<생각해보기> 답안

최종 업데이트 : 2021. 10. 13

* 생각해보기는 독자들이 직접 고민해보거나 포털에서 검색해 더 깊이 있게, 또는 보다 다양한 관점에서 문제를 살펴볼 수 있도록 하는 가이드입니다.

Chapter 01

1.1

직류 전원공급기의 입력인 전원(電源)도 다중화해야 한다. 안전필수 시스템의 제어용 전원장치는 직류 전원장치의 입력으로 AC 입력과 배터리 전원으로 공급되는 UPS(Uninterrupted 직류 전원공급기)를 설치하는 방식이 가장 많이 사용된다. 즉 전원공급기 장치와 전원이 각각 이중화되는 것이 좋은 방법인데, 이들에 대한 고장 진단이 가능해야 한다. 전원 두 종류와 전원장치 두 종류 각각에 대해서 진단이 가능하고, 운전중 유지보수가 가능하면 최고의 설계라고 할 것이다. 다시 이야기하면 장치(전원공급장치)와 전원(전기 공급원)을 모두 이중화해야 한다. 하나의 전원은 교류 입력을 사용하고, 다른 하나는 DC battery를 사용하는 방식이고, 장치는 정류형과 인버터형이 각각 사용되고, DC 출력단은 다이오드를 통해 이중화하는 것이 가장 완벽한 방법이라 할 수 있다.

1.2

이런 문제를 해결하기 위해 다중화에 사용되는 하드웨어나 소프트웨어는 다양성(diversity)을 갖도록 하는 것이 필요하다. 전원공급기에 사용되는 SMPS 모듈을 서로 다른 회사의 제품으로 이중화를 한다면 공통고장원인(CCF: common cause failure)으로 전원공급기가 동시에 고장나는 확률을 최소화 할 수 있다. 마찬가지로 같은 기능을 하는 메모리 소자의 경우라도 한 회사의 제품을 사용하는 것보다는 둘 이상의 회사 제품을 사용하거나, 동일 회사의 제품을 사용해야 하는 경우 Lot 번호가 다른 제품을 사용하는 것이 권고된다.

1.3

인화성 물질의 처리작업(도장 작업)과 발화성 작업(용접 작업)을 같이 수행하는 실수를 저지르지 않았나? 이를 방지하기 위한 방법으로 FMEA를 적용해야 한다. 이는 공정 FMEA를 적용하여, 도장작업으로 발생하는 인화성 가스가 용접작업의 불꽃에 의해 폭발하는 위험(가능성)은 없는가를 검토하여야 한다.

1.4

주변에서 찾아보자.
50층 아파트에 한 통로에 두 집만 있는 아파트인데, 엘리베이터가 자주 고장이 난다면 50층을 걸어올라가야 하는가?

1.5

안전 관련 시스템의 설계 관점에서 생각해본다면 원래 전화기는 안전기능을 수행하는 용도가 아니었다. 그런데 여러분은 집의 경비 시스템을 개선하면서 집의 방범 및 화재 등에 관한 모든 안전관리 및 비상정보를 휴대전화로 받도록 설정했다. 그러나 이전과 같이 회사에서 회의를 하거나 업무에 집중하는 시간에 무음으로 해놓거나 전화기를 꺼두면 비상연락을 받지 못해 조치를 취하지 못하고 큰 실패를 겪을 수 있다. 이 원인은 다음 한 마디로 요약할 수 있다. '비안전 등급 기기(일반 전화기)로 안전의 핵심인 비상연락 기능을 담당하도록 했는데, 전화기를 비안전등급 활동 형태로 관리한 것이다(지금은 이 말을 이해하기 어려울 것이다. 4~5장을 거치면서 이 문제를 이해하게 되면 귀하의 수준은 크게 높아졌다고 볼 수 있다).' 많은 사고는 이런 형태로 일어난다. 다시 설명하면, 매우 중요한 기능을 수행하는 기기가 원천적으로 신뢰성이 떨어지는 기기라면 중요한 기능을 수행할 수 없을 것이라는 의미이다.

1.6

각자 생각해보자.

자동 슬라이딩 도어의 경우에 자동 모드가 고장이면 수동으로 개폐가 가능해야 한다.

1.7

교재의 원문을 다시 읽으며, 본 생각해보기 등과 검토하기 바란다.

미리 살펴보기

Q1) "직류 전원공급기의 신뢰도가 0.95다."라는 표현은 맞는 말인가?

A1) 틀린 말이다. 신뢰도는 시간의 함수로서 시간 $t=0$에서는 1이며 $t=\infty$에서는 0이 되어야 한다.

예 $R(t)=e^{-\lambda t}$, $\lambda=10^{-k}/\mathrm{hr}$($k$는 양수)와 같은 형태로 표시되는 것이 일반적이다. λ는 고장률로 일정 값이지만 신뢰도 $R(t)$는 시간에 따라 감소한다. 신뢰도는 단조감소함수이다.

Q2) 고장허용설계가 제어 시스템을 완벽하게 다중화 했는데도 그 지역에 강한 지진이 발생해 시스템이 동작하지 않았다면 어떻게 해야 하는가?

A2) 여기서는 지진을 예로 들었으나 사실은 그 제어 시스템이 설치되는 환경과 운전 조건에 대해 모두 검증시험을 해야 한다. 예를 들어 진도 7까지의 지진이 올 수 있는 지역이면 진도 7보다 높은 수준의 지진을 가정하고 이런 경우에도 제어 시스템이 정상동작할 수 있도록 물리적으로 강하게 설계하여 내진시험을 해야 한다. 이에 대해서는 11장의 기기검증에서 상세히 다룬다. 다른 예로 설치 지역의 온도가 매우 높다고 하면, 이런 온도에서 동작 수명 동안 정상적으로 동작할 수 있는가에 대한 시험이 필요하다.

Q3) 아날로그 시스템은 회로도나 회로기판을 보면 상당부분의 논리나 기능을 파악할 수 있다. 이를 반대로 이야기하면, 아날로그 회로가 제대로 설계되고 제작되었는지는 일정 수준 이상의 사람이라면 쉽게 확인 가능하다는 의미다. 그런데 디지털 시스템에서는 소프트웨어가 보이지 않고 소스 코드를 봐도 전체를 이해하고 틀린 부분이 없는지 확인할 수가 없다. 이런 디지털 시스템에서는 소프트웨어를 어떻게 확인할 수 있을까?

A3) 소프트웨어는 봐도 알기 어렵고 특히 대상 시스템에서 필요로 하는 모든 기능이 구현되어 있는지 한 번에 파악할 수 없다. 그러므로 소프트웨어 개발자는 제3의 조직 또는 인사가 모든 소프트웨어 작업(문서작성부터 코딩, 시험 등)을 확인 및 검증할 수 있도록 작업해야 한다. 이를 위한 모든 절차와 작성 방법이 기술표준으로 상세히 정해져 있다. 이에 대해서는 7~8장에서 다룬다.

Q4) 휴대폰을 가지고 고압선 밑에 가니 잡음이 심한데, 이는 고압선의 전자장에 의해 통신장애가 발생하기 때문이다. 내가 만드는 디지털 제어 시스템은 운전 중 전자파에 의해 영향을 받지 않을까? 받는다면 어떻게 해야 할까?

A4) 모든 제어 시스템은 정해진 기기검증 시험을 받아야 한다. 기기검증 시험 중에서 전자파 시험이 문제에 해당하는데, 전자파시험은 피시험기기에서 나오는 전자파가 일정 기준 이하일 것과 피시험기기에 일정 수준의 전자파를 가하더라도 정상 동작에 이상이 없다는 것을 본다. 여기서 전자파는 공간으로 방사되는 방사파와 전기선을 타고 이동하는 전도성의 두 가지에 대해 시험한다. 또한 전기적인 서지 등에 의한 오동작 여부를 확인하는 과정을 거친다.

Q5) 포털사이트에서 **『집중해부-보잉 737 맥스 8 연쇄추락사고의 내막(Monthly Chosun, July 2019)』**을 찾아 읽고, 다음의 관점에서 문제점을 나열해보자. 어떤 항목은 이후의 장에서 답이 나오는 어려운 문제도 있다. 이 책의 목표가 이런 문제들이 다시는 발생하지 않도록 하는 것임을 미리 생각해보게 하는 문제다. 이 책을 모두 읽고 나서 다시 이 문제를 풀어보면 귀하의 실력은 준 고수의 반열에 이르게 될 것이다.

A5)

- **설계절차와 과정 문제**
  - 설계과정과 최종 항공기 출고시의 제작은 완전히 달랐다.
  - 최초 설계과정에서는 고각 센서 이중화로 설계하였다고 알려진다.
- **시뮬레이터 문제**
  - 항공기 시뮬레이터는 실제 항공기 상태 및 응동특성과 완전히 같아야 하는데, 조종사들이 훈련했던 시뮬레이터와 실제의 항공기는 별개의 물건이었다.
  - COVID로 인해 조종사들이 실제 항공기 조종을 일정기간 이상 못하게 되면 조종사 면허가 취소되도록 되어있다. 이를 보완하는 방법이 같은 기종의 시뮬레이터를 일정 횟수 이상 조종해야 하는데, 시뮬레이터가 없는 항공사는 조종사들의 면허가 취소되는 경우들이 발생했다. 이는 시뮬레이터가 실제 항공기를 거의 완전하게 모사할 수 있음을 보여주는 사례이다.
- **조종사에 대한 사전 교육 문제**
  - 상기 시뮬레이터 문제처럼 조종사들은 비행기가 어떻게 바뀌었는지에 대한 충분한 교육을 받지 못했다.
- **품질 문제**
  - 설계품질뿐만 아니라 전사적 품질경영이 전혀 안 된 최악의 품질사태라고 할 수 있다.
- **경영 문제**
  - 보잉 737 Max의 문제는 99.9%의 확률로 최고 경영자의 지시가 아니면 일어날 수 없는 일이다.
- **설계 문제**
  - 최초 설계 엔지니어들은 제대로 된 과정을 거쳤다고 판단된다. 그러나 설계 엔지니어들은 제작과정이나 품질검사 과정에서 잘못되고 있음을 알았을 것으로 예상된다. 아무도 할 말을 하지 않았던 것 이 아닐까?
- 조**직의 투명성과 책임, 권한 문제**
  - 조직의 권한부여가 독립적이지 못했다.
- **인허가 기관의 문제는 전문성 부족인가? 도덕성 결여인가?**
  - 인허가 기관도 무언가 심각한 문제가 있었을 것으로 생각된다.
- **공학적 신뢰도 계산 방법은?**
  - 3장을 공부한 후에 받음각 센서의 고장률을 임의의 값(예: $10^{-5}/\mathrm{hr}$로 하고, 10시간 동안의 신뢰도를 구해보기 바란다.
- **신뢰도 병목지점은?**
  - 항공기의 많은 제어부품은 다중화되어 있는데, 받음각 센서가 하나이기에 이것이 신뢰도 병목이다.
- **사고의 원**인은? (우선순위로 나열)
  - 이런 사고 재발방지대책으로, 위의 원인들에 우선순위를 정해보기 바란다.

Chapter 02

2.1

Google 에서 "Auto Sliding Door Mechanism"을 검색하여 상세한 자료를 검토하고 연습하기 바란다.

2.2

(a) Google에서 standby sparing, hot standby sparing, cold standby 등에 대하여 검색하여 차이를 이해하기 바란다.

(b) Google에서 duplication with comparison을 검색해보자.

(c) Google에서 검색, 6장의 TMR Exciter에서 DC converter 삼중화가 Flux summing의 예가 된다. 발전기 계자권선에 흐르는 전류는 병렬인 3개의 converter의 전류가 합해지는 것이며, 목표는 300A이다. 3대의 converter가 병렬로 연결되어 있으면 각각의 converter는 개략 100A씩, 전체가 300A가 되도록 전류를 공급하는데, 어느 converter 하나가 고장이면 2개의 converter가 300A를 공급하기 위해 대략 150A씩을 공급하게 되는 방법이다.

(d) Google에서 redundant memory checking을 검색하여 살펴보기 바란다. 최근의 추세는 RAM이나 Register의 오류를 막기 위해 반도체 설계단계에서 많은 방법들이 사용된다.

2.3

교재 278쪽 다수호기 설치 이후의 문제들을 살펴보자.

Chapter 03

3.1

고장률 0.0001/hr인 경우에 신뢰도는 $R(t)=\exp(-0.0001t)$이다. 여기에 $t=2000$을 대입하면 $R(2000\,\mathrm{hr})=\exp(-0.2)=0.818$이며, 이 값은 0.95보다 작다.
이중화의 경우를 계산하면 신뢰도는 $1-$(2개의 모듈 모두 고장인 확률)이 되며 $R(t)=1-[1-\exp(-0.0001t)]^2=2\exp(-0.0001t)-\exp(-0.0002t)$이고, $t=2000$을 입력하면 $R(2000\,\mathrm{hr})=2\exp(-0.2)-\exp(-0.4)=2\times0.818-0.670=0.966$이다. 이 값은 0.95보다 크다.
즉 이중화를 통해서 2000시간 동안의 신뢰도를 0.95보다 크게 유지할 수 있다. 삼중화의 경우를 고려하지 않아도 된다.

상기의 계산 및 필요한 경우에 그래프를 그리는 것은 Wolframalpha software를 사용할 것을 권한다.
실제 공학설계에서는 이중화에 대한 정확한 정의와 구현이 필요하다.

3.2

고장률 $\lambda=\dfrac{6}{5000\times100}/\mathrm{hr}=1.2\times10^{-5}/\mathrm{hr}$

3.3

일 년은 8760시간으로 계산한다.
일 년 동안에 사용할 수 없는 기간은 두 번 정기점검 48시간, 오일 교체 12시간 등 60시간이다.
그러므로 평균 가용도는 최댓값이 $\dfrac{8760-60}{8760}=0.993$, 즉 99.3%가 된다. 만약에 1년에 평균적으로 고장이 2회 발생하며, 고장 수리에 각각 24시간이 소요된다면, 평균 가용도는 $\dfrac{8760-60-48}{8760}=0.9876$, 즉 98.76%가 된다.

3.4

교재에서 이야기한 교통신호등의 고장 시에 적색 및 황색 등이 점멸하도록 하는 설계,
엘리베이터 고장 시에 문은 항상 닫혀 있도록 하는 설계,
복잡한 계통(예 압력이나 레벨 조절용 밸브)의 밸브 제어장치 고장 시에는 밸브의 위치가 항시 open 또는 close 상태가 되도록 사전에 설정하는 방식으로 시스템의 안전을 유지한다.

3.5

마코프모델은 다중화된 시스템에서 운전중 고장감지 및 유지보수가 가능한 경우를 해석하기 위한 방법론이다. 이를 통해 매우 높은 신뢰도를 확보할 수 있다. 제6장의 해석결과를 공부하기 바란다.

3.6

교재 126쪽을 살펴보기 바란다.

3.7

여기서 삼중화는 2 out of 3를 의미한다고 가정한다. 그래프가 x축과 교차한다는 의미는 $R_3(t)=R(t)$인 경우이다.

$R_3(t) = 3R^2(t) - 2R^3(t)$

그러므로 $R_3(t) = 3R^2(t) - 2R^3(t) = R(t)$이고, $R(t) = R$로 놓으면 $2R^3 - 3R^2 + R = 0$이다.
그러므로 $R = 0,\ 0.5,\ 1$의 세 경우가 있으며, 여기서 의미를 갖는 해는 $R = 0.5$이다.

즉, $R = R(\lambda t) = R(-6931 \times \lambda) = \exp(-6931 \times \lambda) = 0.5$
그러므로 $-6931 \times \lambda = \ln(0.5) = -0.6931$이다.
따라서 $\lambda = 10^{-4}/\mathrm{hr}$

3.8

$R_2(t) = 2\exp(-\lambda t) - \exp(-2\lambda t)$

3.9

$R(t) = \exp(-2\lambda t)$

3.10

이 모델이 실질적으로 이중화된 모델이다. 생각해보기 3.8의 경우에 해당하는 것인데, 여기에서 고장인 모듈을 운전 중에 수리도 가능하다고 하면 마코프모델을 적용해야 하며, 이 경우에 신뢰도 및 가용도는 상상외로 향상된다.

Chapter 06

6.1

VME system은 기본적으로 RTOS(Real Time Operating System)을 사용한다. RTOS 중에는 Vx-Works가 시장 지배력이 가장 높고, 이는 뛰어난 성능을 갖고 있기에 가능한 것이다. 이 성능은 당양한 서비스 기능과 사용이력을 갖고 있다. 그러나 안전필수시스템에서 요구되는 기능인 결정론적 특성과 모든 기능에 대한 확인검증이 요구되는 수준까지 이루어지지 않았기 때문입니다. 이는 다양한 편리기능을 넣기 위해서 그 소스 코드가 방대한 규모인데, 이에 대한 적절한 수준의 확인검증은 거의 불가능에 가깝기 때문이다. 우선 OS가 안전필수시스템에서 사용할 필수기능에 필요한 부분만이 있도록 해야 한다는 것이 인허가 관점에서의 요구이다.

6.2

Vx-Works는 소스 코드가 모두 확인검증(설계단계의 모든 문서부터 추적성 및 확인검증, 테스팅 등)이 가능한 OS인, 소규모 OS가 적합하다. 기능은 단촐해서 안전필수시스템 구현에 필요한 것만 포함하도록 하는 OS가 필요하며, 이를 위해서 마이크로급 OS가 사용되며 많은 경우에 open-source OS가 사용된다.

6.3

결정론적 통신이 가능한 방식으로 Prdfi-bus가 많이 쓰인다.

6.4

교재 8장을 복습하기 바란다.

6.5

교재 10장과 교재 5장의 234, 235 및 237쪽을 살펴하기 바란다.

Chapter 07

7.1

최근 일반 소프트웨어 개발 과정은 주로 생산성 향상에 주안점을 두고 발전하고 있다. 예를 들어 전통적인 폭포수 모델과 같이 단계별 활동을 수행하기보다는 일정 주기를 가지고 빠르게 프로토타입을 개발하고 덧붙여 나가는 애자일 방법론이 유행하는 것도 같은 이유로 생각된다. 이와 같은 방법을 적용할 수 있는 이유는 빠르게 시장 변화에 적응하기 위함도 있지만, 원할 때 상대적으로 쉽게 대상 소프트웨어를 변경할 수 있는 이유도 크다.
안전필수시스템의 경우 소프트웨어가 한번 개발되면 이에 대한 확인 및 검증, 안전성분석, 사이버 보안 평가 등 다양한 활동이 수반되기 때문에 소프트웨어 변경 비용이 매우 높다. 또한 출시 후 오류로 인한 인적, 사회적, 경제적 피해를 가늠할 수 없으므로 V 모델과 같이 단계별 활동을 중요시하는 경향이 있다.

7.2

(각자 생각해보기) 7.2.2절의 '기능 요구사항(functional requirements)'의 [예시 7-3]과 같은 가상의 기능을 자연어로 기술해보고 이때 발생할 수 있는 모호성을 고민해보자.

7.3

(각자 생각해보기) 최신의 자동차는 굴러다니는 컴퓨터로 칭할 만큼 수없이 많은 전자제어 시스템이 들어간다. 예를 들어 핸들을 통해 자동차를 조향하는 경우에도 전자 모터를 통해 회전을 쉽게 해준다. 만일 이와 같은 장치의 오류가 발생한다고 하면 어떤 일들이 벌어질까? 만일 제어장치 이상으로 원하는 방향과 반대로 모터가 회전하면 아마도 큰 사고로 이어질 것이다.
그래서 자동차 제어기에는 수없이 많은 fail-safe 기능이 포함되어 있다. 즉 원하는 주요 기능을 수행할 수 없을 때도 차량을 안전하게 제어할 수 있도록 제어기의 오류를 지속적으로 진단하고, 이상이 발생하면 최소한의 안전을 보장하는 보조 기능이 동작하도록 구현된다.

7.4

우리가 일상생활에서 흔히 접하는 엘리베이터에도 많은 안전 기능이 포함되어 있다. 전자적으로 제어하는 엘리베이터의 대표적인 안전 기능 및 장치의 예는 다음과 같다.

- 과부하감지장치 : 적재하중을 초과하여 승차 시 경보가 울리고 문이 열리며 해소 시까지 문을 열고 대기함
- 출입문 안전장치 : 문이 완전히 닫히지 않거나 고장인 경우를 감지해 엘리베이터 문이 다시 열리거나 운행이 되지 않도록 제어
- 과속조절기 : 엘리베이터가 특정 속도를 넘어서면 추락이나 이상 동작을 방지하기 위해 정지하도록 제어
- 리미트 스위치 : 승강기가 최상층 이상 및 최하층 이하로 운행되지 않도록 엘리베이터의 초과 운행을 방지
- 개문출발방지장치 : 엘리베이터의 구동기 또는 제어시스템의 결함으로 승차장 문이 잠기지 않거나 엘리베이터 문이 닫히지 않은 상태로 움직이지 않도록 제어

7.5

(각자 생각해보기) https://llvm.org/docs/CodingStandards.html에는 다양한 컴파일러 제작에서 사용되고 있는 llvm 프로그램 개발을 위한 코딩 규칙이 정해져 있다. 해당 규칙을 보면 몇몇 안전을 위한 규칙도 존재하나 여러 사람이 협업하기 위한 코드 작성 규칙이 많은 부분을 차지하고 있다.

만일 해당 프로그램이 안전필수시스템을 위한 것이었다면 코드 스타일 규칙과 함께 'strcpy 함수 사용 금지'와 같이 보안 측면에서 버퍼 오버플로우 공격이 발생할 수 있거나 안전 측면에서 메모리 오류로 프로그램이 이상 종료할 수 있는 위험 요소를 제거하기 위해 널리 사용되는 코딩 규칙들이 포함되었을 것이다.

7.6

(각자 생각해보기) 최근 미국에서는 송유관 업체 '콜로니얼 파이프라인'을 마비시킨 사이버 공격이 발생하였다. 미국 연방수사국(FBI)은 이번 사건의 배후로 러시아에 있는 것으로 추정되는 신생 랜섬웨어 조직 '다크사이드(DarkSide)'를 특정하였는데, 이 사건의 영향으로 미국의 휘발유 가격이 7년 만에 최고가로 치솟고 동남부 일대를 중심으로 기름 '사재기'가 극성을 부리며 일부 주유소의 재고가 바닥이 나는 등 심각한 후유증을 남겼다.
이 사건에 대한 조치로 바이든 대통령은 연방정부 기관뿐 아니라 민간 분야의 사이버 안보 기준을 상향하는 행정명령을 내렸다. 이 명령은 모든 연방 기관에서 다중인증(multi-factor authentication)을 사용하는 것과 같이 기본적 사이버 안보 조치를 골자로 한다.
추가로 최근에는 공급망에 대한 사이버 보안이 주목을 받고 있다. 왜냐하면 최종 설치 시설의 경우 많은 보안 장치들이 있지만, 이 시스템을 개발하는 하도급 업체들은 이에 비해 보안이 허술한 경우가 많다. 따라서 정교해지고 있는 최신 사이버 공격에서는 납품 업체의 개발 단계에서부터 침투하여 설치 후 공격할 수 있는 시점을 기다리는 경우도 많을 것으로 예상되고 있다. 이를 위해서 최근 많은 보안 지침에서는 공급망에 대해서도 사이버 보안을 평가하고 유지하고 있는 규칙들을 보강하고 있다.

7.7

(각자 생각해보기) 안전필수시스템 개발 시에는 사이버 보안 기능과 안전 기능이 상충하는 경우가 많이 발생한다. 예를 들어 비상 버튼을 포함하는 화면을 생각해 볼 수 있다. 사이버 보안 측면에서는 허가받지 않은 인원이 비상 버튼을 눌러 시스템을 정지하는 것을 방지하고자 패스워드 잠금 기능을 요구할 수 있다. 하지만 안전 측면에서는 사건이 발생하면 즉시 대응할 수 있어야 하므로 비상 버튼 화면이 항상 표시될 수 있도록 요구할 것이다. 이 비상 버튼의 역할에 따라서 다른 결정을 내릴 수 있겠지만 촌각을 다투는 상황이라면 아무래도 비밀번호를 입력한다거나, 비밀번호를 여러 번 틀려 화면이 잠긴다든가 하는 상황은 받아들이기 힘들 것이다.
안전필수시스템에서는 상충하는 요구사항이 있을 때 많은 경우 안전 기능이 우선하나 상황에 따라서 두 가지 요건을 모두 만족하도록 변경이 가능할 수 있기 때문에 개발, 안전, 보안 담당자가 서로 협력하여 소프트웨어를 개발하여야 한다.

Chapter 08

8.1

소프트웨어 검증은 제품을 올바르게 만들고 있는가를 검사하는 과정으로 현 단계의 산출물이 이전 단계의 제약 또는 요구사항을 위반하지 않음을 보이기 위한 과정이다. 즉 소프트웨어 요구사항은 시스템의 사양을 만족해야 하며, 소프트웨어 설계는 소프트웨어 요구사항을 만족해야 한다. 같은 의미로 소프트웨어 구현 코드는 소프트웨어 설계를 벗어날 수 없다. 이와 같은 과정은 추상적인 사용자 요구사항이 구현으로 상세화되는 과정에서 단계마다 지켜져야 하는 원칙으로 요구사항 및 제약을 위반하는 설계 및 구현이 되지 않도록 막는다.
소프트웨어 확인은 올바른 제품을 만들고 있는가 검사하는 과정으로 최종 개발 산출물이 요구되는 속성을 만족함을 보이기 위한 과정이다. 소프트웨어 확인 기법에 따라 요구되는 속성은 사용자 요구사항, 소프트웨어 요구사항, 설계 요구사항 등이 될 수 있고, 소프트웨어 테스트 기법이 주로 사용된다.
따라서 안전필수시스템 개발에서는 개발 단계별로 소프트웨어 검증을 수행하고, 개발이 완료된 산출물에 대해 소프트웨어 확인을 수행하는 V 모델을 사용하고 있고, 소프트웨어 확인 및 검증이 모두 성공적으로 완료되었을 때 최종 개발이 완료된다.

8.2

소프트웨어 정적 분석은 검사하고자 하는 특정 속성을 프로그램의 실행 없이 소스 코드의 구문과 의미만으로 해석하여 속성이 만족하는지를 검사하거나 속성이 만족하지 않는 오류를 찾아내는 기술이다.
소프트웨어 정형 검증은 정형 명세가 주어진 속성을 만족하는지 (반)자동으로 검사하는 기술이다.
두 기술 모두 소프트웨어의 속성이 만족하지 않는 오류를 찾아내거나 속성이 만족함을 보이기 위해서 적용할 수 있으나 일반적으로 다음과 같은 차이점이 있다.
정적 분석은 이미 결정된 특정 속성을 분석하기 위해서 개발된다. 예를 들어 array index out of bound를 찾아내기 위한 정적 분석기는 index 변수의 범위는 잘 예측할 수 있지만, 다른 속성(예를 들어 무한 회귀 호출)과 같은 오류를 찾기는 힘들다. 따라서 정적 분석 도구는 이미 검사할 수 있는 속성들이 사전에 정해져 있는 경우가 대부분이다. 하지만 특정 속성만을 검사하기 때문에 정형 검증보다는 성능이 좋아 대규모 프로그램에도 적용할 수 있는 도구들이 많이 개발되어 있다.
정형 검증은 입력받은 정형 명세를 대상으로 검증하고자 하는 검증 속성을 자유롭게 기술하면 해당 속성의 만족 여부를 검사할 수 있다. 따라서 정형 검증 도구는 대상 정형 명세에 대해서 검증하고자 하는 속성을 정의하기 위한 언어가 제공되고, 사용자는 이 언어로 검사하고자 하는 다양한 속성을 기술하여 검증할 수 있다. 정형 검증은 정적 분석과 비교할 때 더 많은 계산이 필요하므로 개발 초기 요구사항이나 설계에 해당하는 정형 명세를 검증하는 데 사용되어 왔으나 최근 소스 코드를 입력받는 정형 검증기가 개발되는 등 정적 분석과 정형 검증의 구별이 약해지고 있다.

8.3

(각자 생각해보기) 소프트웨어 테스팅의 한계는 완전한 시험이 불가능하다는 것이다. 즉 소프트웨어의 오류가 있는 경우 이를 찾을 수는 있지만, 오류가 없는 것은 보장할 수 없다. 따라서 안전성이 매우 중요한 시스템에서는 오류가 없음을 보장할 수 있는 정형 검증 기법을 사용하거나, 정적 분석으로 특정 속성이 위반되는 경우가 없음을 분석하고 있다.

8.4

(각자 생각해보기) https://www.opencoverage.net에는 floglogic사에서 몇 가지 오픈소스 프로젝트에 대해 시험 후 테스트 커버리지를 측정한 결과가 소개되어 있다. 대표적인 오픈소스 파일 데이터베이스인 sqlite의 예시의 경우 현재 조건 커버리지를 기준으로 89.4%를 기록하고 있다.

이 예제에서 100% 커버리지 미만의 소스 코드들을 살펴보면 구문 커버리지는 만족하나 조건 커버리지가 만족하지 않는 구문들이 있는데, 그중 특별한 상황이 아니면 실패하지 않는 OS 서비스 함수를 호출한 결괏값에 대한 오류 처리가 포함되어 있다. 이 같은 경우에 오류 처리가 제대로 되는지 시험하기 위해서 실제 함수가 아니라 오류 값을 반환하는 가상의 함수 호출하도록 수정하여 시험하기도 하는데 이와 같은 가상의 함수를 테스트 스텁(test stub)이라 한다.

8.5

구문 커버리지와 분기 커버리지가 차이가 나는 대표적인 경우로 else 구문이 없는 조건문을 들 수 있다. 다음과 같은 소스 코드를 생각해보자.

```
1 : if (input > 0) {
2 :     printf("success");
3 : }
```

위의 코드에 대해 input이 3인 경우를 실행한다면 1번째 줄에서 조건이 참이 되므로 2번째 줄에서 'success'를 출력하고 3번째 줄에서 종료한다. 따라서 {input = 3} 인 시험 사례는 구문 커버리지를 만족한다. 하지만 이 시험 사례는 1번째 줄의 조건이 거짓이 되는 경우를 시험하지 않았기 때문에 분기 커버리지는 만족하지 못한다.

Chapter 09

9.1
A 사는 원래 품질보증/관리가 철저한 회사인데, CEO의 긴급지시로 급하게 구매발주 절차를 진행하였으며, B 사는 A 사 CEO의 구두지시(요청)를 먼저 받았으므로 사전 작업에 들어간 것이다. A 사는 CEO의 지시가 있었더라도, 절차를 지키며 구매를 진행하였어야 한다. A 사의 구매 절차에 의하면 B 사는 납품을 할 수 있는 유자격자 심사를 통과해야 하고, B 사의 설계/제작 과정을 사전에 확인하여야 한다.
더 큰 문제인식으로는, 최고 경영진은 항시 절차를 지키며 업무를 할 것을 지시해야 한다. 만약에 A 사 CEO가 담당 임원에게, "B 사가 모터 제어는 정말 잘하더라. 우리가 필요한 것을 해결할 수 있을 것 같은데, 그 회사는 기술전문가만 있지 품질문제는 있을 거야. 품질문제를 잘 짚어보면서 우리가 필요한 문제를 같이 풀어가 보게."라고 했더라면 문제가 없었을 것이다.

9.2
단순한 사항이지만 기록물 관리의 허점, 작업자의 자격관리, 기재사항의 실시간/주기적 기재 여부 및 오류를 사전에 점검하였어야 한다.

9.3
제조라인에 평소와는 다른 물량의 주문이나 여러 형태의 프로젝트 수주가 동시에 진행되면 적용요건의 상이한 점이나 차별화나 공정의 압박으로 인해 여러 가지 문제가 발생할 수 있다. 따라서 적정한 공급역량을 사전에 유지하기 어렵다면 이러한 취약점에 대해 분석하고 특별한 사전 점검 조치를 하는 것이 필요하다. 특히 장비나 인력의 중복 및 부족 우려에 대해서는 발주자에게 요청하여 적절한 보상계약을 받아내고 대신 주어진 납기를 철저히 준수하는 것이 두 회사 모두에게 도움이 된다.

9.4
단위공정에 대한 표준 일정을 준비하여 두고 이를 철저히 준수할 수 있는 여유 공정을 확보하도록 하여야 한다.

9.5
부품은 설계 산출물의 가장 기본인 부품목록(BOM)으로부터 시작할 수 있도록 한다. 즉, 설계시점부터 주민등록번호를 가지고 추적성이 확보될 수 있도록 한다. 그렇게 해야 부품 구매, 인수 검사, 창고 및 재고 관리, 품질기록, 부품변경, 기기검증, 납품 후 사후 관리 및 예비품 공급 등에도 유용하게 사용할 수 있다. 따라서 일관성 있게 적용할 수 있도록 번호 체계를 부여하고, 이를 부품에 식별할 수 있도록 해야 한다. 그리고 바코드, RFID 등 인식체계를 갖추는 것이 좋다.

9.6
시험자 자격관리는 IT 기술을 활용하여 교육 훈련 등의 개인 실적이 시스템적으로 자동 개정 확인이 될 수 있도록 개선한다.

9.7
절차서는 품질문서 작성요건에 따라 판정 기준을 명확하게 규정하고 누구나 식별할 수 있도록 기재하여야 한다. 시험 방법에 대해서도 시험자 및 검사자 모두 오독 또는 혼선이 없도록 손쉽게 작성되어야 한다. 그리고 절차서의 완벽한 검토 및 사전승인은 철저히 이행되어야 한다.

9.8

이해관계자들은 기기검증에 대한 기본취지를 제대로 이해하고 있어야 한다. 시제품을 통하여 단순히 시험데이터를 확보하고 합격 여부를 판정하는 것이 아니라 실제 설계와의 동일성을 입증할 수 있는 형태로 시제품이 제작되고 이 시제품을 검증해야 본품과의 동일성이 확보된다. 그리고 설계가 확정된 이후 기기검증을 착수해야 오류의 가능성을 최소화할 수 있다. 설계 변경이 진행될 경우에는 항시 시제품 및 기기검증 보고서와의 일치성을 검토승인과정에 확인해야 한다.

설계변경시에는 해당 기기검증을 위한 시험절차서를 동시에 개정하여 승인자/승인기관의 검토 및 승인을 거친 후 수행해야 유효성이 확보된다. 품질절차에도 해당 절차서의 승인현황(review status)을 사전 확인하도록 되어 있다. 또 현실적인 기기검증일정을 수립해야 한다. 설계확정, 부품구매, 인수검사, 시제품 제작 및 검증시험 단계별 소요기간 등의 영향을 구체적으로 산정해야 한다.

부품이 다른 계통에 공통으로 사용될 경우에는 해당 부품의 환경요건 및 사용 계통의 성능요건을 분석하여 이들을 모두 만족할 수 있도록 해야 한다. 개별 요건에 대하여 별도 식별하여 검증함으로써 통합검증이 되도록 하여야 한다.

9.9

다음의 개선조치를 하도록 한다.

① 도면 배포서 현황 작성 시에 이해관계자와 공유하도록 하고 실시간 개정이 필요하다.(설계자, 작업자, 품질검사자, 설계업체, 외함업체 등 이해관계자 모두 배포처 명시, 승인현황 표기)

② 제작도면에 외부 연계 치수 검사 항목을 명시할 것(인간공학 치수, 설치도면 치수, 설계변경 식별 등)

③ 공통 형상관리시스템 구축(경험사례 포함)

9.10

작동전압 값은 검출기의 절연 내력을 고려하여 계산 근거를 가지고 설계 사양서에 반영하여야 한다. 오차범위에서의 이상신호가 발생할 가능성에 대해서는 계통의 응답시간을 검토 확인 후 저 대역필터를 이용하면 오동작 신호를 제거할 수 있다.

9.11

자재 입고 시 다음과 같은 조치를 취해야 한다.

① 검사성적서의 진본 여부 확인

② 실제 시험한 결과가 표기되어 있는지 확인

③ 자재와 성적서의 상호 일치 여부를 반드시 사전에 확인하여 기록으로 남김.

9.12

① 위변조 품목의 공급으로 경제적 이익이 발생하기 때문

② 위변조 품목의 확인이 어려울 경우

③ 구매요건 및 기술사양의 내용이 미흡하거나 잘못 규정하였을 때

④ 구매요건을 확인하는 방법이나 기준이 부적절할 때

⑤ 긴급 보수나 교체가 요구될 때(즉, 스케줄 압박)

⑥ 공급자 검증을 다급하게 진행해야 할 때

⑦ 신뢰할 수 없거나 역량이 확인되지 않은 단독 업체로부터 구매할 때

⑧ 조직 내에 강력한 안전문화가 존재하지 않을 때

9.13
설계 자료를 통해 확인하기 어려운 특성의 경우에는 본 검사 이전에 사전 내전자파 측정을 통하여 주어진 요건의 수치를 충분히 포락하는지 확인한다. 역율 개선 부품을 사용하거나 고조파의 원인 부품을 설계 계획 단계에서 걸러내는 절차가 필요하다. 사용부품별 이력현황을 공유하거나 데이터베이스화하여 다른 용도로 사용할 경우에도 이를 통하여 확인 및 점검이 가능하도록 한다. 부품 이름, 파트 번호 등 추적이 가능한 식별정보를 반드시 포함하도록 한다.

9.14
구매 사양서에 주요 부품별로 공급사의 단종에 대한 책임사항 및 사전 통지 규정을 명시하도록 한다. 공급사의 제품 공급 유지기간을 공식 확인하고 계약 요건으로 명시하여 유지보수 계획을 수립할 수 있도록 한다.

9.15
벌크 자재나 단순 부품의 경우에는 실물을 사용하여 설계 요구사항을 확인해야 한다. 특히 조립자 등에게 작업지시를 할 경우에는 작업 표본을 만들어 두고 작업지시를 하는 것이 오류를 최소화하는 방법이 될 수 있다.

9.16
선행호기 자료를 참조 자료로 사용할 수 있다. 그러나 설계 완전성을 위해서는 품질문서 작성요령에 명시된 것과 같이 항시 설계 해석 또는 계산 근거를 가지고 있어야 한다. 근거가 없어 새로운 해석을 통해 설계변경을 입증할 경우에는 해석 근거 자료를 형상관리를 통하여 품질기록물로서 사용할 수 있도록 해야 한다. 모든 설계 기준 값에 대해서는 근거가 되는 계산시트(calculation sheet)를 가지고 있어야 한다. 설계변경이 발생하면 이를 기준으로 분석하여 설계값(마진포함)을 최종 결정할 수 있어야 한다.

Chapter 10

10.1

구조물이나 생산공정(절삭가공, 용접, 단조, 주조, ...)을 거쳐 생산되는 물건은 생산공정의 영향으로 조직이 변화되고 그 영향력이 생산된 제품에 남아 있게 되는데 이를 잔류응력이라고 하는 물리적인 양으로 나타낼 수 있다고 하겠다.
구조물은 부재를 사용하여 형상을 만들어 가는 과정에 이를 연결하기 위하여 용접을 하게 된다. 용접을 하면 용접변수, 재료의 고온 거동, 국부 가열, 냉각 수축 및 구속조건 등의 상호 작용에 의해 잔류응력이 발생하고 이로 인하여 구조물의 건전성과 수명에 영향을 미치게 된다. 이러한 용접잔류응력은 구조물의 사용기간 동안 일정한 크기로 유지되지 않고 하중 크기 및 하중반복수에 따라 이완되거나 재분포한다고 한다. 따라서 용접 구조물의 건전성 및 수명을 예측하기 위해서는 주요 인자인 잔류응력을 정확하게 평가하여야 하며 해석적인 방법이나 실험적인 방법에 의해 측정되어질 수 있다.

10.2

설비의 수명은 일반적으로 인허가 규제기관에서 허가하는 인허가수명(혹은 운영허가기간), 설비공급사가 발전소 설계 당시에 결정하는 설계수명, 건설을 위한 초기투자비를 회수하는 기간인 경제수명 등으로 분류할 수 있다. 인허가수명은 인허가체계와 밀접한 관계를 맺고 있어 일반적으로 정의하기는 어렵다. 설계수명은 발전소의 안전성과 성능기준을 만족하면서 운전 가능한 기간을 의미하며 설계단계에서의 기기공급자 및 설계사의 경험과 공학적 판단 그리고 Code & Standards 등 기술기준에 따른 설계해석의 기준이 된다.

10.3

형식시험, 운전경험, 해석적 방법, 조합된 방법

10.4

기기 검증 대상기기가 설계기준 사고 직전까지 운전한다고 할 때 수십 년 동안 주위 환경조건을 견뎌내어야 한다. 따라서 시편 및 시제품을 이를 모사한 최악의 열화(노화)상태로 만들어 둔 상태에서 기기검증을 수행하게 되면 설계 수명 마지막 시점에 사고가 발생하여도 안전기능을 제대로 작동함을 입증하게 된다.

10.5

온도, 압력, TID, 전기적특성치, 운전시간 및 지진동 등에 대하여 반영하여야 한다. 상세한 수치는 본문을 찾아보도록 하자.

10.6

온도, 습도, 염무, 모래, 먼지, 폭발성가스, 결빙, 우주선, 방사선, 압력, 기계적 영향, 전기적 영향, 내전자파, 진동, 지진 등 모든 요인을 고려하여야 한다.

10.7

크게 계획단계, 수행단계, 승인단계로 나누어 볼 수 있다. 수행단계에는 인수검사. 성능시험, 노화시험, 사고모의시험(내환경, 내전자파, 내진), 최종검사 단계를 거치게 된다. 완성된 보고서는 사업자 및 인허가책임기관의 승인과정을 거쳐서 제품 제작 및 납품을 수행할 수 있는 근거 서류가 된다.

10.8

① 열화 : 전기 기기는 동손 및 철손등으로 인하여 열이 발생하고 기기 외부로 방열하여 열평형이 이루어질 때까지 일정 온도까지 상승하게 된다. 이러한 온도 상승은 물리적 화학적 변화를 일으켜 재료가 열화하게 된다, 열화 과정은 일종의 화학적반응으로 간주되고 수식으로 해석된다.
② 전기열화(방전열화) : 전압이 인가되면 높은 전계에 의한 절연 조직내의 기체 및 액체의 전기적 파괴(부분방전)가 발생한다. 이는 고체 절연물의 주요 열화 요인이 된다.
③ 기계적열화 : 절연재료는 내전압재료인 동시에 구조적 재료로 역할하며 기계적 스트레스를 받는다.
④ 흡수 흡습에 의한 열화 : 물 분자는 수소결합의 능력이 있으며 극성기를 갖는 고분자 특히 OH, NH기 등을 갖는 고분자와 강한 친화력을 갖는다.
⑤ 화학약품에 의한 열화 : 고분자재료의 환경열화는 환경재(가스, 증기, 액체)가 고분자 재료 속으로 침투 확산하는 것이다.

10.9

활성화 에너지는 어떤 물질이 화학반응을 일으키는데 필요한 에너지를 말한다. 활성화 에너지가 작으면 외부환경의 변화에 쉽게 반응하여 전기재료의 노화가 빠르게 일어나게 된다.

10.10

생략(각자 생각해보기)

10.11

지진파속의 주파수 성분별 최대 가속도를 파악하기 위해서는 수학적 도구를 사용하여 분석하여야 한다. 이러한 방법 중 하나가 응답스펙트럼이다. 응답스펙트럼 해석은 복잡한 구조물을 단일자유도 시스템으로 가정하여 전체 구조물의 응답을 구하는 방법이다.
단일자유도 시스템이란 개별 진동 모드를 뜻한다. 고유주기마다 단일자유도 시스템의 최대응답을 스펙트럼의 형식으로 생성하는 과정과 이 결과를 조합하여 전체 구조물의 응답을 구하는 과정으로 이루어진다.

- 지진판 위에 여러 종류의 스프링이 있다고 가정하면 지진동에 의해 이 판이 흔들리면 이 추(스프링)들은 각자의 고유주기에 따라 흔들리게 된다.
- 이때 개별 추들의 시간에 따른 응답치를 측정한다.
- 이들 응답치중 주기별 최대치를 찾아 x축에 고유주기를 표기하고, y축에는 고유주기에 대응하는 응답의 최대치를 표시한다.
- 응답의 최대치를 연결하여 표시한 그래프는 단일자유도 시스템의 고유주기마다 최대응답을 대응시킨 것으로서 이것이 응답스펙트럼이 된다.

10.12

- 층응답스펙트럼(FRS) : 지진 발생후 내진시험 대상 기기가 위치한 장소로 파급되는 지진의 강도를 세 방향으로 표시한 것이다. 일반적으로 고객 결정 사항으로 제공되는 요건이다.
- 요구응답스펙트럼(RRS) : 기기공급자가 층응답스펙트럼에 근거하여 산출하며 내진 검증을 위한 지진시험장치의 가진을 위한 입력 조건이다. 기술표준은 모든 주파수 대역에 대하여 10% 마진을 주도록 요구하고 있다.
- 시험응답스펙트럼(TRS) : 요구응답스펙트럼으로 설정한 지진시험장치를 사용해 지진시험을 수행하면서 피 시험체의 각 부위에 실제 가속도계를 부착하여 측정한 값으로 시험대상기기에 가해지는 지진강도를 알 수 있으며 이를 통하여 각 부위 및 내부 부착물의 견고성을 평가할 수 있다.

10.13

TRS는 피시험체의 각 부위에 지진가속도계를 설치하고 내진 시험을 수행하여 구할 수 있다. IERS는 전체 시스템을 유한요소법으로 해석하고 지진 가속도계를 설치한 부위의 지진 가속도를 해석적 방법으로 구할 수 있으며 이를 TRS와 비교함으로써 해석모델의 상사성과 내진 안전성을 확인하기 위한 목적으로 사용된다.

10.14

① 시험시편 또는 시제품을 지진대에 설치하고 구조적 건전성을 확인한다.
② 공진탐색 시험을 수행한다.
③ OBE 시험을 수행한다.
④ SSE 시험을 수행한다.
⑤ 공진시험을 다시 시행한다.
⑥ 최종 검사를 수행한다.

10.15

발전소의 유지 보수를 위하여 필요한 부품이 생산중단(단종) 되었을 때 대체품을 사용하기 위한 검증 활동에 기기검증데이터를 활용하게 된다. 즉 일반 규격품의 필수 특성 확인 과정에 필요한 기존 부품의 기기검증 결과를 활용하여 대체품의 검증을 수행할 수 있다.

10.16

적합성 확인을 위하여 다음의 방법 중에서 선택하고 허용기준을 사전에 설정하여 문서화 한 이후에 평가를 수행한다. 적합성 평가는 결과를 문서화 하여야 하며 수용여부를 명확히 기재하여야 한다. 추적성이 유지될 수 있도록 절차서와 수행절차를 명확히 식별하고 관리하여야 한다.

① 방법1 : 특수시험 및 검사
② 방법2 : 일반규격품(상용제품) 공급자 실사
③ 방법3 : 제작 중 입회 검사
④ 방법4 : 공급자 및 공급품목의 이력평가
⑤ 조합방법 : 상기 중 두 가지 이상의 확인 방법 사용

10.17

물리적 형태, 성능, 의존성에 대하여 구분한다,

① 물리적 형태: 포맷(사양요건에 따른 포맷과의 일치성)
② 성능
- 출력의 정확도, 정밀도, 허용오차
- 기능성(안전기능, 알고리즘, 완전성, 정확성)
- 연계성(필수입력변수, 대역, 출력변수)

③ 의존성
- 개발과정의 품질활동 및 감독
- 정형화된 개발 과정
- 복잡도, 간결성
- 관련 코드, 표준 및 산업인증 만족 여부
- 내부 검토 및 확인(에절발생비율/ 수명주기별)
- 시험 가능성 및 완전성
- 훈련 성과 측정

10.18

산업별로 용어에 대한 의미와 정의가 차이가 있을 수 있다

일반적으로 어떠한 직업이나 채용에 있어 해당 분야에 대한 자격인증서(certification)까지 요구하거나 이를 위해 필요한 qualification 과정을 요구할 수 있다고 할 것이다.

산업 분야에서는 certification은 법으로 정해진 인증요구조건을 말하며 qualification은 품질인증(기기검증)에 사용된다고 할 수 있다. 따라서 합치 판단기준도 certification은 법으로 정하하게 되며 qualification은 사업별 품질요구사항(제품규격, 계약서)에 따라 정해지는 차이가 있다.

항공기 승인과 관련하여 여러 가지 용어(certfication, approval, qualification)를 사용하고 있으며 이들은 한글로 번역할 경우 모두 "인증" 이라는 단어로 해석할 수 있다.

- "certification"은 항공기, 엔진, 혹은 프로펠러에 그리고 일부 인증 당국에 따라서 보조전원 유닛에 적용하며 소프트웨어는 항공기 또는 장비의 일부로 간주한다.
- 임베디드 소프트웨어를 포함한 시스템과 장비는 인증의 한 부분으로 "승인"을 받아야 한다.
- 인증당국의 승인은 성공적인 시연 또는 수명주기에 대한 리뷰를 통하여 이루어진다.
- 인증기준은 신청자와 인증 당국이 협의하여 사전에 수립한 후 이에 맞게 공식적인 개발 과 인증 절차가 이루어진다.

부록 A

A.1 ~ A.10
답안 생략(각자 생각해보기)

A.11
조직의 독립성 및 권한 보장

A.12
품질보증계획서

A.13
설계계획서(design plan)

A.14
설계검토, 대체계산, 인증시험(qualification test)

A.15
검사자 및 감사자의 오독을 방지하기 위하여 정량적/정성적 판정기준은 구체적이고 명확하게 작성되어야 한다.

A.16
추적성이 확보되어야 한다. 위변조 품목이 아니며 적합한 판정기준에 의해 시험 및 검사가 적합하게 이루어졌음을 확인 및 입증할 수 있도록 품질 기록이 정확하게 기록되어야 한다. 초기 부품 인수부터 제작단계의 불출, 설치, 시험 및 납품 후에도 식별이 가능하도록 하여야 한다.

A.17
용접, 열처리, 비파괴검사, 단말처리, 도장, 세척, 운송 등

A.18
장비의 정밀도 유지, 사용범위 확인, 교정상태 유지, 장비 식별 상태 확인 등

A.19
시장상황을 우선적으로 고려한 의사결정 및 일정 독려

A.20
원가 구조의 세분화를 통한 이익 달성, 신흥국의 구매단가

A.21
수 %

A.22
무게중심의 이동으로 인한 기수의 상승

A.23

안전해석 보고서(Minor, Major, Hazardous , Catastrophic)를 찾아보고 설명

A.24

급격한 조종이 필요한 특수한 상황에 대한 대책 마련이 필요

A.25

조류충돌

A.26

사고해석 결과 설계변경 내용의 설명이 필요하지 않은 것으로 판단.

A.27

본 교재의 강의 내용인 최고 수준의 안전필수 시스템을 운용하는 관련 산업

A.28

경영 총괄 대신 기술총괄에게 직접 보고하는 체계로 개선함.

A.29

1) 강대국 국민 탑승 사고 시에는 엄청난 외교적 압박
2) 보잉과 다르게 회생할 수 없는 회사 부도 및 국가적 위기
3) 제도개선보다는 처벌과 정쟁거리 등
4) 우리나라에서는 항공기 관련 이런 사고는 일어날 수가 없다.