

# What is the difference between DO-178C & DO-178B?

UC\_Laboratory

201371150

은애천

# What is the differences between DO-178C & DO-178B?

## DO-178B

- 항공 관련 시스템에서 감항능력에서 요구되는 기준을 만족하는 특정 레벨의 안전 기준을 가지게 하는 것과 그러한 의도된 기능을 수행하는 소프트웨어 생산을 위한 가이드라인을 제공

## DO-178C

- DO-178B에서 low-level requirements에 대한 개념이 모호하여 기존에 제시 되어왔던 문제들이 완전히 해결되지 않을 수 있다는 점 때문에 등장

# Contents

- 인증을 적용 하기 위한 툴 자격
- 모델 기반 디자인 & 객체지향
- 명확한 언어와 용어의 사용을 통한 일관성
- 표준 적용 레벨에 따른 추가 목표 적용
- 추적 불가능한 소스 코드 검증의 달성
- 매개변수 데이터 항목 파일
- 여러 종류의 기술적인 문서들

# 인증을 적용하기 위한 툴 자격

## Tool Qualification

- DO-178B에서는 “development tool”와 “verification tool” 두 가지의 자격을 판단하는 기준을 따로 다루었는데 DO-178C에서는 소프트웨어 설계를 보증하는 수준에 따라 3가지의 툴의 자격 판단 기준을 만들었는데 이것들을 “Tool Qualification”이라 함

# 인증을 적용하기 위한 툴 자격

## Criteria of Tool Qualification

- 기준 1. 툴의 output이 airborne software의 일부이면서, error를 추가할 수 있는가  
(Development)
- 기준 2. 검증을 자동화 하는 툴은 error 감지에 실패할 수 있으면서,  
그 output을 제거하거나 output 감소를 정당화 하는데 사용될 수 있는가  
(Verification & Augments other development or verification activities)
- 기준 3. 사용 목적의 범위 내에서 error를 감지 하지 못할 수 있는가  
(Verification only)

# 인증을 적용하기 위한 툴 자격

## Tool Qualification

- TQL은 1~5까지 존재하며, 1이 가장 정확한 것이고 5가 제일 부정확한 것

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

Figure1. Tool Qualification Level Determination

# 모델 기반 디자인 & 객체지향

## Model-based Design & Object-Oriented

### DO-178B

- Structured design을 가정
- OO수용하지만, 사용자정의
- 가시성을 극대화
- OO와 MBD 추적에 약함

### DO-178C

- OO와 컨트롤 모델링 허용
- MBD와 OO 수용
- 추적을 강조
- 주소 메모리 관리 및 예외처리
- 상세한 MBD와 OO 설계 기준 강조

# 모델 기반 디자인 & 객체지향

## Memory Management

### DO-178B

- 명시적으로 정의 하지 않음

### DO-178C

- 메모리 관리자의 취약점
- 단편화(Fragmentation)
- 모호한 참조(Ambiguous references)
- 힙 메모리(Heap memory)
- 기억 장소 반환(Deallocation)
- 폐영역 회수(Garbage collection)

# 명확한 언어와 용어의 사용을 통한 일관성

## Formal Methods

- 설명 및 표기법으로써, 개발 및 시스템 동작에 관련된 것들을 명확하게 정의 하기 위한 수학적 기법

# 명확한 언어와 용어의 사용을 통한 일관성

## DO-178B

- 명시적으로 규정하지 않음
- 주관적으로 적용  
(예: 유럽의 ED-128B)

## DO-178C

- 요구사항 정확성 및 일관성 리뷰
- 소스코드 리뷰, 오토코드 생성
- Low-level까지 포함하는 테스트케이스
- 메서드 기반의 리뷰를 통해 테스트의 일부를 대체
- 코드 분석을 통해 테스트를 줄이기 위한 가능성 제공

# 표준 적용 레벨에 따른 추가 목표 적용

## Additional Objective

- DO-178B에서 일정 수준의 인증 레벨을 받기 위해 적용하던 Objective 수보다 추가 된 Objective를 사용

Table. 추가적인 요소들에 따른 Objective 사용

Software DAL	DO-178B	DO-178C
A	66	71
B	65	69
C	57	62
D	28	26
E	0	0

# 표준 적용 레벨에 따른 추가 목표 적용

## Hidden Objective

- 숨겨진 목표로는 명시적으로 ANNEX A의 테이블 A-7 #9에 있는 것이 존재
  - A-7 #9 : Verification of additional code, that cannot be traced to Source Code, is achieved.

# 추적 불가능한 소스 코드 검증의 달성

**Table A-7** Verification of Verification Process Results

	Objective		Activity Ref	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref		A	B	C	D	Data Item	Ref	A	B	C	D
1	Test procedures are correct.	<a href="#">6.4.5.b</a>	6.4.5	●	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
2	Test results are correct and discrepancies explained.	<a href="#">6.4.5.c</a>	6.4.5	●	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
3	Test coverage of high-level requirements is achieved.	<a href="#">6.4.4.a</a>	6.4.4.1	●	○	○	○	Software Verification Results	<a href="#">11.14</a>	②	②	②	②
4	Test coverage of low-level requirements is achieved.	<a href="#">6.4.4.b</a>	6.4.4.1	●	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
5	Test coverage of software structure (modified condition/decision coverage) is achieved.	<a href="#">6.4.4.c</a>	6.4.4.2.a 6.4.4.2.b 6.4.4.2.d 6.4.4.3	●				Software Verification Results	<a href="#">11.14</a>	②			
6	Test coverage of software structure (decision coverage) is achieved.	<a href="#">6.4.4.c</a>	6.4.4.2.a 6.4.4.2.b 6.4.4.2.d 6.4.4.3	●	●			Software Verification Results	<a href="#">11.14</a>	②	②		
7	Test coverage of software structure (statement coverage) is achieved.	<a href="#">6.4.4.c</a>	6.4.4.2.a 6.4.4.2.b 6.4.4.2.d 6.4.4.3	●	●	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
8	Test coverage of software structure (data coupling and control coupling) is achieved.	<a href="#">6.4.4.d</a>	6.4.4.2.c 6.4.4.2.d 6.4.4.3	●	●	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
9	Verification of additional code, that cannot be traced to Source Code, is achieved.	<a href="#">6.4.4.c</a>	6.4.4.2.b	●				Software Verification Results	<a href="#">11.14</a>	②			

# 매개변수 데이터 항목 파일

## Parameter Data Item

- 매개변수 데이터 아이템은 보통 데이터들의 집합으로 구성되며 실행 가능한 오브젝트의 동작에 영향을 미치는 요소들의 정보를 제공
  - A-5 #8 : Parameter Data Item file is correct and complete.
  - A-5 #9 : Verification of Parameter Data Item file is achieved.

# 매개변수 데이터 항목 파일

**Table A-5** Verification of Outputs of Software Coding & Integration Processes

	Objective		Activity Ref	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref		A	B	C	D	Data Item	Ref	A	B	C	D
1	Source Code complies with low-level requirements.	<a href="#">6.3.4.a</a>	6.3.4	●	●	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
2	Source Code complies with software architecture.	<a href="#">6.3.4.b</a>	6.3.4	●	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
3	Source Code is verifiable.	<a href="#">6.3.4.c</a>	6.3.4	○	○			Software Verification Results	<a href="#">11.14</a>	②	②		
4	Source Code conforms to standards.	<a href="#">6.3.4.d</a>	6.3.4	○	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
5	Source Code is traceable to low-level requirements.	<a href="#">6.3.4.e</a>	6.3.4	○	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
6	Source Code is accurate and consistent.	<a href="#">6.3.4.f</a>	6.3.4	●	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
7	Output of software integration process is complete and correct	<a href="#">6.3.5.a</a>	6.3.5	○	○	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	
8	Parameter Data Item File is correct and complete	<a href="#">6.6.a</a>	6.6	●	●	○	○	Software Verification Cases and Procedures Software Verification Results	<a href="#">11.13</a> <a href="#">11.14</a>	① ②	① ②	② ②	② ②
9	Verification of Parameter Data Item File is achieved.	<a href="#">6.6.b</a>	6.6	●	●	○		Software Verification Results	<a href="#">11.14</a>	②	②	②	

## 여러 종류의 기술적인 문서들

### Technology supplements were added

[DO-330](#) "Software Tool Qualification Considerations" - clarifying software tools and avionics tool qualification

[DO-331](#) "Model-Based Development and Verification Supplement to DO-178C and DO-278" - addressing Model-Based Development (MBD) and verification and the ability to use modeling techniques to improve development and verification while avoiding pitfalls inherent in some modeling methods

[DO-332](#) "Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A" - addressing object-oriented software and the conditions under which it can be used

[DO-333](#) "Formal Methods Supplement to DO-178C and DO-278A" - addressing [formal methods](#) to complement (but not replace) testing

감사합니다