

COTS SW dedication

-Introduction and concept

정세진

Dependable Software Laboratory

Konkuk Univ.

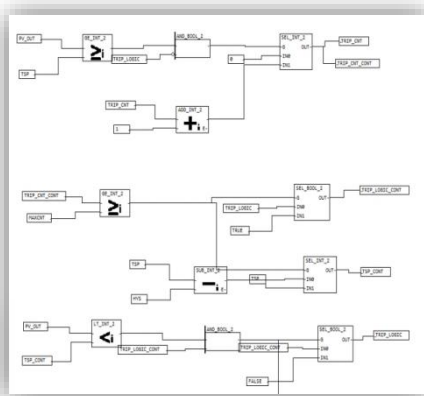
What is the COTS (Software) Dedication

- COTS is the acronym for Commercial Off-The-Shelf
- The hardware/software component/module, which is used in NPP, **should be demonstrated** safety, correctness, etc.
- COTS (Commercial Off-The-Shelf) dedication is **an effort for using COTS product** to NPP
 - COTS SW dedication : An acceptance process for demonstrating correctness and safety of commercial software (COTS) used directly or indirectly

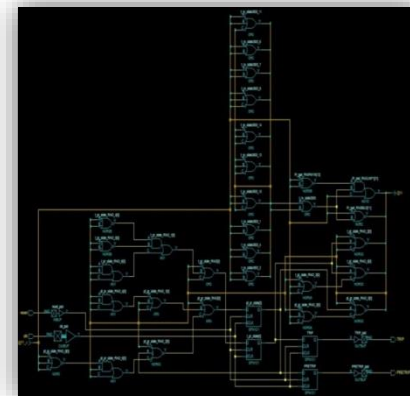
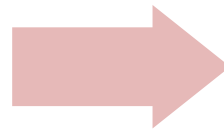
Why COTS SW dedication is related with FPGA

-Platform Change from PLC to FPGA

- **PLC**(Programmable Logic Controller) has been widely used to implement I&Cs
 - **SW development** on industrial computers (CPU & OS)
 - However, increasing maintenance cost and CCF(Common Cause Fault) problem in security
 - Request for alternative implementation platforms
- **FPGA**(Field Programmable Gate Array) is an alternative platform of PLC for I&Cs
 - Higher computation performance and stronger security
 - Diversity of system also can be provided
 - **HW development**



FBD program for **PLC**

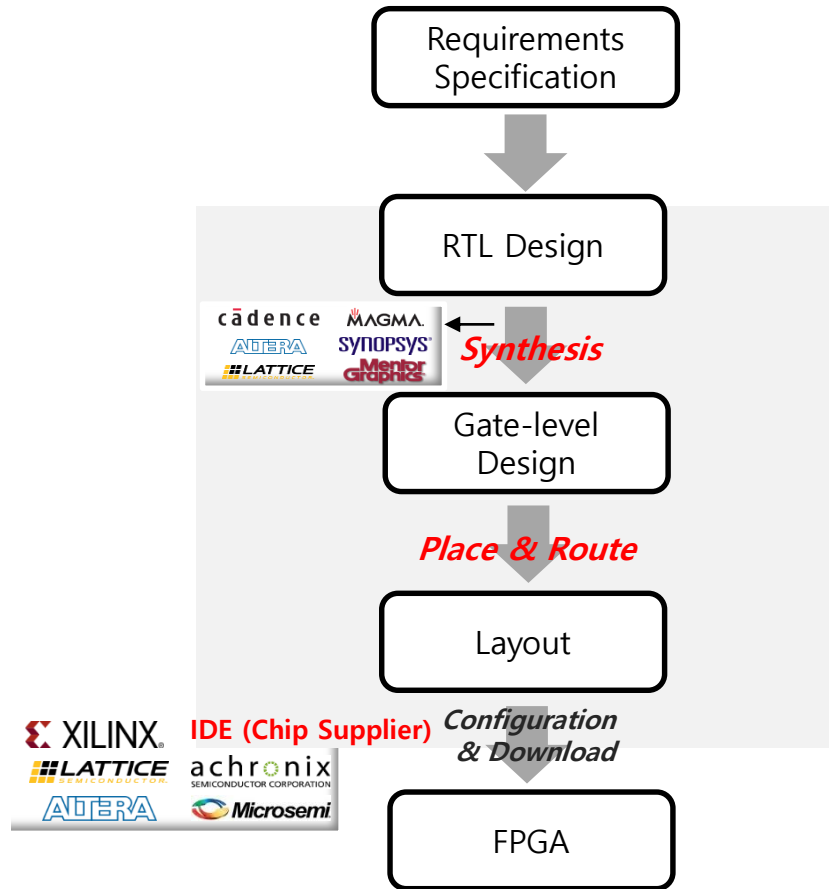


Netlist design for **FPGA**



FPGA Software Development

- Several Commercial Software is used to develop FPGA software



Software Used in FPGA Development Process

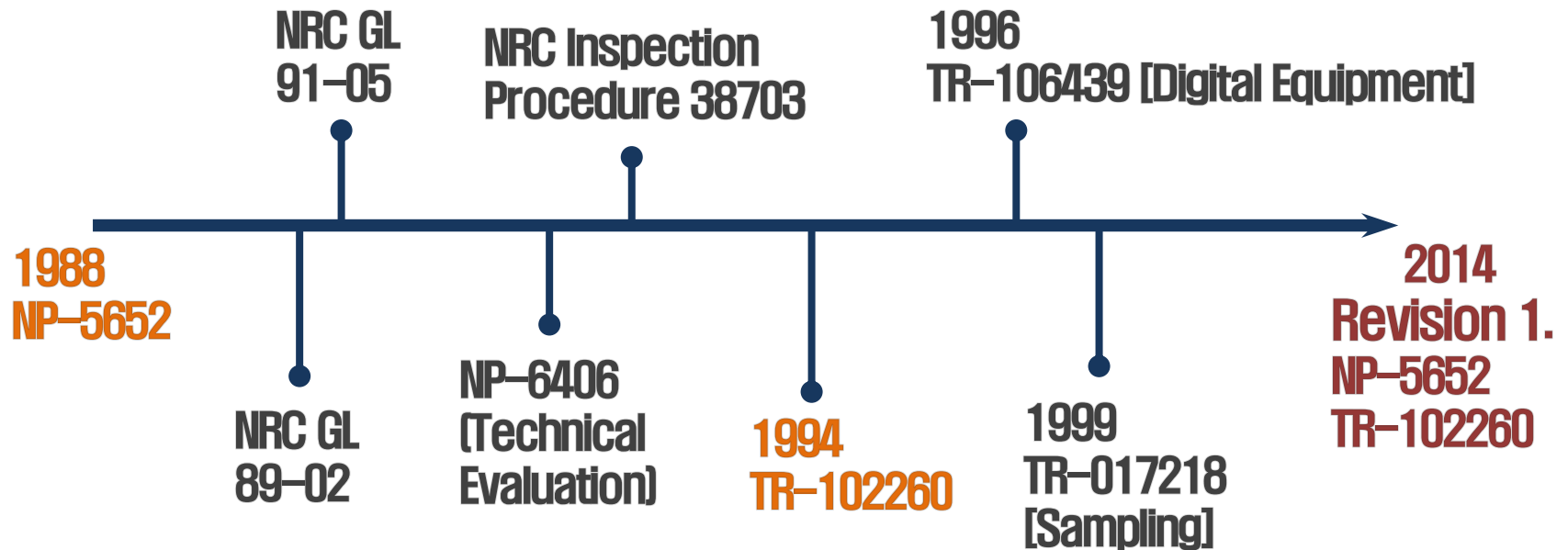
- All SW used in directly or indirectly as a safety-related application should be developed under quality assurance program **10CFR App.B** or **NQA-1**
 - If not, they should be **dedicated** by international standards
- COTS SW in FPGA development process
 - **Synthesis, Place & Route** also should be dedicated before using
- **International standards** and **guidelines** for using COTS component in NPP
 - NP-5652/TR-106439
 - Supplement guidelines for NP-5652/TR-106439
 - NUREG/CR-6421

COTS Dedication

- *"In the mid-1970s, more attention was given to commercial-grade item procurement practices in the nuclear industry due to the growing unavailability of equipment from suppliers with QA programs meeting the requirements of 10CFR50, Appendix B"*
- Some suppliers **discontinued support** of their nuclear QA programs
- **10CFR50 Appendix B** does not specifically address the acceptance of CGI for use in safety-related applications
 - QA program, Design Control, Document Control, Test, Corrective action, QA records, etc.
- In the later, 1977, 1979, the revision of 10CFR21 required a CGI dedication and 1988 the first version of NP-5652 is proposed
- Code of Federal Regulations

Overview of History about COTS Dedication

- Overview of history about COTS dedication standards by KEPCO
 - A lot of standards are existed also exception in figure

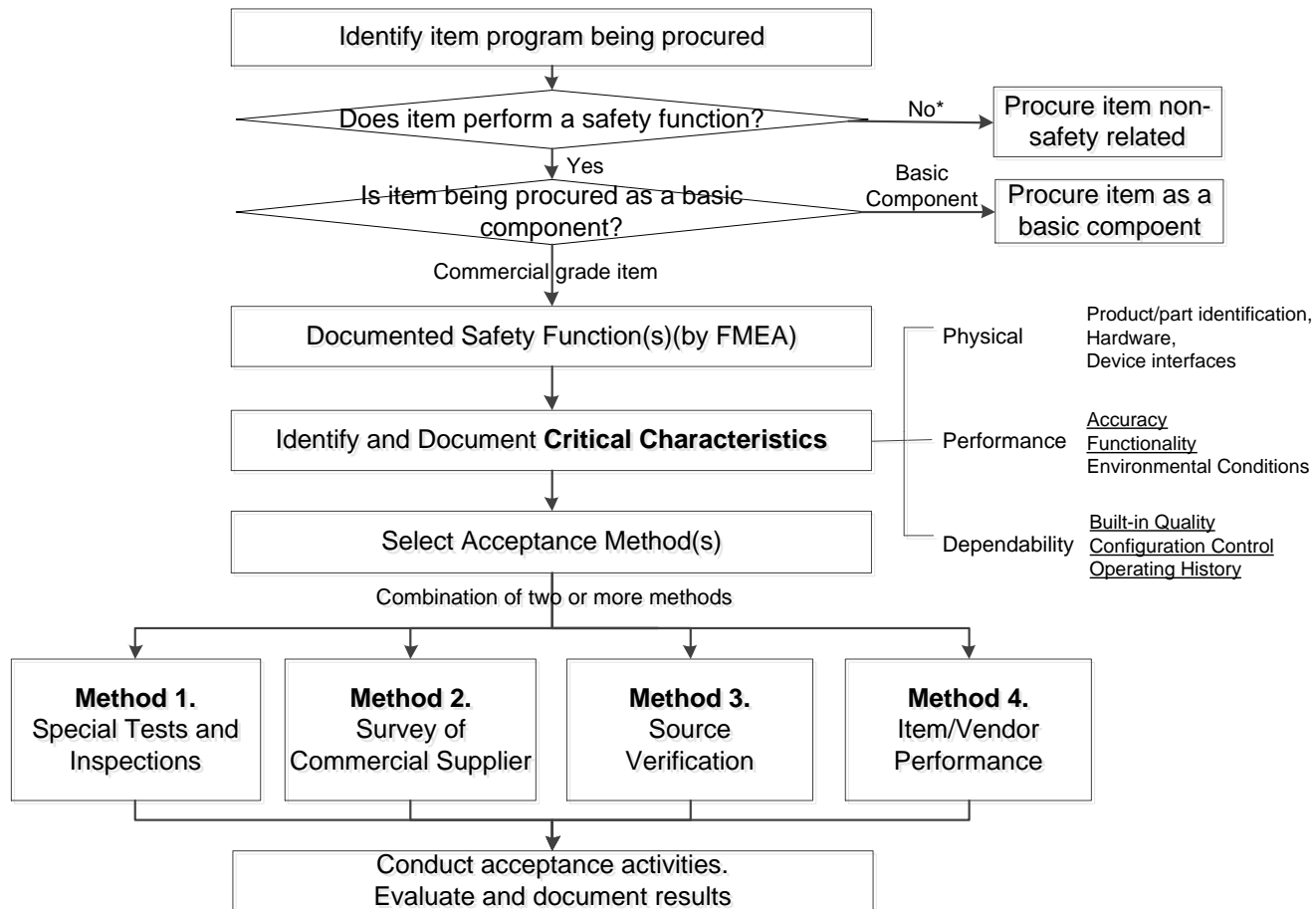


NP-5652/TR-106439

- NP-5652 is the *“Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications”*
- NP-5652 suggests applicable acceptance process of **commercial-grade items** for use in safety-related applications
- In Korea accept NP-5652/TR-106439 to dedicate of CGI by *“KINS/RG-17.12 안 전성관련품목 대체사용을 위한 일반규격품의 품질검증”*
- TR-106439 is *“Guidelines on Evaluation and Acceptance of Commercial Grade **Digital Equipment** for Nuclear Safety Applications”*, 1996
 - TR-106439 suggests dedication guidelines for software based digital equipment
 - At the time, a software based digital equipment is PLC

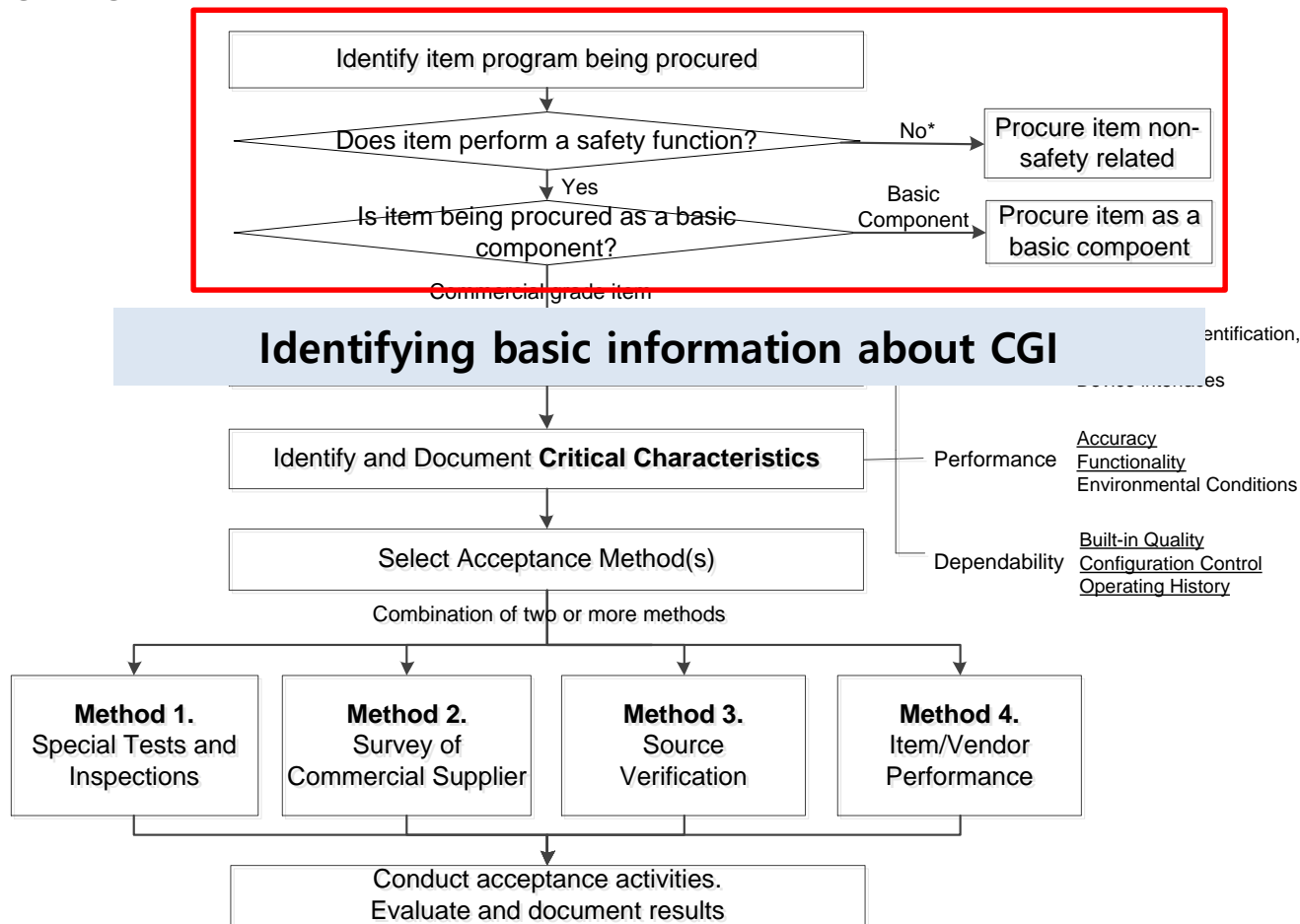
NP-5652/TR-106439

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



NP-5652/TR-106439

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

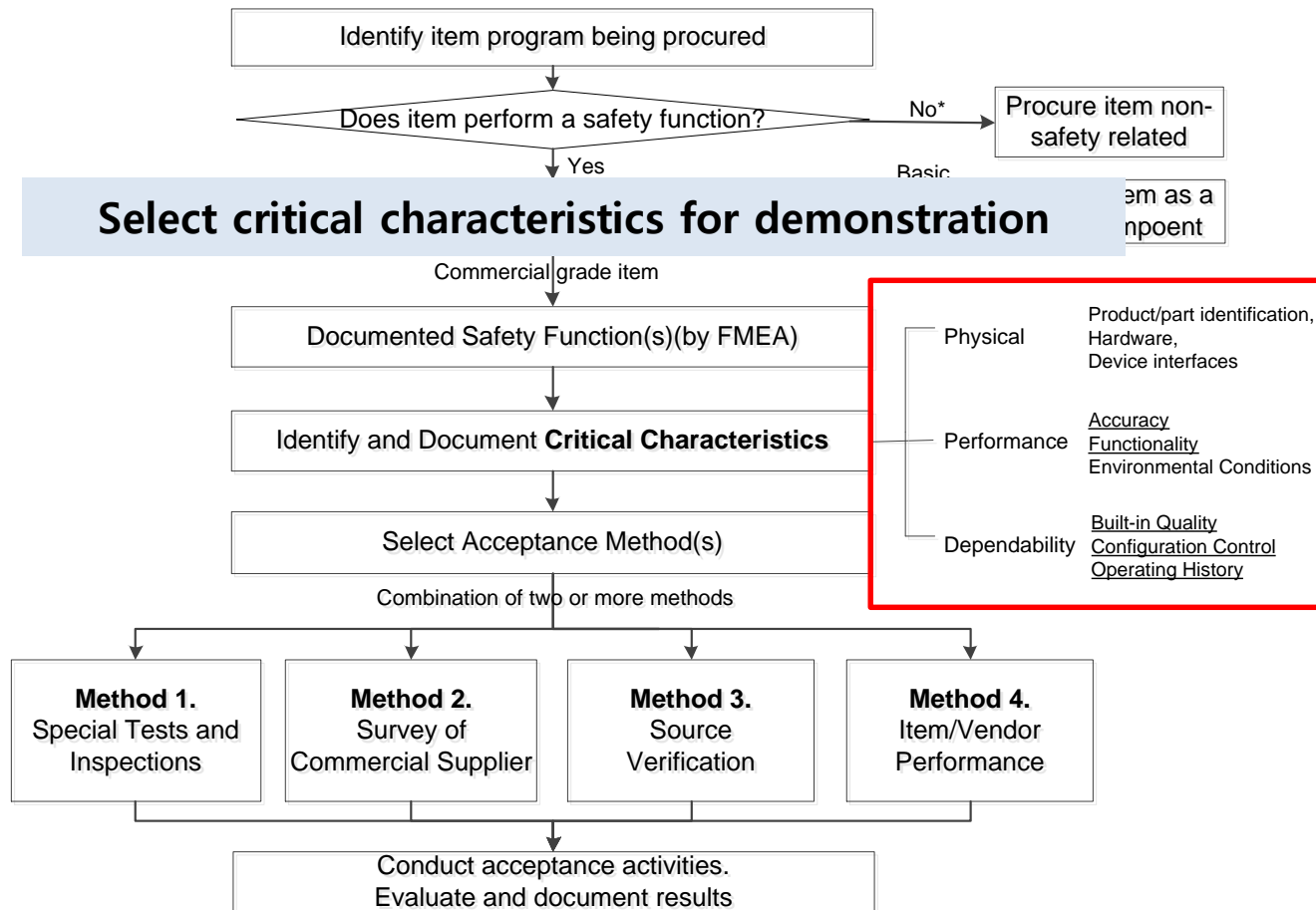


Identifying basic information about CGI

- **Identifying basic information about CGI is the process of selecting which CGI is dedicated by the process**
 - In this step, identifying whether item performing safety function
 - If the item does not perform safety function, the item can be procured non-safety related
 - If the item as a basic component, it is procured without dedication
- **In NP-5652, dedication process can be applied that the item is not a basic component and performing safety function**
- **Safety function : the function to prevent failure of system, to manage the risk of system**
 - Ex>The function which performs to decrease the temperature, When the temperature of plant is too high

NP-5652/TR-106439

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



Select Critical Characteristics for Demonstration

- **Critical characteristics are**

Critical characteristics are those important design, material, and performance characteristics of a commercial grade item that, once verified, will provide reasonable assurance that the item will perform its intended safety function(s). [4]

- **It consists of 3 kinds of characteristics**

- Physical
- Performance
- Dependability

- **Physical characteristics concerns about weight, height, size of item, hardware**

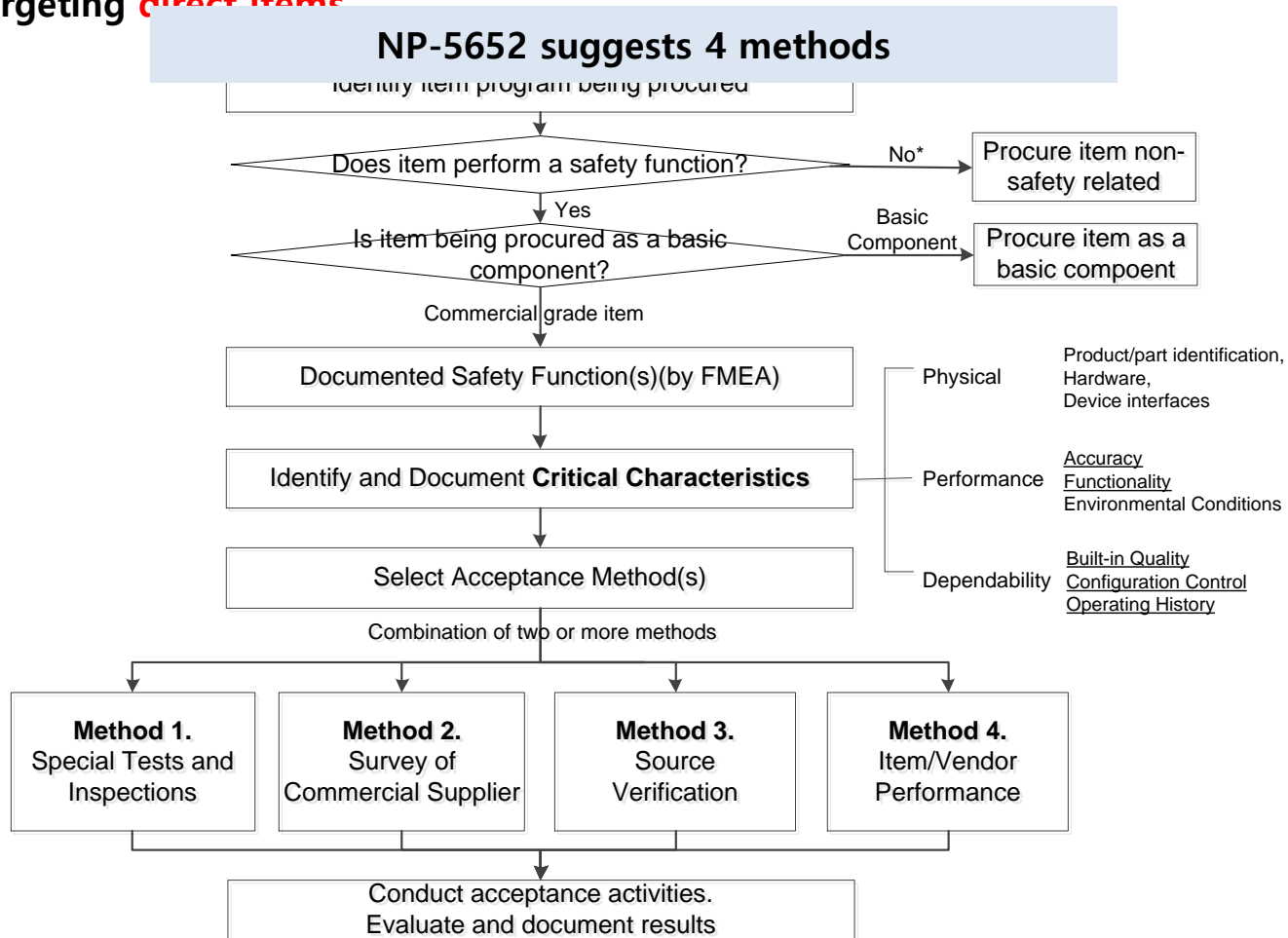
- **Performance characteristics are accuracy, functionality, environmental condition, etc**

- **Dependability characteristics has added by TR-106439**

- It contains built-in quality, operating history, configuration control

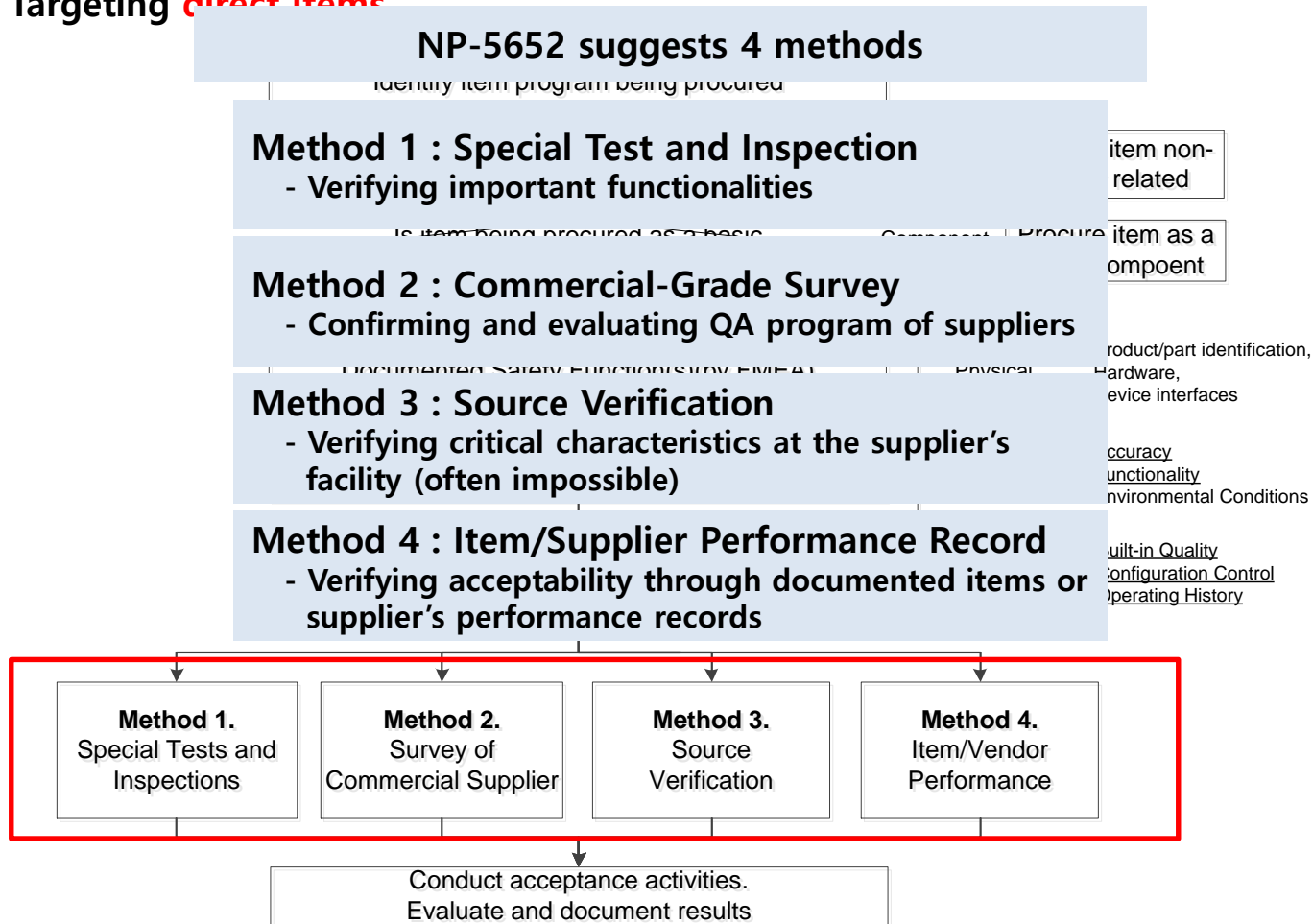
NP-5652/TR-106439

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



NP-5652/TR-106439

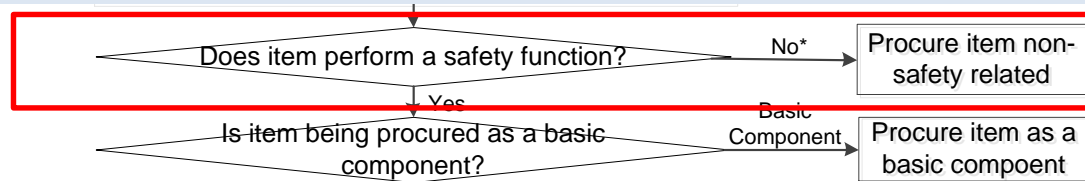
- The process overview of NP-5652
 - Performing combination of 4 methods to dedicate
 - Targeting **direct items**



NP-5652/TR-106439

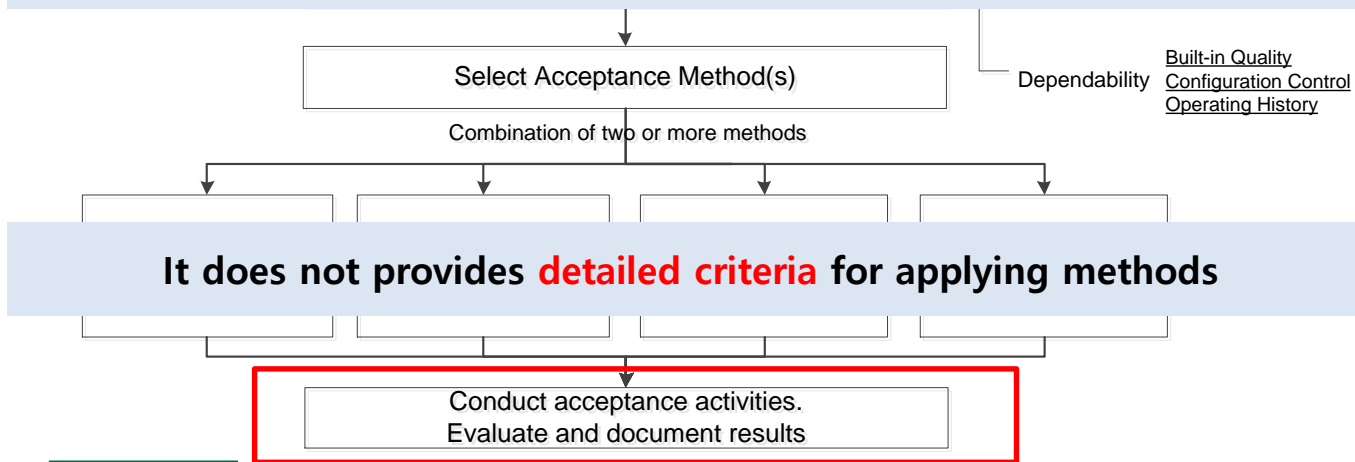
- The process overview of NP-5652
 - Performing combination of 4 methods to dedicate
 - Targeting **direct items**

It is not applicable for applying **indirect COTS SW**



If suppose

- **performance** and **dependability** characteristics are applicable for indirect COTS SW
- **Method 1, 2 and 4** are selected for characteristics of indirect COTS SW

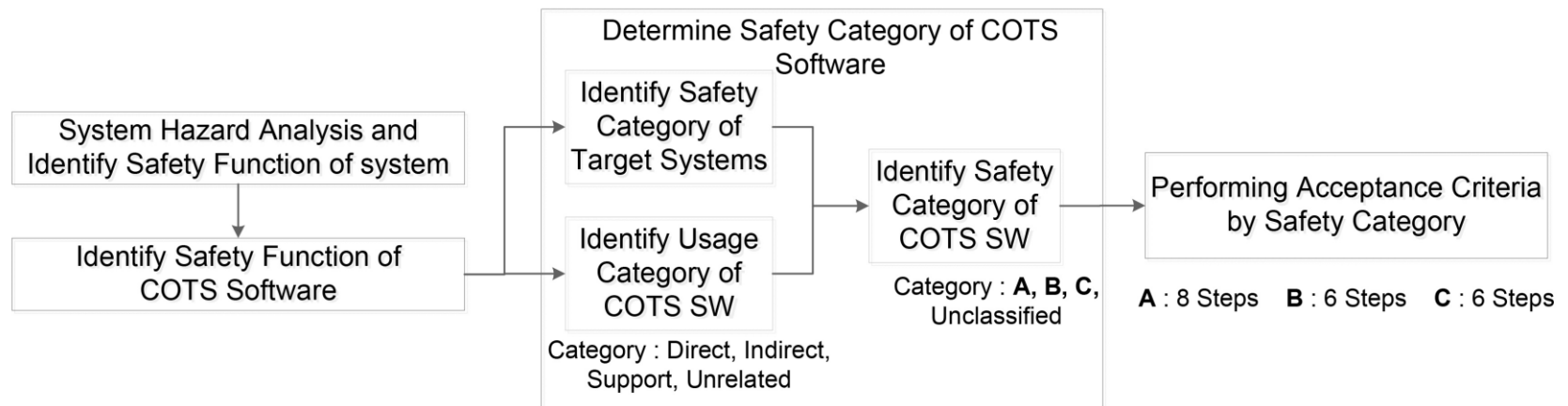


NUREG/CR-6421

- NUREG/CR-6421 is *“A Proposed Acceptance Process for Commercial Off-The-Shelf (COTS) Software in Reactor Applications”*
- It also suggests acceptance **process for COTS SW dedication**
 - It is based on several standards about software quality assurance
- Unlike NP-5652, the focus of NUREG/CR-6421 is software
- It provides detailed criteria using standard about **SW** quality rather than NP-5652
- However, it is not an international standard,
 - It is just guidelines for NRC Constructors

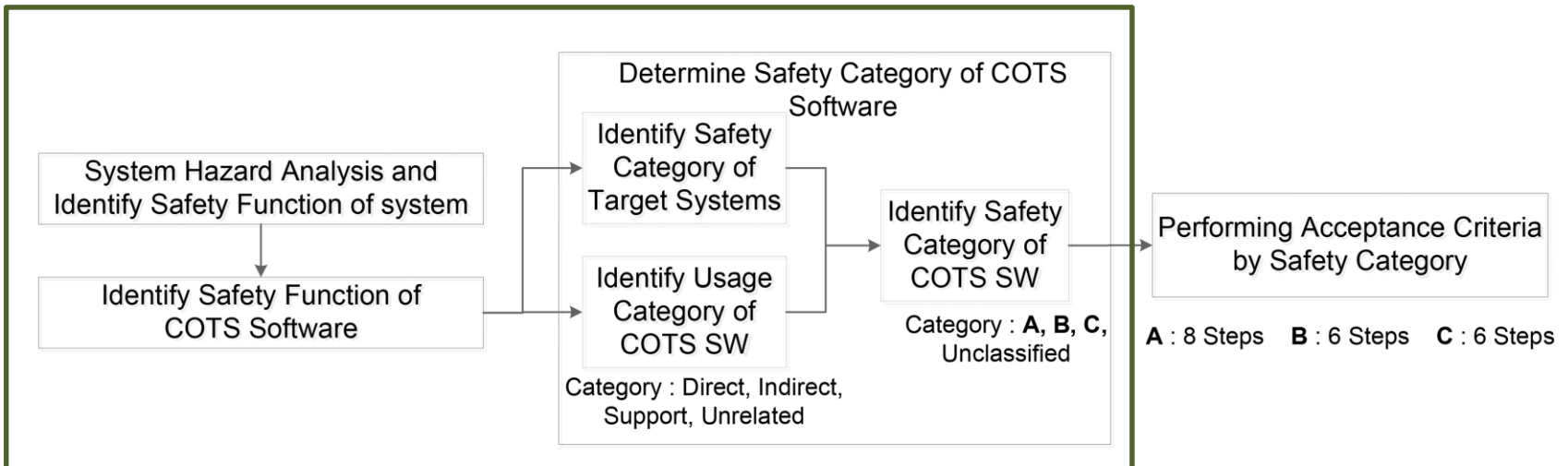
NUREG/CR-6421 process overview

- 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



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

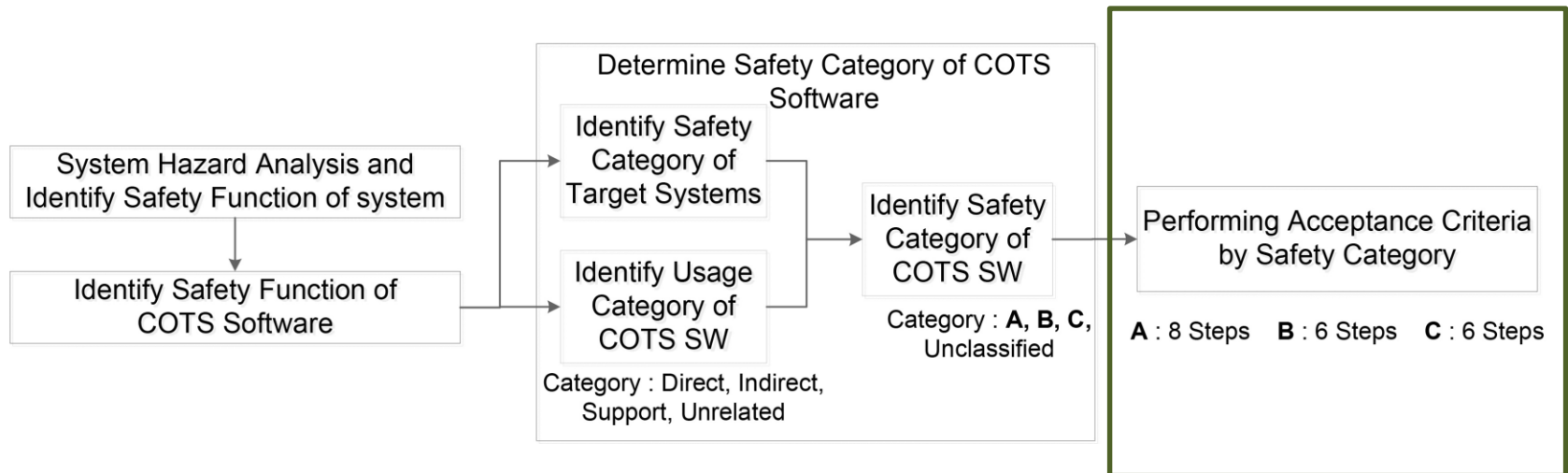


Preliminary Phase of Acceptance Criteria

- **Preliminary phase of acceptance criteria consists of 3 steps**
 - Identify safety function of target system by hazard analysis
 - Identify safety function of COTS SW
 - Determine safety category of COTS SW
- **Safety function of target system and safety function of COTS SW is used to determine safety category of COTS SW**

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



Determine Safety Category of Target COTS SW

- This step is able to divide 3 steps
 - Identify safety category of target systems
 - Identify usage category of COTS SW
 - Identify safety category of COTS SW

- Safety category
 - It is categories which is divided by important to safety of system
 - IEC 61226 proposes the safety category **A**, **B**, **C** and **Unclassified**
 - The safety category is used to determine safety category of COTS SW

Table 1. Safety Categories

IEC 1226 Category	Example Systems	RG 1.97 Equivalent Category
A	Reactor Protection System (RPS) Engineered Safety Features Actuation System (ESFAS) Instrumentation essential for operator action	A,B A,B A,B,C,D
B	Reactor automatic control system Control room data processing system Fire suppression system Refueling system interlocks and circuits	E
C	Alarms, annunciators Radwaste and area monitoring Access control system Emergency communications system	B,C,D,E C,E

Determine Safety Category of Target COTS SW

- Identify usage category of COTS SW
 - Usage category is determined by the usage of software
 - It consists of **Direct**, **Indirect**, **Support** and **Unrelated**
 - The usage category is used to determine safety category of COTS SW

Table 2. COTS Usage Categories

Usage Category	Description	Equivalent IEC 1226
Direct	Directly used in an A, B, or C application.	A, B, or C
Indirect	Directly produces executable modules that are used in A, B, or C applications (software tools such as compilers, linkers, automatic configuration managers, or the like). Produces A modules Produces B modules Produces C modules	A or B ⁵ B or C ⁶ unclassified
Support	CASE systems, or other support systems that indirectly assist in the production of A, B, or C applications, or software that runs as an independent background surveillance system of A, B, or C applications.	unclassified
Unrelated	Software that has no impact on A, B, or C applications.	unclassified

Identify safety category of COTS SW

- Safety category of COTS SW is determined by using safety category of system and usage category of SW
- **Direct**
 - The COTS safety category is determined by the IEC 61226
- **Indirect**
 - If the output of the COTS SW is able to verify other methods (e.g. testing, simulation), the safety category of COTS SW is determined one step lower category
- **Support & Unrelated**
 - Support and Unrelated categories are classified Unclassified category

Detailed Acceptance Criteria

- **Applying acceptance criteria according to the safety category of COTS SW**
 - A category consists of 8 criteria
 - B and C category consists of 6 criteria
 - Unclassified is not the target of dedication
- **The level of criteria is different each other**
 - Criteria of A category has the most strict contents of quality of SW
 - Several standards about quality and V&V, etc is used in this step

An Acceptance Criteria of the Category A

Table 5. Category A COTS Acceptance Criteria

A5	The COTS product shall have been developed under a rigorous Software Quality Assurance Plan as defined by IEEE 730.1, ISO 9000-3, or IEC 880. This shall include full V&V. See Table A-3 for detailed SQA criteria. See Table A-5 for detailed V&V criteria. See Table A-12 for minimum required V&V tasks.
A6	Documentation shall be available for review that demonstrates both Criterion A5 and that good software engineering practices were used, as detailed in Table A-7. Evidence shall be available that the minimum required reviews of Table A-8 were conducted.
A7	It shall be demonstrated that the COTS product meets the requirements identified in Criterion 2 (Table 4).
A8	It shall be demonstrated that the COTS product does not violate system safety requirements or constraints.
A9	The interfaces between the COTS product and other systems or software shall be identified, clearly defined, and under configuration management.
A10	The COTS product shall have significant (greater than 1 year) operating time, ⁸ with severe-error-free operating experience. At least two independent operating locations shall have used a product of identical version, release, and operating platform encompassing the same or nearly the same usage as the proposed usage. Any adverse reports, regardless of operating location, shall be considered. The configuration of the products in the experience data base shall closely match that of the proposed COTS product. ⁹
A11	All errors, severe or otherwise, shall be reported to and analyzed by the COTS supplier. Procedures and incentives shall be in place to ensure a high level of demonstrated compliance, or the COTS supplier shall demonstrate with statistical certainty ¹⁰ that the error reporting system achieves this compliance. An error tracking, documentation, and resolution procedure shall document each error from report to resolution.
A12	Additional validation and testing shall be performed if needed to compensate for a small amount of missing documentation or alterations in configuration.

An Acceptance Criteria of the Category A

- Category A QA criteria example

Table A-3. SQA Criteria

1	Does the SQA plan cover the minimum required subjects in the required format?	Format and subject matter is standard-dependent, but most standards specify similar approaches See IEEE 730.1
2	Does the plan describe responsibilities, authority, and relations between SQA units and software development units?	IEEE 730.1
3	Is minimum documentation available?	See Table A-7 for required documentation. See Table A-10 for optional documentation.
4	Were the minimum SQA reviews and audits performed?	See Table A-8 for minimum required reviews and audits
5	Are standards, practices, conventions, and metrics that were used, described?	See Table A-11 for suggested areas of standardization
6	Were procedures for problem reporting, tracking, and resolving described? Problems documented & not forgotten Problem reports validated Feedback to developer & user Data collected for metrics & SQA	IEEE 730.1 IEEE P730.2 IEEE P730.2 IEEE P730.2 IEEE P730.2
7	Were configuration management practices followed?	See Table A-4
8	Were V&V tasks performed?	See Table A-5
9	Did other software suppliers contribute to the product?	See Table A-9. "The supplier is responsible for the validation of subcontracted work." ISO 9000-3
10	What records were generated, maintained, and retained?	IEEE 730.1
11	What methods or procedures were used to identify, assess, monitor, and control risk during development of the COTS product?	IEEE 730.1

An Acceptance Criteria of the Category A

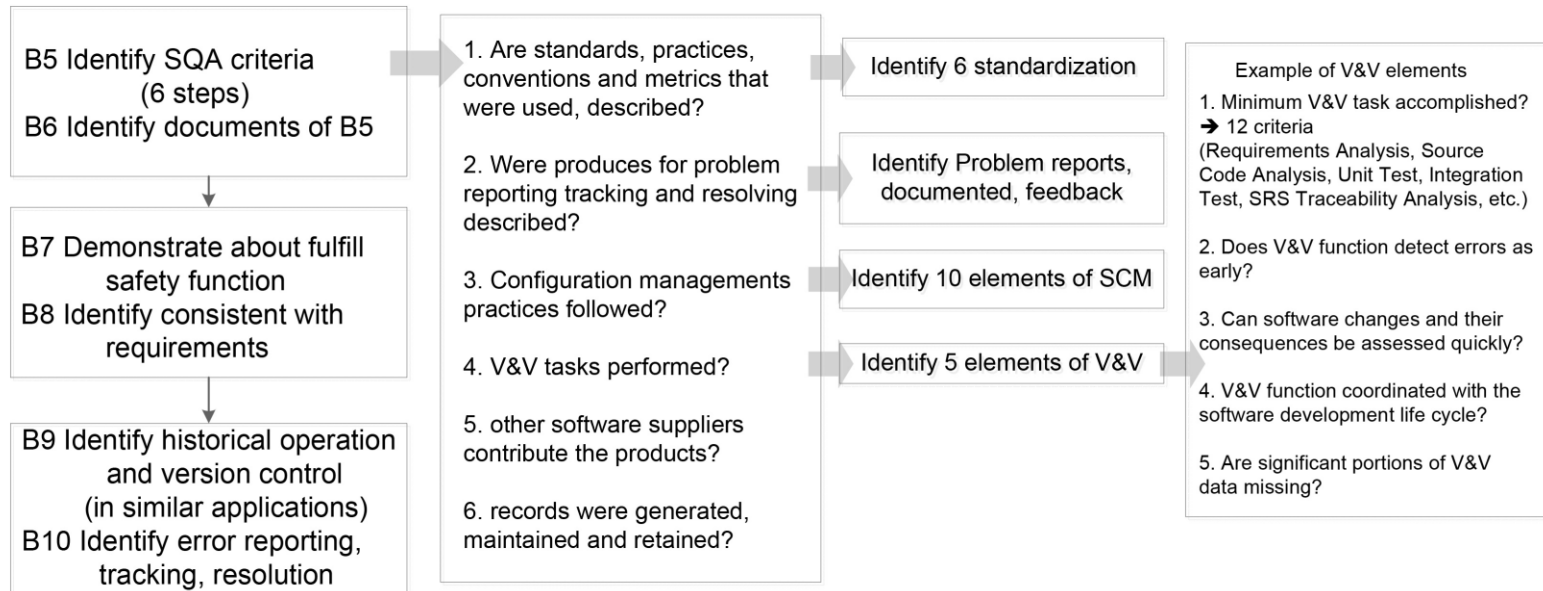
- V&V criteria example

Table A-12. Minimum V&V Tasks

1	SVVP	IEEE 730.1 and IEEE 1012
2	Requirements (e.g., SRS) Analysis Existence Clarity Consistency Completeness All functions included Environment specified Inputs & outputs specified Standards used specified Correctness Feasibility Testability	IEEE 1012 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4
3	SRS Traceability Analysis	IEEE 1012 & ANSI/ANS-10.4
4	Interface Requirements Analysis	IEEE 1012 & ANSI/ANS-10.4
5	Test Plan Generation	IEEE 1012 & ANSI/ANS-10.4
6	Acceptance Test Plan Generation	IEEE 1012
7	Design Analysis Completeness Correctness Consistency Clearness Feasibility	IEEE 1012 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4
8	Design Traceability Analysis	IEEE 1012 & ANSI/ANS-10.4
9	Interface Design Analysis	IEEE 1012
10	Unit Test Plan Generation	IEEE 1012 & ANSI/ANS-10.4
11	Integration Test Plan Generation	IEEE 1012 & ANSI/ANS-10.4
12	Test Designs Code test drivers	IEEE 1012 ANSI/ANS-10.4
13	Source Code Analysis Conformance to standards Adequate comments Clear and understandable Consistent with design Strong typing Error-checking	IEEE 1012 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4 ANSI/ANS-10.4
14	Source Code Traceability	IEEE 1012
15	Interface Code Analysis Well-controlled software interfaces	IEEE 1012 ANSI/ANS-10.4
16	Documentation Evaluation	IEEE 1012
17	Test Procedure Generation Unit Test Integration Test System Test Acceptance Test	IEEE 1012 & ANSI/ANS-10.4

An Acceptance Criteria of the Category B

- It also contains contents about SQA, V&V, CM



COTS SW Dedication : Comparison

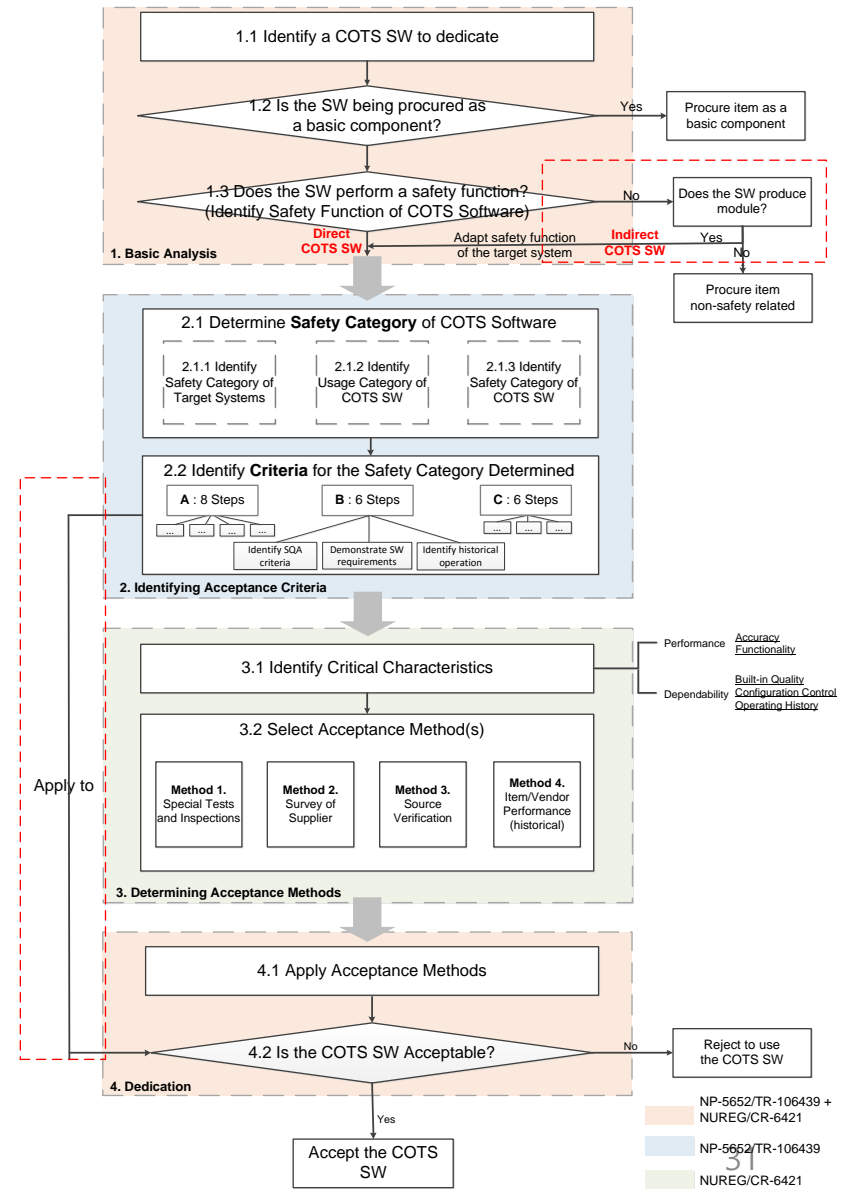
- Two standards have difference and similar points to dedicate
 - NP-5652/TR-106439 are not targeted to indirect COTS SW and detailed criteria is needed to apply

	NP-5652/TR-106439	NUREG/CR-6421
Target	Commercial-grade item (COTS HW + COTS SW)	COTS SW
Usage of dedication items	Direct	Direct/Indirect
Grading/Categorization	X	O
Use of before dedication records available	O (lately 3 years)	X
Detailedness of dedication criteria	Abstract	Detailed
Identification of SW QA plans	O	O
Review of Operating History	O	O

An Integrated Dedication Process for COTS SW

- Proposed integrated dedication process for COTS SW
 - Consisting of **four parts**

- Basic Analysis**
 - Identifying an item(SW)
 - Identifying as a basic component
 - Identifying safety function
- Identifying Acceptance Criteria**
 - Determine safety category of COTS SW
 - Identifying criteria for each category
- Determining Acceptance Methods**
 - Identifying critical characteristics
 - Selecting acceptance methods
- Dedication**
 - Applying acceptance methods (applying criteria)
 - Determine acceptability of COTS SW



An Integrated Dedication Process for COTS SW

- Proposed integrated dedication process for COTS SW
 - Consisting of **four parts**

1. Basic Analysis

- Identifying an item(SW)
- Identifying as a basic component
- Identifying safety function

2. Identifying Acceptance Criteria

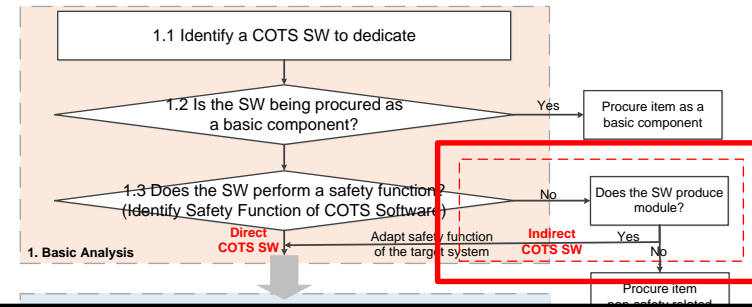
- Determine safety category of COTS SW
- Identifying criteria for each category

3. Determining Acceptance Methods

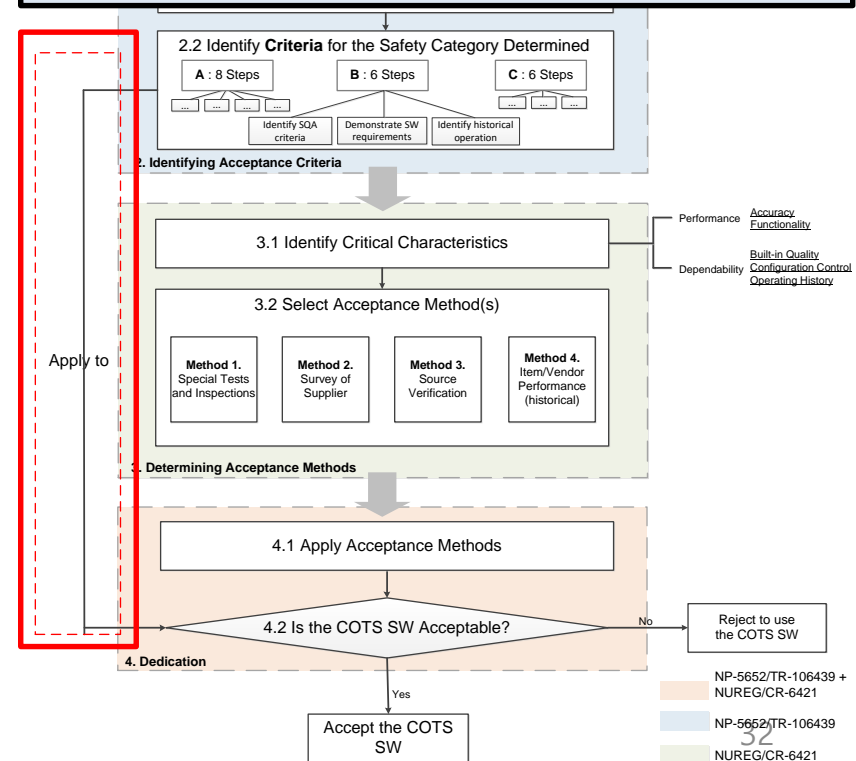
- Identifying critical characteristics
- Selecting acceptance methods

4. Dedication

- Applying acceptance methods (applying criteria)
- Determine acceptability of COTS SW



Our additional idea for dedicating indirect COTS SW

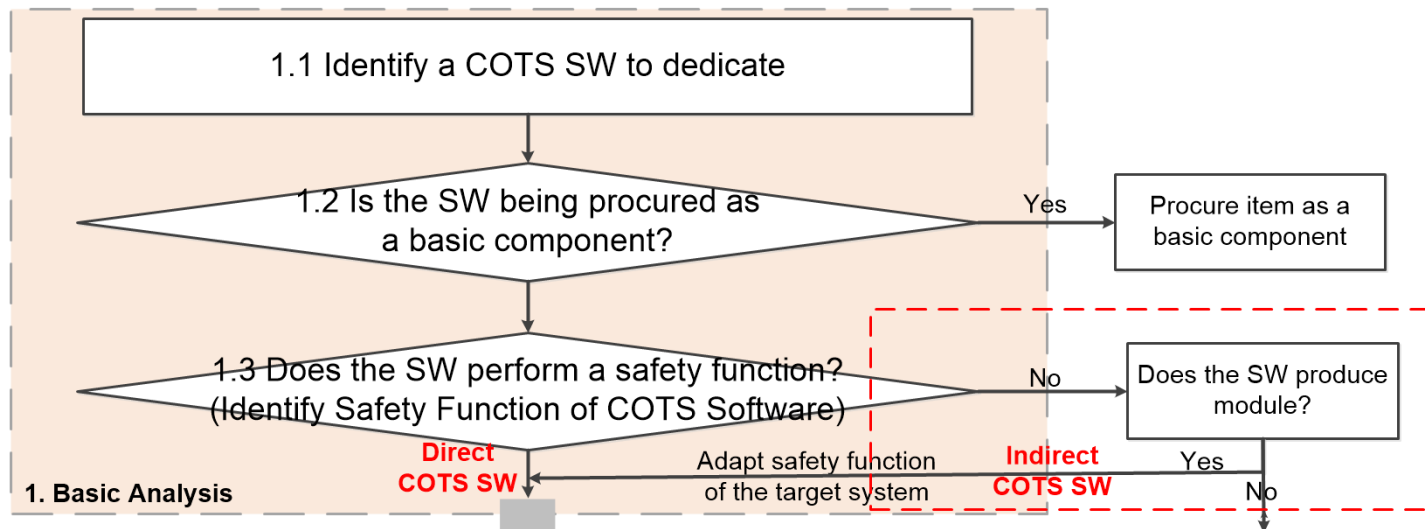


NP-5652/TR-106439 +
NUREG/CR-6421
NP-5652/TR-106439
NUREG/CR-6421
Our additional idea

Parts 1 : Basic Analysis

1. Basic Analysis

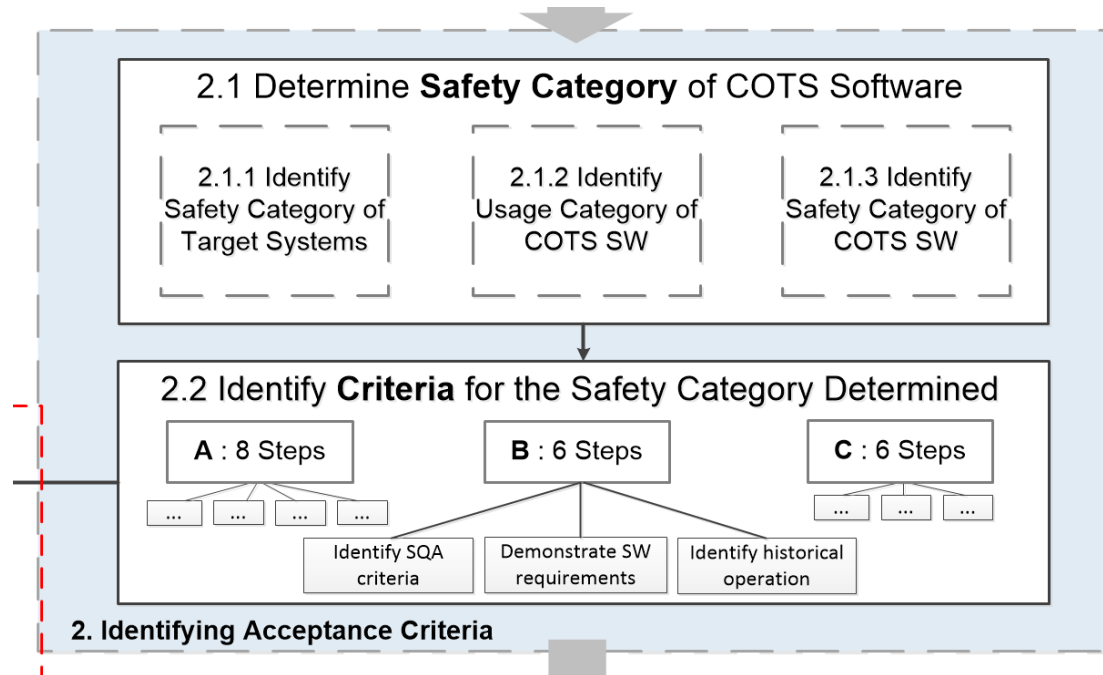
- Identifying an item(SW)
- Identifying as a basic component
- Identifying safety function



Parts 2 : Identifying Acceptance Criteria

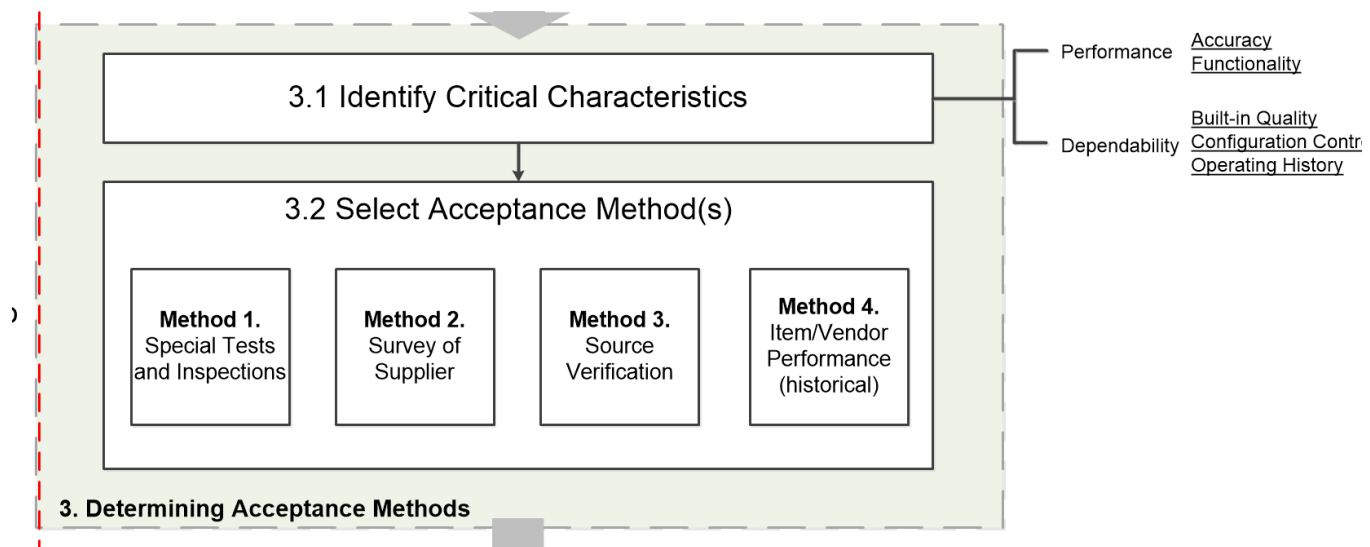
2. Identifying Acceptance Criteria

- Determine safety category of COTS SW
- Identifying criteria for each category



Parts 3 : Determining Acceptance Methods

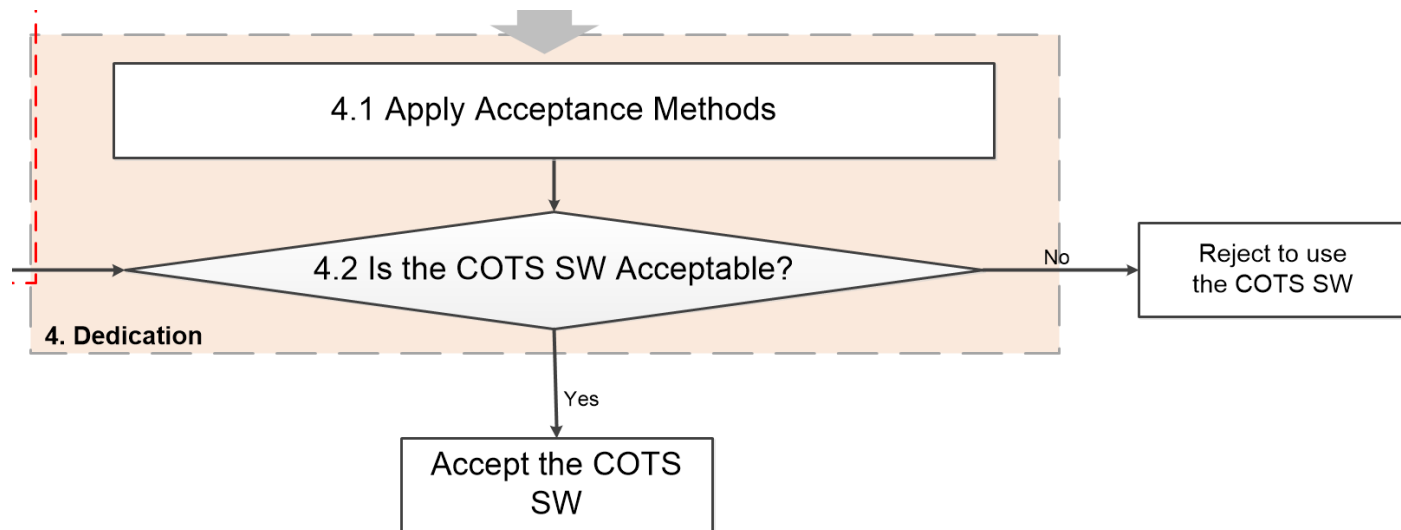
- 3. Determining Acceptance Methods**
- Identifying critical characteristics
 - Selecting acceptance methods



Parts 4 : Dedication

4. Dedication

- Applying acceptance methods (applying criteria)
- Determine acceptability of COTS SW



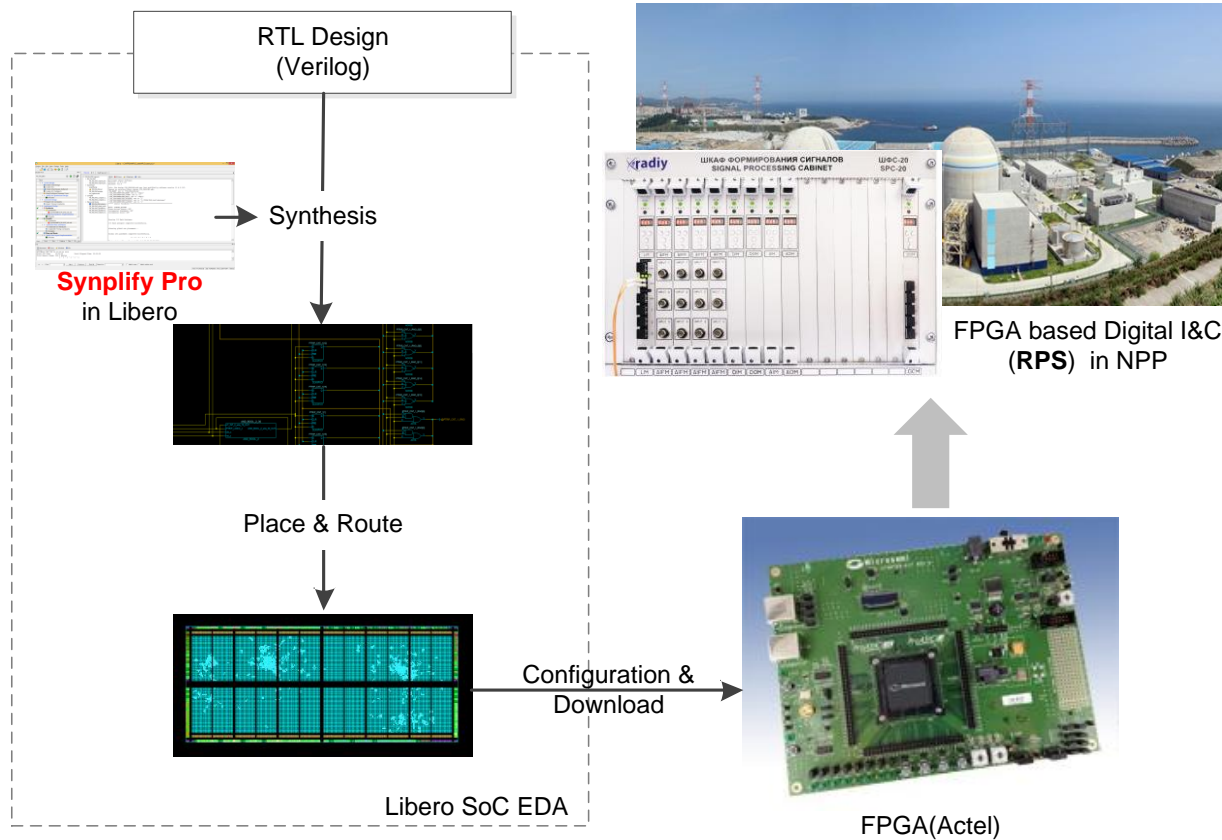
Parts 4 : Dedication

- Applying criteria for determining acceptability of COTS SW

Critical Characteristics for indirect SW	Acceptance Methods	The Criteria by Safety Category		
		A	B	C
Performance	Method 1	A7, A8, A9, A12	B7, B8	C7, C8
Dependability	Method 2	A5, A6	B5, B6	C5, C6
Performance	Method 3	A7, A8, A9	B7, B8	C7, C8
Dependability	Method 4	A10, A11	B9, B10	C9, C10

Case Study (Example)

- Perform a case study with an indirect COTS SW (logic synthesis tool)
 - Which are widely used to develop a new FPGA-based digital I&C in Korea
 - 'Synopsys Synplify Pro' used embedded in the 'Actel Libero SoC'



Case Study : Basic Analysis and Identifying Acceptance Criteria

- **Basic Analysis**
 - Identified target SW is synthesis tool 'Synposys Synplify Pro'
 - It is **not a basic component**
 - It does not perform a safety function
 - It **produces a module** which will be a performing safety function
 - Regarding its safety function is RPS
- **Identifying Acceptance Criteria**
 - The safety category of 'Synposys Synplify Pro' is determined '**B**' by three steps
 - The acceptance criteria for the category '**B**' software consists **6 steps**
 - Contains identifying SQA, requirements, history, etc.

Case Study : Determining Acceptance Methods

- **Determining Acceptance Methods**
 - Critical characteristics of 'Synopsys Synplify Pro' is 'Performance' and 'Dependability'
 - Selected acceptance methods are 1,2 and 4

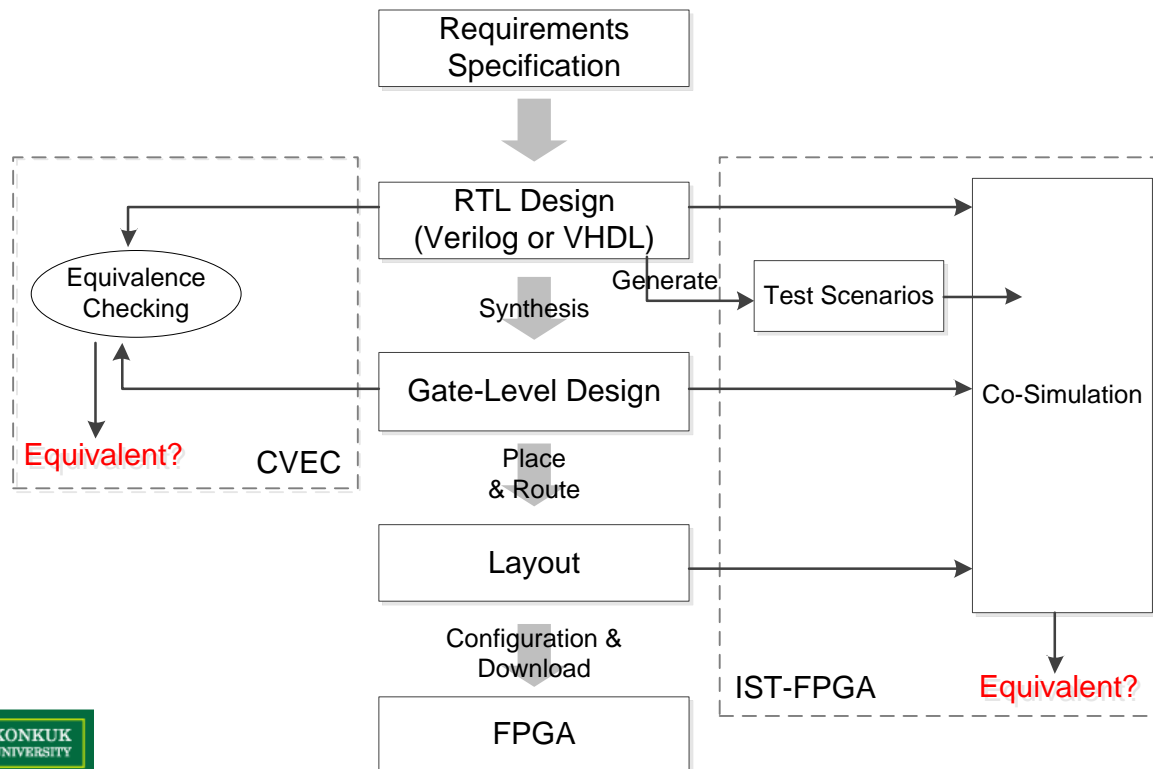
Critical Characteristics	Attributes	Definition for 'Synopsys Synplify Pro'	Selected Methods
Performance	Accuracy	The software should synthesize RTL design to gate-level design correctly	Method1
	Functionality	The software should produce behaviorally-equivalent outputs from inputs as a compiler	
Dependability	Built-in Quality	The software should have appropriate quality	Method2
	Configuration Control	Supplier should manage the software configuration well	
	Operating History	The software should maintain operating history about having been operated successfully	Method 4

Case Study : Dedication

- **Dedication**
 - Applying method 1, 2 and 4 by using criteria of 'B' category
- **Method 1. Special Tests and Inspections**
 - Compiler verification techniques is not applicable to commercial synthesis software
 - Source code is not made public by vendors
 - We use indirect verification technique for special tests
 - CVEC (Customized VIS-based Equivalence Checking)
 - IST-FPGA(Integrated Software Testing framework for FPGA)

Dedication : Method 1

- CVEC
 - Equivalence checking with RTL design and gate-level design
- IST-FPGA
 - Simulation based testing
- These verifications successfully demonstrated that the input and output into/from 'Synplify pro' are **behaviorally-equivalent**.



Dedication : Method 2 and 4

- **We try to survey the suppliers, 'Synopsys' and 'Microsemi' for collecting information applying method 2**
 - Found only the record of certification about ISO9001 and AS9100C
- **We found records that 'Synopsys Synplify Pro' was used to develop Kozloduy NPP applying method 4**
 - It used for an alternative platform of ESFAS
 - Finding history of update release also
 - Do not find error/bug tracking reports

Case Study : Dedication

- Determining acceptability of 'Synplify Pro' by using criteria and results of applying methods

Critical Characteristics	Attributes	Criteria	Contents	Match information	Methods	
Dependability	Built-in Quality	B5	The COTS SW should be developed under a appropriate QA plan	N/A (But it can be provided by ISO9001 and AS9100C)	2	
		B5-1	Are standards, practices, conventions, and metrics that were used, suggested described?			
		B5-2	Problem reporting, tracking and resolving described?			
	Configuration Control					Configuration Managements practices followed?
		B5-3.1	Does the plan describe responsibilities, authority, and relations between CM and development?			
		B5-3.2	At least one configuration control board is required			
		B5-3.3	Does the configuration management operation provide the following required functions?			
		B5-3.4	CM is founded upon the establishment of "configuration baselines" for each version of each product?			
		B5-3.5	Is the level of authority required for change described?			
		B5-3.6	Dose status accounting include			
		B5-3.7	Software products under control for each supplier?			
	B5-3.8	All Records to be maintained and identified?				
	Built-in Quality					V&V tasks performed
		B5-4.1	25 kinds of V&V Tasks are performed?			
		B5-4.2	Do V&V function detect errors early as possible?			
		B5-4.3	Can software change be assessed quickly?			
		B5-4.4	Are V&V function coordinated with the development?			
		B5-5	Well-managed other supplier? If exists			
B5-6	Were records of product generate and maintained?					
Performance	Accuracy	B7	It shall be demonstrated that the COTS SW will fulfill its safety function	Available by CVEC and IST-FPGA	1	
	Functionality	B8	The COTS SW should be consistent with system requirements			
Dependability	Historical operation	B9	The COTS SW should have operated satisfactorily in similar applications.	historical usage information is available	4	
			Configuration management and update should provide traceability	release notes exists		
		B10	Error reporting, tracking and resolution should be consistent and correctly attributable to version and release is well managed	N/A		
			The version and release have no major unresolved problems and bug list should be available to COTS purchaser as a support option	N/A		

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
- TR-104159 : “Experience with the Use of Programmable Logic Controllers in Nuclear Safety Applications”
- 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

Other Standards

- **TR-103699 V1-2 : “Programmable Logic Controller Qualification Guidelines for Nuclear Applications”, 1994**
- **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-6895 : “Guidelines for the Safety Classification of Systems Components, and Parts Used in Nuclear Power Plant Applications (NCIG-17)”, 1991**

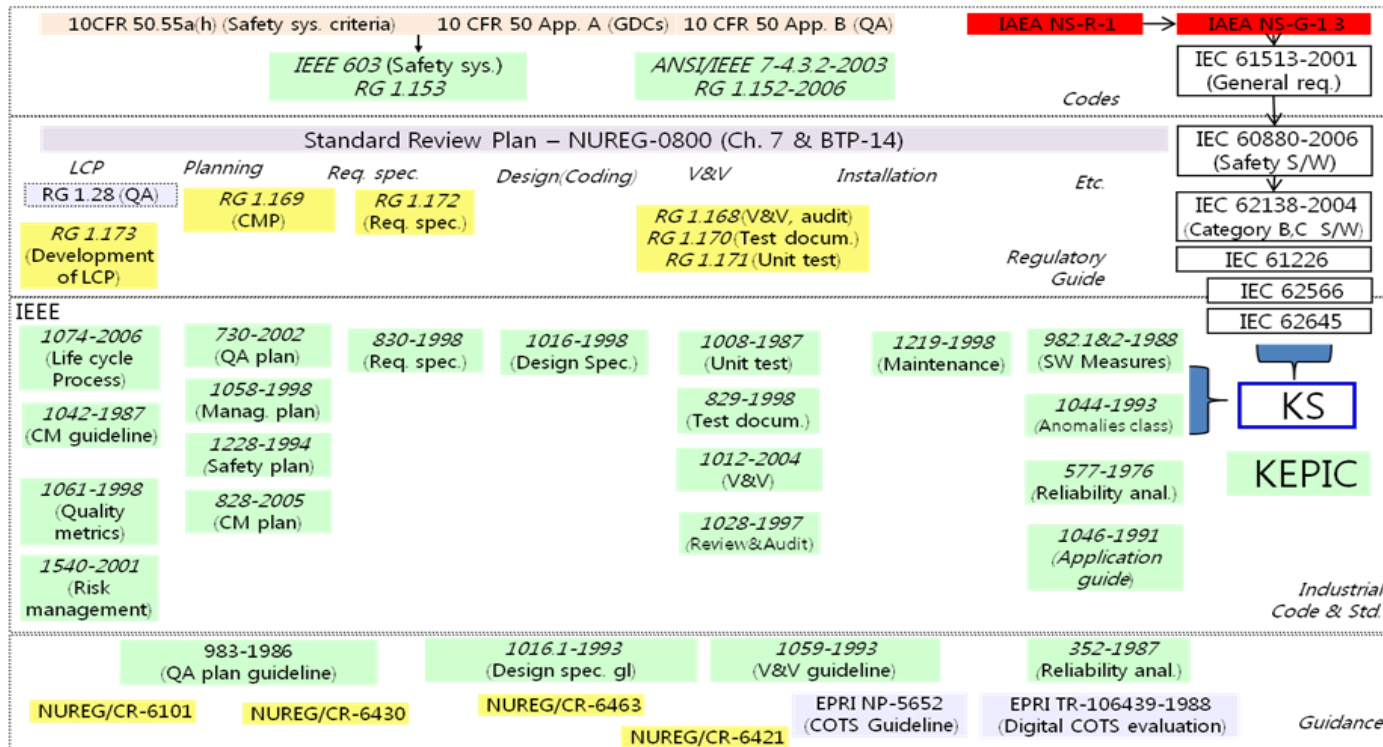
Other Standards

- **IEEE 730-2010 : IEEE Standards for Software Quality Assurance Plants**
- **IEC 61226 : “Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of I&C Functions”**
- **ASME NQA-1**
- **TR-112679 : “Critical Characteristics for Acceptance of Seismically Sensitive Items”**
- **TR-1016157 : “Plant Support Engineering: Information for Use in Conducting Audits of Supplier Commercial Grade Item Dedication Programs”**
- **IEEE-7.4.3.2 : “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”**

Other Standards

- Organizing standards map like above figure

원자력 소프트웨어 표준 체계



19

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.

Functional Safety Certification

- **Functional Safety**
 - Functional safety is part of the overall safety of a system or piece of equipment and generally focuses on electronics and related software
 - It looks at aspects of safety that relate to the function of a device or system and ensures that it works correctly in response to commands it receives
 - In a systemic approach Functional safety identifies potentially dangerous conditions, situations or events that could result in an accident that could harm somebody or destroy something
 - Freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly
- **Safety Function**
 - the function to prevent failure of system, to manage the risk of system
- **SIL(Safety Integrity Level) : 제품의 안전 기능에 요구되는 신뢰도 수준**
 - Using Performance Measures, probability of the safety function operation

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

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



CERTIFICATE



**SGS
TÜV
SAAR**

CERTIFICATE NO FS/71/220/14/0030 **PAGE 1/1**
ZERTIFIKAT NR. SEITE 1

LICENCE HOLDER <small>GENEHMIGUNGSINHABER</small>	MANUFACTURING PLANT <small>FERTIGUNGSSTÄTTE</small>	
GASTRON CO. LTD 18-8, DOGEUMDANJI1(IL)-GIL, SANGROK-GU, ANSAN-SI, GYEONGGI-DO, KOREA	GASTRON CO. LTD 18-8, DOGEUMDANJI1(IL)-GIL, SANGROK-GU, ANSAN-SI, GYEONGGI-DO, KOREA	

PROJECT NO./ID <small>PROJEKT-NR./ID</small>	LICENSED TEST MARK <small>GENEHMIGTES PRÜFZEICHEN</small>	CERT. REPORT NO. <small>ZERTIFIKATSBERICHT NR.</small>
F1MW		F1MW0003

Tested according to <small>Geprüft nach</small>	IEC 61508: 2010
Certified product(s) <small>Zertifizierte(s) Produkte</small>	Infrared Type Gas Detector
Model(s) <small>Modelle</small>	GIR-3000
Technical Data and Parameter <small>Technische Daten und Parameter</small>	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 <small>Spezielle Anforderungen</small>	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
Zertifizierungsstelle für Funktionale Sicherheit

The test mark registered as an integral part of this certificate
is a valid certification mark for the product.

Post-13/14 New Street, 104 3Lancaster 14, 15241, Tammob 14

Web: www.sgs-tuv-saar.com E-mail: sgs@sgs.com



Munich, 2014-02-11

Marcus Rau



TI development process

- SafeTI software development process receive functional safety certification

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.

그래서...

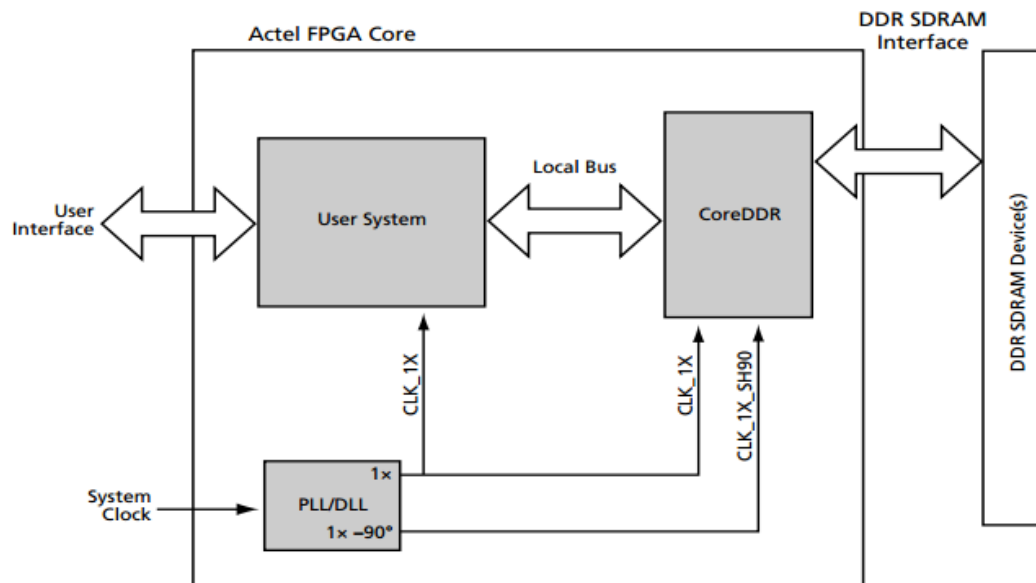
- IEC 61508, 61513, ISO 26262와 같은 기능 안전성 소프트웨어 요구사항에 적합한 개발 프로세스 인증 (V&V 내용 포함) 을 받는 것 중 사용되는 도구들의 인증과 dedication 하여 사용하는 것과의 관계 및 차이점에 대해 고려 필요

IP Core Library

- **IP (Intellectual Property) Core in FPGA**
 - Intellectual Property : reusable unit of logic, cell, or chip layout design that is the intellectual property of one party
 - Predefined library of function or circuits for supporting development of FPGA by Vendor/User
 - Supporting memory management, data bus interface, security, etc.
- **Microsemi (Liberio SoC) provides 2 kinds of IP Core**
 - Direct Core : providing in liberio by Microsemi vendor
 - Companion Core : providing by third-party developer
 - Direct core is able to use in liberio tool with adding design block
- **Other FPGA vendors also provide several IP library**
- **Accordance with NUREG/CR-7006, IP core library is not recommended to use in safety systems**

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



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

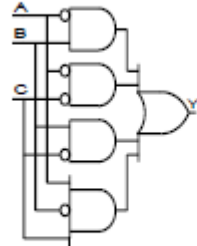
NUREG/CR-7006 Design Entry Example

- **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

Vendor (Chip) specific macro libraries

- 각 벤더 (chip) 별로 합성, P&R 등의 편의성을 이유로 macro libraries 를 지원

AO12 IGLOO, ProASIC3, SmartFusion, Fusion



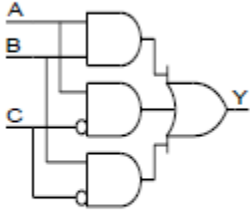
Input: A, B, C
Output: Y

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

AO13 IGLOO, ProASIC3, SmartFusion, Fusion



Input: A, B, C
Output: Y

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

The END

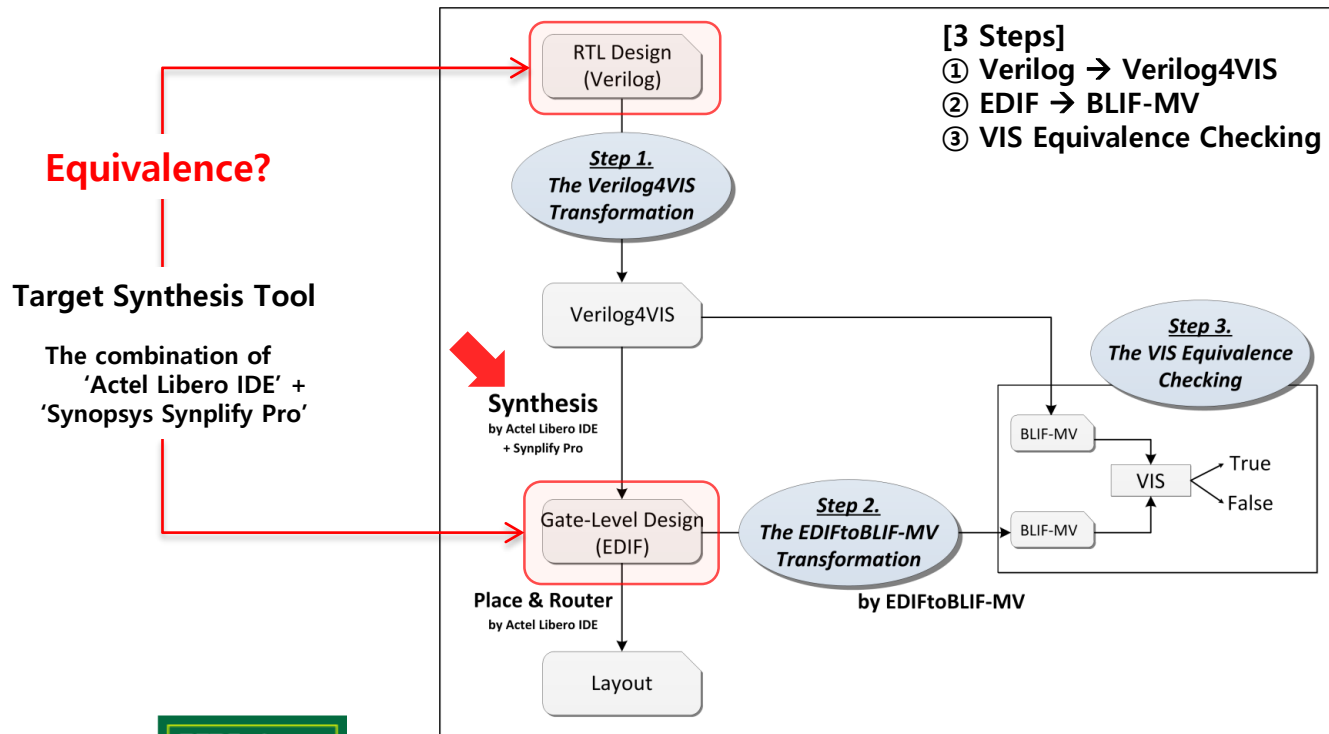
END

CVEC (A Customized VIS based Equivalence Checking)

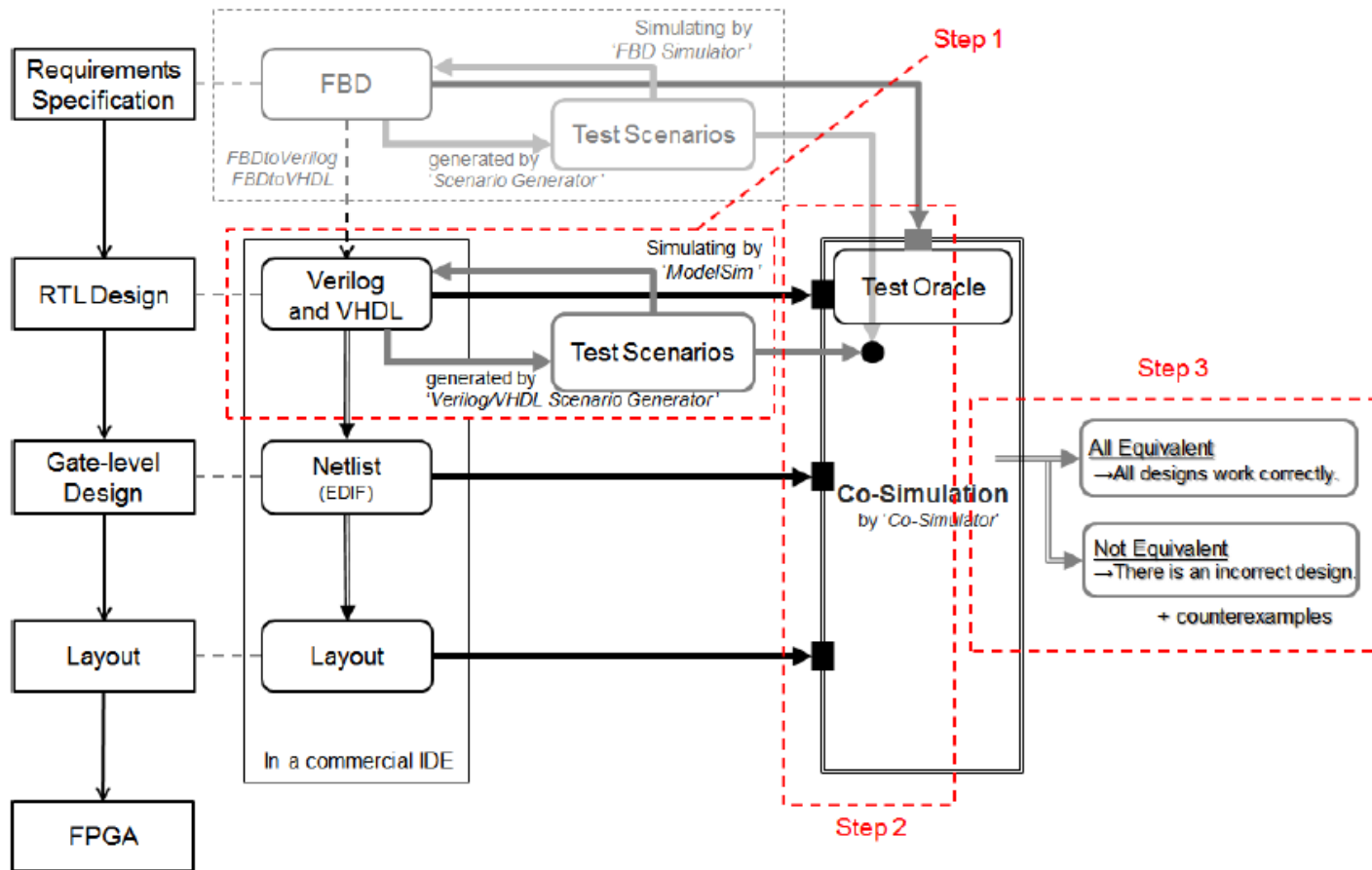
A VIS based solution (VIS : Verification Interacting with Synthesis)

It can verify the combination of 'Synopsys Synplify Pro' with 'Actel Libero SoC'

- An open-sourced formal verification tool, VIS
- Translators requires (step1,2) to use the VIS
- Verification performance is up to the VIS



IST-FPGA(Integrated Software Testing framework for FPGA)



Linting Rules for FPGA Development

- RTL linting is kinds of rule checking for RTL design
- There are several linting tools
 - Leda of Synopsys
 - Ascent Lint of Real Intent
 - VHDL rule checker of Sigasi
 - Etc..
- They checks with their own rules and user defined rules also
- Example
 - Mixed language
 - Coding style check

App. TIMES for FPGA

- Timed automata를 이용한 HDL(Verilog, VHDL) formal verification?
- Timed automata를 이용한 digital circuit의 timing analysis?
 - Generally, timing analysis is performed after place & route
 - Because it needs timing constraints information which contains clock skew delay, synthesis information, etc.