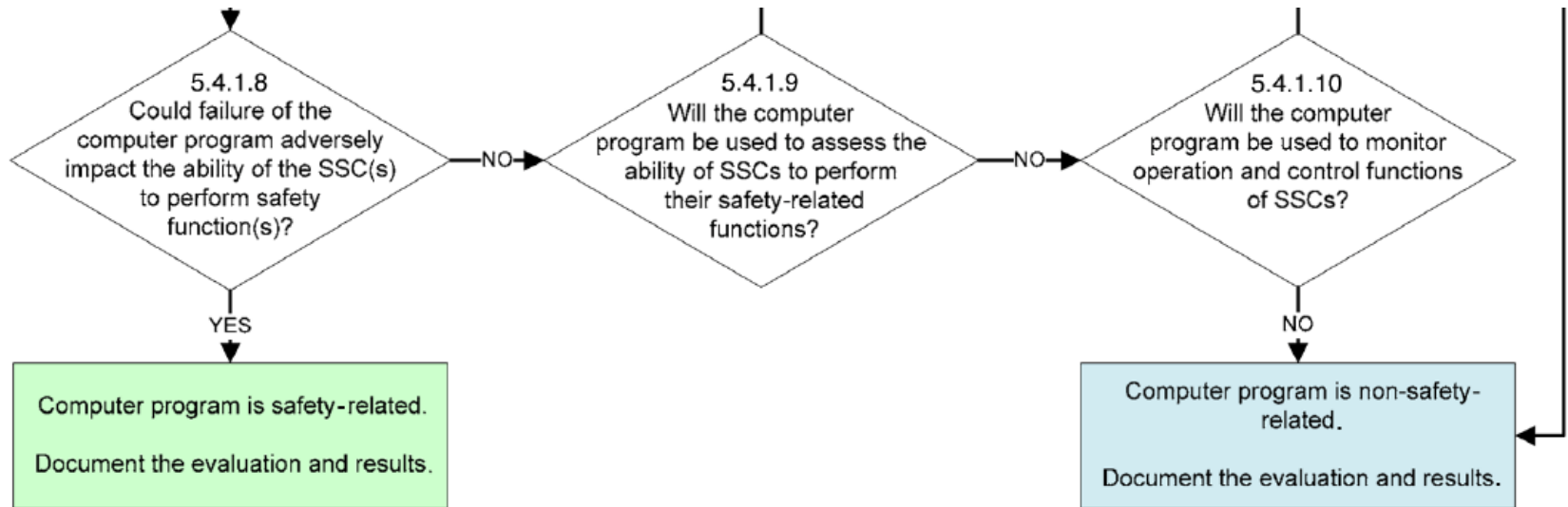
Safety Classification – FME

- 5.4.1.4
 - SSC의 design or analyze에 사용되는 Computer program이 safety function 을 수행하는 SSC의 ability or design에 영향을 미치는가?
 - 대상 타겟 고려
 - No? -> 5.4.1.3
- 5.4.1.5
 - Computer program의 결과(design, analysis 결과) 가 independently verified by other acceptable method 인가?
 - Manual review
 - 다른 대안이 되는 도구 등
 - Yes? -> non-safety related but augmented quality
- 5.4.1.6
 - Computer program 과 associate 되는 safety function 확인
- 5.4.1.7
 - Computer program 의 failure mechanism에 대해 결정
 - Computer program의 가능한 failure
 - Erroneous result, cannot produce results 등

Examples of Failure Mechanisms for 5.4.1.7

Postulated Failure	Description
Conceptual Error	Errors resulting when the computer program is applied outside its intended use or when the computer program is syntactically correct, but the programmer or designer intended it to do something else.
Arithmetic Error	Errors such as division by zero, stack over/underflow, and loss of precision resulting from incorrect programmatic calculations.
Interface Errors	Errors generated by or through incorrect interfacing of the computer program with other programs, hardware, or operating systems.

Safety Classification – FME



Safety Classification – FME

- 5.4.1.8
 - Computer program의 failure가 대상 SSC의 safety function 수행에 영향을 미치는가?
 - Yes -> Safety-related
- 5.4.1.9
 - Computer program이 SSC의 safety function 을 수행하는 능력을 평가 (assessment) 하는데 사용되는가?
 - YES -> Non-safety-related, but augmented quality
- 5.4.1.10
 - Computer program이 SSC 의 operation이나 control을 모니터하는데 사용되는가?
 - YES -> Non-safety-related, but augmented quality
 - NO -> Non-safety-related
- TR-1025243의 첫 번째 classification 방법을 적용한다면
 - Analysis 도구들 (simulator, linter, timing analyzer 등) 에 대해서 정확하게 판단할 필요성 존재

Safety Classification – Impact Categorization

- **Classification considering impact categorization은**
 - Impact 를 고려하여 classification하는 방법
- **Impact category는 4 단계로 분류**
 - High
 - Medium
 - Low
 - Other
- **High**
 - Safety function에 직접적으로 영향을 미치거나 (direct), design하는데 사용되고 SSC가 safety function 을 제대로 수행 할 것을 assure 하지만 verify가 다른 대안이 없는 경우
- **Medium**
 - Operation이나 control을 모니터하는 computer program
 - SSC의 ability를 assess 하는 computer program
- **Low, Other**
 - Non-safety-related
- High impact category에 속하는 것에 대해서만 safety-related 로 분류
- Medium impact category에 속하는 것들은 Non-safety-related지만 augmented quality로 분류

Safety Classification – Impact Categorization

Impact	Safety-Related	Augmented Quality (Non-Safety-related)/Non-Safety-Related SSCs – Significant Contributors to Plant Safety	Non-Safety-Related
High Impact (Note 1)	Software that has a direct active effect on the ability of a safety-related SSC to perform its intended safety functions.		
High Impact (Note 2)	Software used for the design of an SSC that ensures that the SSC meets its intended design basis safety function as defined in the nuclear license documents without using alternative methods to verify the results.		
Medium Impact (Note 3)		Software used to assess the ability of an SSC to meet its intended safety function.	
Medium Impact (Note 4)		Software used to monitor operation and control functions of a plant SSC.	
Low Impact			Software used to support activities that have no direct impact on nuclear operations, design, or license commitments, but may be used to monitor compliance or optimize performance.

ISL-ESRD-TR-14-04 TASK 3

Task 3 Report : Technical Basis for RG

- Task 3 : RG 개정 및 새로운 RG 개발 시 Software tool의 review 및 approval (acceptance) process 에 대해 고려할 점들
- Software Tool : Supporting or used in design, development, testing, review, analysis, or maintenance
- Future regulatory guidance 에서 고려할 내용을 11개 요소에 대해서 설명
- 필요에 따라 software tool 의 개발 및 인증 과정을 3 가지로 구분
 - Developed under 10CFR50 Appendix B QA requirements
 - Does not developed under 10CFR50 Appendix B QA requirements
 - Commercial grade item, SW dedication
 - Developed using high-quality life cycle approach of RTCA DO-330
 - Software Tool Qualification Considerations : 항공 분야의 software tool 인증 표준

Task 3 Report : Technical Basis for RG

- **2.1 Software Lifecycle Processes**
- **2.2 Software Tool Categories**
 - modeling, analysis, simulation 도구를 포함해서 software tool 의 category를 분류할 필요가 있다
- **2.3 Software and Software Tool Integrity Levels**
 - Software tool의 SIL분류는 이렇게 하는 걸 고려해야 한다 인데...
- **2.4 Software Tool Planning**
 - 수정에 대한 고려 사항 : software 개발 life cycle의 여러 plan (V&V plan, QA plan 등)시 software tool 에 대한 내용이 포함 되어야 함
 - Software life cycle planning 등에 software tool의 변화나, 버전업 등에 대해 planning 이 세워져야 함
- **2.5 Software Tool Selection and Use**
 - Safety system 개발에 Software tool 을 선택하고 사용할 때 고려해야 할 사항들
- **2.6 Software Tool Documentation**
 - Software Tool에 대해 문서화 되어 있어야 하는 사항들에 대한 고려
- **2.7 Software Tool Development, Qualification, and Dedication**
 - System 개발에 사용하기 위해 Software tool을 개발하거나, qualification 하거나 dedication 할 때 고려해야 할 사항들
- **2.8 Software Tool Quality Assurance**
 - Software tool의 qualify assurance 를 확인 할 때 고려되어야 하는 사항들
- **2.9 Software Tool Training**
- **2.10 Software Tool Configuration Management**
- **2.11 Software Tool Review, Approval, and Acceptance Criteria**

Task 3 Report : Technical Basis for RG

- **2.7 Software Tool Development, Qualification, and Dedication**
 - 17. Future RG might consider endorsing, adopting or adapting the methods of TR-1025243 for the dedication of commercial-grade design and analysis tools
 - 18. Future RG might consider adapting the TR-102348
 - 와 같이 dedication을 할 경우 고려되어야 할 사항에 대해 언급
- **2.11 Software Tool Review, Approval, and Acceptance Criteria**
 - Phase of commercial dedication
 - Tool qualification을 위해TR-1025243에서 명시하고 있는 critical characteristics에 대해 정의해야 한다
 - CASE tool, development tool의 critical characteristics 는 extensive testing 과 performance history를 통해 검증 되어야 한다
 - Dedication 과정에서 나타나는 모든 critical characteristics는 software tool의 dedication에 필수적임을 확인해야 한다
 - 등
 - Commercial dedication phase에서는 dedication 을 받아들이기 위해 고려되어야 할 사항을 언급

The END

END

FUNCTIONAL SAFETY

IEC 61508 Functional Safety

- 전자, 전기 시스템의 기능 안전을 위한 표준
 - 특정 분야에 구매 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 안전무결성 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, N₂가스를 연속적으로 감지

적외선 타입 가스감지기



CERTIFICATE

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 편집후

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

제(대표이사 켄트-진)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 프로세스를 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 플 수주를 이용하고 있다. 또한, 이들 CSP는 LDRAunit을 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 TM557011x/12x 및 RM46x MCU는 향후 고객들이 “기능 안전 애플리케이션을 간편하게 개발할 수 있도록 도와주는 포괄적인 SafeTI 설계 패키지, 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 평가란 뿐만 아니라 1인증 또는 멀티인증 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

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

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.