



2020

---

**부록 Y-1.**

**디지털인터페이스 ‘안전 및 보안’  
인증을 위한 기준**

**ANNEX Y-1.**

**Certification Guideline for  
Digital Interface – Safety and  
security**

---

**한 국 선 급**

## “디지털 인터페이스 ‘안전 및 보안’ 인증을 위한 기준”의 적용

1. 이 기준은 ICT 장비 제조자 및 시험기관의 제품개발, 시험 및 형식승인 업무를 지원하기 위해 작성 되었으며 별도로 명시하는 것을 제외하고 선박용 ICT 장비의 선급 형식승인 또는 정부를 대행한 형식승인(MED 등) 시 활용될 수 있습니다.
2. 이 기준은 인용 규격의 최신화 등에 따라 세부 내용이 변경 될 수 있으며 선급 형식승인 또는 정부를 대행한 형식승인에 활용하고자 하는 제조자는 반드시 우리 선급과 사전 협의 하에 인증 업무를 진행하여야 합니다. 사전 협의를 거치지 않은 제품 설계 및 시험 성적서 등에 대해서는 형식승인 과정에서 인정 되지 않을 수 있음을 유의하시기 바라며, 우리 선급이 위임을 받지 않은 정부를 대행한 형식승인 업무에 이 기준을 활용할 경우에 대해서는 우리 선급은 어떠한 책임의무도 없음을 인지하기 바랍니다.

**적용일자 : 2020년 11월 1일**

---

# 차 례

<b>제 1 장 총칙</b> .....	1
제 1 절 일반사항 .....	1
제 2 절 용어의정의 .....	4
<b>제 2 장 설계요건</b> .....	6
제 1 절 일반사항 .....	6
제 2 절 성능요구사항 .....	7
<b>제 3 장 형식시험</b> .....	12
제 1 절 일반사항 .....	12
제 2 절 성능시험 .....	14

## 제 1 장 총칙

### 제 1 절 일반사항

#### 101. 적용

1. 이 기준은 해상 전자 계측장치 및 항해통신장비에 사용되는 디지털인터페이스 장치의 시험 및 형식승인에 적용한다.
2. 해상 항해, 무선통신장비 및 시스템에 적용되는 디지털 인터페이스 장치의 승인은 적용되는 모든 기기와 연동하여 성능이 평가되어야 한다.
3. 이 기준에 포함되지 않은 사항에 대하여는 우리 선급이 적절하다고 인정하는 바에 따라 ISO, IEC, KS 또는 이와 동등 이상의 인정된 기준 또는 공학적인 검증에 따르며 이 기준 이외의 추가적인 요건이 요구될 수도 있다.
4. 해상 항해, 무선통신장비 및 시스템에 적용되는 디지털 인터페이스 장치의 승인은 해당 기기에 포함 또는 개별 승인될 수 있다.

#### 102. 인용 표준

IEC 61162-460 Ed2.0	2018	Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security
------------------------	------	--

#### 103. 승인 절차

1. **승인 신청자** 승인 신청자는 원칙적으로 승인 신청한 장비의 제조자로 한다. 다만, 우리 선급이 지장이 없다고 인정하는 경우에는 제품의 제조자가 아니라도 신청할 수 있다.
2. 형식승인은 다음과 같은 절차로 이뤄진다.
  - (1) 형식승인 신청서 접수  
아래 링크의 신청서가 103.3의 첨부자료 및 시험방안과 함께 전자파일 형태로 제출되어야 한다.  
(가) [형식승인 신청서](#)  
(나) [MED 승인 신청서](#)
  - (2) 자료검토  
제품 설계가 각 부록에서 요구하는 설계요건에 적합한지 검토되어야 한다.
  - (3) 시험대상 장비(EUT) 샘플링  
시험대상 장비는 시험방안을 포함한 자료검토가 완료된 후 검사원 입회하에 임의로 선정되어야 한다.
  - (4) 형식시험  
선정된 시험 샘플에 대하여 다음의 형식시험이 검사원 입회하에 실시되어야 한다. 단, 해당 장비의 시험분야에 대해 우리 선급의 인정을 받은 시험기관에서 시험을 할 경우 시험 일부 또는 전부에 대해 검사원 입회를 생략할 수 있다. ([KR 승인시험기관 목록](#))  
(가) 외관검사  
시험품의 외관, 구조 등을 확인하며 사양서와 일치하여야 한다.  
(나) 형식시험  
3장의 형식시험이 실시되어야 한다.
  - (5) 형식시험의 면제  
우리 선급이 인정하는 선급 또는 시험기관에서 시행한 시험성적서나 증명서를 가진 경우에는 형식시험의 일부 또는 전부를 생략할 수 있다.
  - (6) 공장조사  
공장조사는 신청된 제품의 제조공장이 안정된 작업 아래 품질이 균일한 제품을 제조할 수 있는가를 확인하기 위하여 실시하여야 하며 검사원 입회하에 아래 사항에 대해 조사하여야 한다.  
(가) 품질시스템 일반  
(a) 품질시스템의 확립 및 실행 상태

- (b) 고객 불만 처리절차의 수립 및 준수 여부
- (c) 직원의 교육 및 훈련 계획수립 및 실시 여부
- (나) 공정관리 및 품질관리
  - (a) 작업표준의 확립 및 준수 여부
  - (b) 품질관리 공정도의 확인 및 준수 여부
  - (c) 부적합품의 관리 및 시정조치
- (다) 제조 및 검사설비의 관리
  - (a) 설비의 관리기준 설정 및 준수 여부
  - (b) 검사장비의 규정 여부 및 교정 상태
- (라) 기타
  - (a) 적용규격 등 문서의 확보 여부 및 최신화 상태
  - (b) 선급검사업무에 대한 이해도
- (마) 상기 공장조사 항목의 조사방법 및 평가기준에 대하여는 우리 선급이 적절하다고 인정하는 바에 따른다.
- (7) 형식승인 증서 발행
 

형식시험 완료 후, 제출된 공장조사 보고서 및 형식시험 성적서가 양호하다고 인정되는 경우, 우리 선급은 형식승인 증서를 발행하여 신청자에게 송부하며 승인증서의 유효기간은 증서발행일로부터 5년 이내로 한다.
- (8) 형식승인 증서 갱신
 

우리 선급은 제조자로부터 승인증서 유효기간 연장신청이 있을 경우, 승인증서 유효기간 만료 후 3월의 범위 내에서 승인증서의 유효기간을 연장할 수 있다. 다만, 연장 종료 후 다시 발행하는 증서의 유효기간은 구증서의 유효기간 만료일의 익일부터 5년 이내로 한다.

### 3. 첨부자료

#### (1) 승인용 자료

- (가) 환경시험과 성능시험 방안(Test Program)(이 기준 2장 및 3장의 항목을 모두 포함하여 작성하되 EUT(시험편) 상세도 및 EUT 구성, 그리고 구체적 시험방법과 판정결과를 포함하여야 한다)
- (나) 관련 도면(조립단면도, 주요부품 등의 도면과 필요시 그 단면도로서, 각부 치수와 사용재료의 종류가 표기되고 또한 주요부품에 있어서는 부품별 형식명과 제조자 명이 표기될 것) 및 자료
  - (a) 제품사양 또는 기술매뉴얼
    - 시스템 사양
    - 정상 및 비정상 장비조작에서의 시스템 성능
    - 정상 및 비정상 조작보드에서의 사용설명서
    - 제어권 이전(transfer of control)
    - 예비(redundancy) 또는 복귀(reversionary) 모드
    - 시험장치
    - 고장감지(failure detection) 및 식별장치(자동 및 수동)
    - 자료보안
    - 접근 가능 목록
    - 사용자의 주의를 요구하는 특이사항
    - 시동, 복구, 유지보수, 정기적 시험, 데이터 백업, 소프트웨어 재가동, 고장위치 및 보수 등에 대한 절차
    - 프로토콜 정보
    - 입출력 장치의 상세
    - 전력공급의 상세
  - (b) 재료명세, 제품 카탈로그(브로슈어), 데이터자료, 계산서, 기능설명서, 부품목록 등과 같은 자료 (해당되는 경우)
  - (c) 적용분야 및 운전 제한사항
  - (d) 각 주요부품간의 상호작용을 나타내는 도면(해당되는 경우)
  - (e) 인쇄회로기판, 회로도(해당되는 경우)

- (f) 시스템 블록다이어그램(개별 구성부품, 입력 및 출력장치 및 상호접속장치의 배치)
- (g) 제어배선도, 결선도(해당되는 경우)
- (h) 제어순서도(해당되는 경우)
- (i) 설치될 소프트웨어의 이름, 버전 및 그 품질 보증 계획(해당되는 경우)
- (j) 운전 및 설치 매뉴얼(필요한 경우)
- (k) 제품표기 방법
- (다) 제품이 소프트웨어 기반의 제품일 경우 다음의 자료
  - (a) 품질계획
  - (b) 다음을 포함하는 소프트웨어의 상세
    - 각 구성부품에 설치하는 기본소프트웨어
    - 네트워크(network)의 노드(nodes)에 설치되는 통신 소프트웨어
    - 응용소프트웨어(프로그램 목록이 아님)
    - 시스템 설정 및 처리장치 구성을 위한 도구
  - (c) 다음을 포함하는 응용소프트웨어의 상세
    - 다른 시스템에 대한 독립성을 포함하여, 기능을 유지하는데 효과적인 시스템 모듈에 대한 정보
    - 각 모듈에 대하여 기능을 이해하는데 충분한 수준의 상세
    - 각각의 기능을 유지하는데 효과적인 소프트웨어 모듈사이의 관계
    - 소프트웨어 모듈 간의 데이터 및 제어 흐름
    - 우선순위 계획(priority schemes)을 포함하는 소프트웨어의 구성
    - 예비 시스템(redundant systems)에 대한 스위칭 방식
  - (d) 범위 및 한계(예상되는 장비조작 범위 및 경고/안전기능의 한계)의 상세
- (라) 사용자 인터페이스 자료
  - (a) 문서화된 설계의 상세(사용자 입력 및 출력장치의 도면, 치수, 그림 등을 포함하는 장치의 설계 및 배치가 실제 작업에 충분히 접근할 수 있는 수준으로 상세히 기술되어야 한다.)
  - (b) 다음을 포함하는 화면 기반 컴퓨터 다이얼로그의 상세
    - 각 입력장치에 배당된 기능
    - 각 화면의 상세
    - 메뉴 사용설명서
- (마) 형식승인 신청 전 형식시험을 완료한 경우 시험 조건과 결과가 포함된 시험 성적서 및 관련 자료 일체
- (바) 필요한 경우 전과 관련된 기능에 대하여는 FMEA 등 적절한 방법을 사용하여 고장영향분석(failure analysis)한 결과를 우리 선급에 제출하여야 한다.

## (2) 참고용 자료

- (가) 제품의 요목 및 시방서
  - (나) **제조공장의 개요**
    - (a) 회사명 및 주소, 공장의 연혁, 공장의 규모 및 배치도
    - (b) 승인 및 증서에 포함되어야 할 자회사를 포함한 조직 및 관리구조
  - (다) 공장조사를 실시하는 경우, 다음의 자료를 요구할 수 있다.
    - (a) 주요 제조설비
    - (b) 제조 공정도
    - (c) 사내규격 및 표준에 관한 자료
    - (d) 품질관리에 관한 자료
    - (e) 검사 및 시험 설비
    - (f) 주요 제조실적
    - (g) 외주공장 및 외주품 일람표
    - (h) 새로이 개발한 제품에 대하여는 개발을 위한 시험에 관한 자료
    - (i) 해당되는 경우, 비석면 검증을 위한 절차서 또는 문서(비석면 제품 선언서 등) (2017)
4. 전 2항에 불구하고 이미 우리 선급의 형식승인을 받은 실적이 있고, 그때 제출한 자료와 중복되는 것이 있는 경우, 형식시험 방안을 제외한 첨부자료의 일부를 생략할 수 있다.

## 제 2 절 용어의 정의

### 201. 450-노드 (450-Node)

IEC 61162-450 을 준수하며, 이 기준에 지정 된 추가 요구사항을 충족하는 장치를 말한다.

참고 1 : ONF 기능블록만 구현되는 노드도 포함한다.

### 202. 460-포워더 (460-Forwarder)

460-네트워크와 다른 460-네트워크를 포함한 다른 제어 네트워크간의 데이터 스트림을 안전하게 교환 할 수 있는 네트워크 인프라 장치를 말한다.

### 203. 460-게이트웨이 (460-Gateway)

460-네트워크와 제어되지 않은 네트워크를 연결하고, 이 기준에 지정된 안전 및 보안 요구 사항을 충족하는 네트워크 인프라 장치를 말한다.

### 204. 460-네트워크 (460-Network)

460-노드, 460-스위치, 460-포워더, 460-게이트웨이와 460-무선 게이트웨이 및 450-노드로 구성된 네트워크를 말한다.

### 205. 460-노드 (460-Node)

450-노드 요구 사항을 준수하고, 이 기준에 지정된 안전 및 보안 요구 사항을 충족하는 장치를 말한다.

### 206. 460-스위치 (460-Switch)

460-네트워크의 노드를 상호 연결하는 데 사용되며, 이 기준에 지정된 안전 및 보안 요구 사항을 충족하는 네트워크 인프라 장치를 말한다.

### 207. 460-무선 게이트웨이 (460-Wireless gateway)

460-네트워크 및 무선 네트워크를 연결하고, 이 기준에 지정된 안전 및 보안 요구 사항을 충족하는 네트워크 인프라 장치를 말한다.

### 208. 고급 암호화 표준 (advanced encryption standard, AES)

대입-치환 네트워크를 기반으로 하고 데이터 암호화 표준 파이스텔 (Feistel) 네트워크를 사용하지 않는 대칭키 블록 암호 알고리즘을 말한다.

### 209. 경보 (alarm)

선박의 안전한 항해를 유지하기 위하여 즉각적인 주의, 결정 및 필요한 경우 선교 팀의 조치가 필요한 상황이나 조건을 알리는 경고의 최우선 순위를 말한다.

### 210. 응용 계층 게이트웨이 (application level gateway)

460-네트워크를 다른 네트워크와 연결하고, 이 기준에 지정된 안전 및 보안 요구 사항을 충족하는 네트워크 인프라 장치를 말한다.

### 211. 백도어 (backdoor)

일반 인증을 우회하는 방법을 제공하여 컴퓨터에 원격 접근을 할 수 있도록 설치된 프로그램을 말한다.

### 212. 제어 네트워크 (controlled network)

네트워크가 연결된 네트워크 노드에 보안 위협을 초래하지 않는다는 기관에서 만족하는 문서화된 증거에 의해 운영되도록 설계된 모든 네트워크를 말한다.

참고 1 : 예를 들어 선급, 기국 또는 공인 기관(RO)에 의해 승인된 모든 IEC 61162-450 호환 네트워크

**213. B 범주 경고 (category B alert)**

중양 경고 관리 HMI에 표시 될 수 있는 정보 외에 의사 결정 지원을 위한 추가 정보가 필요하지 않은 경우의 경고를 말한다.

**214. 주의 (caution)**

가장 낮은 순위의 경고를 말한다.

참고 1 : “주의”는 경보 또는 경계 조건을 보장하지 않지만 상황이나 제공된 정보의 일반적인 고려에서 주의가 필요한 조건에 대한 선교 팀의 인식을 높인다.

**215. DMZ (demilitarized zone)**

조직의 외부 연결 서비스를 포함하고 더 크고 신뢰할 수 없는 네트워크(일반적으로 인터넷)에 노출하는 물리적 또는 논리적 하위 네트워크를 말한다.

**216. 서비스 거부 (denial of service, DoS)**

합법적인 사용자가 기계나 네트워크 리소스에 접근하지 못하도록 시도하는 것을 말한다.

**217. 플로우 (flow)**

다음 정보의 조합 : 소스 및 대상 MAC주소, 소스 및 대상 IP 주소, 프로토콜, 소스 및 대상 포트 번호를 말한다.

**218. 고장 모드 및 영향 분석 (failure mode and effects analysis, FMEA)**

잠재적인 고장모드, 원인 및 시스템 성능에 미치는 영향을 식별하기 위한 시스템 분석을 위하여 IEC 60812에 명기된 방법을 말한다.

**219. 고장 모드, 영향 및 중요도 분석 (failure mode, effects and criticality analysis, FMECA)**

고장 모드의 심각도를 평가하는 방법을 포함하는 IEC 60812에 명기된 분석 방법을 말한다.

참고 1 : FMECA는 중요도 분석을 포함함으로써 FMEA를 확장하며, 이 분석은 결과의 심각도에 대한 실패 모드 확률을 도표로 표시하는데 사용된다.

**220. 인터넷 제어 메시지 프로토콜 (internet control message protocol, ICMP)**

ISOC RFC 792에 따른 프로토콜을 말한다.

**221. 인터넷 그룹 관리 프로토콜 (internet group management protocol, IGMP)**

ISOC RFC 1121 (버전 1), ISOC RFC 2236 (버전 2) 및 ISOC RFC 4604 (버전 3)에 따른 프로토콜을 말한다.

**222. 손실률 (loss rate)**

장치의 입력 포트에서 측정된 총 패킷 수당 손실 패킷으로서 플로우의 수신 장치에 의한 데이터 손실 양을 말한다.

참고 1 : 손실률은 백분율로 표시된다.

**223. 악성 코드 (malware, malicious code)**

컴퓨터 작동을 방해하기 위하여 사용되거나 생성된 소프트웨어를 말한다.



**224. 최대 네트워크 부하 (maximum network load)**

단일 460-네트워크의 모든 네트워크 노드 및 네트워크 인프라 구성요소에서 발생하는 모든 트래픽의 최대 누적량을 말한다.

참고 1 : 네트워크 최대 부하는 초당 바이트로 측정한다. (B/s)

**225. 최대 전송 속도 (maximum transmission rate)**

네트워크 노드 또는 네트워크 인프라 장비에 의해 전송할 수 있는 초당 최대 바이트 수를 말한다.

**226. 다중 스페닝 트리 프로토콜 (multiple spanning tree protocol, MSTP)**

VLAN에 대한 RSTP의 확장인 IEEE 802.1Q에 따른 프로토콜을 말한다.

**227. 인접 MAC 주소 (neighbour MAC address)**

460-스위치에서 인지되고 SNMP(simple network management protocol)에 의해 보고되는 연결된 450-노드 또는 460-노드의 MAC 주소를 말한다.

**228. 네트워크 인프라 요소 (network infrastructure component)**

460 네트워크, 460 스위치, 460 포워드, 460 게이트웨이 및 460 무선 게이트웨이와 같이 다른 두 개의 네트워크에서 두 개 이상의 노드를 연결하는 장치를 말한다.

**229. 명목상의 네트워크 용량 (nominal network capacity)**

설정을 기반으로 하는 바이트 전송 속도로 네트워크 용량을 말한다.

참고 1 : 용량은 모든 트래픽을 라우팅하는 네트워크 스위치 중 가장 낮은 용량이다.

참고 2 : 장비의 기능을 지정하는데 사용된다.

**230. 기타 네트워크 기능 (other network function, ONF)**

IEC 61162-450에 명시한 대로 네트워크에 인터페이스 하는 기능 블록을 말한다.

참고 1 : ONF는 IEC 61162-450 네트워크 인프라를 공유할 수 있지만 IEC 61162-450에 정의된 프로토콜을 사용하지 않는 기능을 나타낸다.

**231. 고속 스페닝 트리 프로토콜 (rapid spanning tree protocol, RSTP)**

네트워크의 활성 토폴로지 계산 및 구성을 위한 IEEE802.1D에 따른 프로토콜을 말한다.

**232. 이동식 외부 데이터 소스 (removable external data source, REDS)**

콤팩트디스크(CD), 메모리 스틱 및 블루투스 등의 장치를 포함한 사용자 이동식 비 네트워크 데이터 소스를 말한다.

**233. 원격 네트워크 모니터링 (remote network monitoring)**

ISOC RFC 3577에 명시된 표준 모니터링 사양을 말한다.

**234. 링 형 토폴로지 (ring topology)**

각 노드가 두 개의 다른 노드에 직렬로 연결된 토폴로지를 말한다.

**235. RSA**

IEEE 1363에 명시된 공개키 암호 시스템을 말한다.

**236. 안전 (safety)**

시스템 고장, 잘못된 구성 및 오작동과 같은 의도하지 않은 위협으로부터 네트워크 보호를 말한다.

**237. 보안 영역 (secure area)**

물리적 입력 제어 또는 접근 지역에 대한 보호 또는 관찰이 가능한 물리적 지역이나 장벽이 정의된 영역을 말한다.

참고 1 : 콘솔 및 선장 또는 항해사의 감시에 의한 접근 관찰이 있는 선박의 항해 선교가 보안 영역의 예이다.

**238. 보안 (security)**

웜, 바이러스, 서비스 공격 거부, 불법 접근 등과 같은 의도적인 위협으로부터 네트워크 보호를 말한다.

**239. 단순 네트워크 관리 프로토콜 (simple network management protocol, SNMP)**

관리 정보를 전달하는데 사용되는 ISOC RFC 3411에 따른 프로토콜을 말한다.

**240. SNMP-트랩 (SNMP-Trap)**

ISOC RFC 1157, ISOC RFC 2021 및 ISOC RFC 2819에 따른 스위치에서 이벤트 및 통계 정보를 수집하는 방법을 말한다.

**241. 선박 네트워크 (shipborne network)**

선상의 장비 사이의 데이터 교환을 위한 선박의 데이터 네트워크 인프라를 말한다.

참고 1 : 이것은 위성 또는 다른 수단에 의해 지상국과 연결 되거나 연결되지 않을 수 있다.

**242. 스니핑 (sniffing)**

네트워크 트래픽에 대한 모니터링 및 분석을 말한다.

**243. 스트림 (stream)**

하나의 장치에서 동일한 프로토콜을 사용하는 모든 플로우의 조합을 말한다.

**244. 시스로그 (syslog)**

IEC 61162-450에서 외부 로깅에 사용하는 ISOC RFC 5424에 따른 프로토콜을 말한다.

**245. 시스템 통합자 (system integrator)**

통합 460 네트워크 기능에 대한 책임을 부담하는 개인 또는 조직을 말한다.

**246. 위협 (threat)**

시스템에 피해가 발생 할 수 있는 컴퓨터 보안 사고의 잠재적 원인을 말한다.

**247. 트래픽 (traffic)**

장치로부터 발생하는 모든 스트림들의 조합을 말한다.

**248. 비제어 네트워크 (uncontrolled network)**

IEC 61162-450 호환 네트워크, IEC 61162-460 호환 네트워크 또는 제어 네트워크가 아닌 데이터 네트워크를 말한다. (예 : 무선 네트워크)

**249. 가상 로컬 영역 네트워크 (virtual local area network, VLAN)**

브리지를 사용하여 상호 연결된 네트워크로 구성된 IEEE 802.1Q에 따른 네트워크를 말한다.

**250. 가상 사설 네트워크(망) (virtual private network)**

공유 또는 공용 네트워크에서 캡슐화, 암호화 및 인증된 링크를 통한 사설 네트워크의 확장을 말한다.

**251. 경계 (warning)**

주의를 요구하는 상황이나 상태를 알리는 것으로 선교 팀에 의해 즉각적인 주의나 행동을 요구하는 않는 것을 말한다.

참고 1 : 경고는 즉각적인 위협 상황은 아니지만 조치를 취하지 않거나 전향적 결정을 내리지 못했을 때 위협을 야기하는 상태의 변화를 선교에서 인지 할 수 있도록 하는 예방 조치로 표시된다.

**252. 무선 액세스 포인트 (wireless access point, wireless AP)**

Wi-Fi(와이파이), 블루투스 등 다양한 무선 기술을 통해 유선 장치에 무선 장치를 연결하는 장치를 말한다.

## 제 2 장 설계요건

### 제 1 절 일반사항

#### 101. 인용 표준

다음 문서의 전체 또는 일부는 이 기준서에서 참조되고 있으며 날짜가 기입된 문서는 그 버전이 적용되며, 날짜가 기입되지 않은 문서는 최신버전이 적용되어야 한다.

- |                    |      |   |
|--------------------|------|---|
| 1. IEC 60945       | -    | Maritime navigation and radiocommunication equipment and system<br>- General requirement<br>- Method of testing and required test results   |
| 2. IEC 61162-450   | 2018 | Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection  |
| 3. IEC 61924-2     | 2012 | Maritime navigation and radiocommunication equipment and systems - Integrated navigation systems - Part 2: Modular structure for INS - Operational and performance requirements, methods of testing and required test results |
| 4. IEC 62288       | 2014 | Maritime navigation and radiocommunication equipment and systems - Presentation of navigation-related information on shipborne navigational displays - General requirements, methods of testing and required test results     |
| 5. IEEE 802.1D     | 2004 | IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges  |
| 6. IEEE 802.1Q     | -    | IEEE Standard for Local and metropolitan area networks: Virtual Bridged Local Area Networks   |
| 7. ISOC. RFC 792   | -    | Internet Control Message Protocol (ICMP), Standard STD0005  |
| 8. ISOC. RFC 1112  | -    | Host Extensions for IP Multicasting   |
| 9. ISOC. RFC 1157  | -    | A Simple Network Management Protocol (SNMP)   |
| 10. ISOC. RFC 2021 | -    | Remote Network Monitoring Management Information Base   |
| 11. ISOC. RFC 2236 | -    | Internet Group Management Protocol, Version 2   |
| 12. ISOC. RFC 2819 | -    | Remote Network Monitoring Management Information Base   |
| 13. ISOC. RFC 3411 | -    | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks  |
| 14. ISOC. RFC 3577 | -    | Introduction to the RMON family of MIB modules  |
| 15. ISOC. RFC 4604 | -    | Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast   |
| 16. ISOC. RFC 5424 | -    | The Syslog Protocol   |

## 제 2 절 설계요구사항

### 201. 일반사항

- 이 기준은 IEC 61162-450을 기반으로 한다. 이 기준은 장비, 시스템 설계 및 작동에 대한 보다 엄격한 요건을 명시 한다.  
네트워크로의 외부 연결과 네트워크 내부 연결에 대한 위협으로부터 추가적인 보호를 이 기준에서는 제공한다. 접근이 통제 될 수 있는 배의 선교와 같은 안전한 구역에 네트워크가 물리적으로만 둘러싸인 경우, 외부 연결로부터 더 큰 위협이 발생한다. 보안구역에 적용 할 수 있는 요건은 IEC 61162-460 4.7에 제시되어 있다.
- 그림 1은 네트워크의 다른 부분과 구성 요소에 대해 이 기준의 요구 사항을 구현하는 네트워크를 보여준다. 회색 기호는 이 기준에 규정 된 장비를 나타낸다. 오각형은 이 기준에 명시된 논리적 소프트웨어 기능을 나타낸다. 빗금 친 기호는 460-네트워크에 포함 될 수 있는 IEC 61162-450호환장비를 나타낸다.

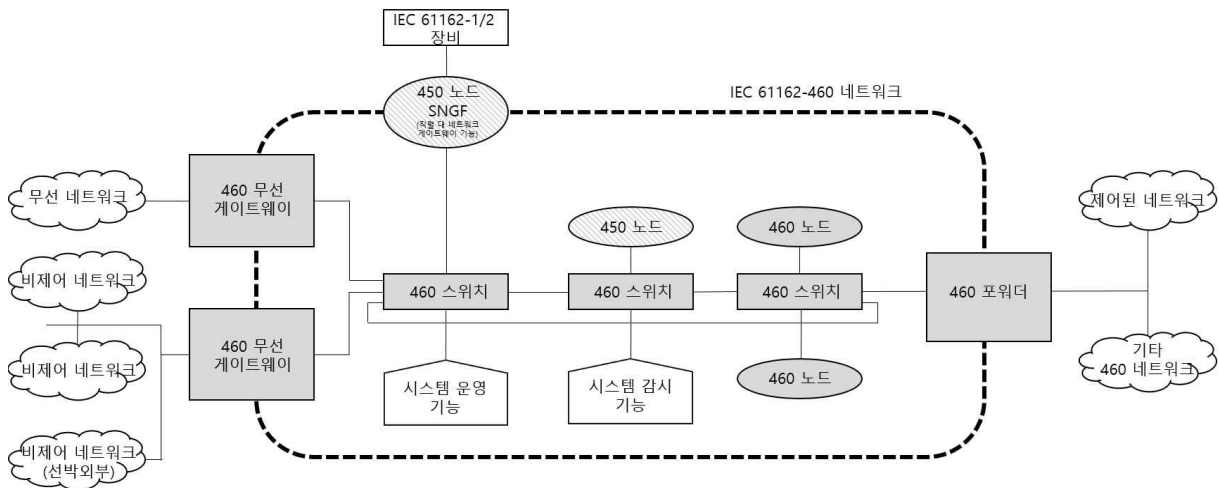


그림 1 - IEC 61162-460 요구사항 애플리케이션의 기능 개요

460-게이트웨이 사용에 대한 일부 예는 부속서 A에, 이 기준 사용에 대한 일부 예는 부속서 D에 명기 되어 이다.

### 202. 설계요구사항

이더넷 연결의 안전 및 보안 사항은 아래의 설계 요구사항을 만족하도록 설계 되어야 하며 승인 과정에서 자료검토에 의한 검증 또는 이 기준서 3장의 성능 시험을 통해 검증 되어야 한다.

No.	요구조건	IEC 61162-460	내용	비고
4.3 일반요구사항				
1	장비와 시스템 요구사항 Equipment and system requirements	4.3.1	- 460-네트워크를 구성하는 모든 장비는 IEC 60945에 명시된 항해 및 무선통신 장비에 대한 일반적인 요건을 충족해야 한다.  참고) IEC60945는 예를 들어 암호화 알고리즘과 보안기능을 개선하기 위해, 네트워크 인프라 장비의 펌웨어에 대한 정기적 업데이트를 지원하는 소프트웨어 유지보수가 선내에서 쉽게 수행 될 수 있도록 장비가 설계 되어야 한다는 요구사항을 포함하고 있다.	IEC 61162-460 (이하 생략) 10.3 참조

No.	요구조건	IEC 61162-460	내용	비고
			- 모든 네트워크 노드, 네트워크 인프라 구성요소 및 케이블은 IEC61162-450:2018 의 4 및 5항의 요건을 충족해야 한다.  - 네트워크 노드 및 네트워크 인프라 구성요소 제조자는 460-네트워크 에서 사용 중인 모든 MAC(매체 접근 제어, Media Access control) 주소 목록을 제공해야 한다. MAC 주소 목록은 라벨, 리스트 또는 이와 동등한 것이 될 수 있다.  참고) 부속서 F는 물리적인 장비주변의 다양한 기능들의 분포에 대한 개요를 포함하고 있다.	
2	물리적 구성 요구사항 Physical composition requirements	4.3.2	- 460-네트워크는 다음의 물리적인 네트워크 노드 또는 네트워크 인프라 구성요소로 구성되어야 한다.  • 450-노드, 즉 IEC 61162-450을 준수하며 4.4.1의 요건을 충족하는 네트워크 노드  • 460-노드, IEC 61162-450을 준수하며 4.4.2의 추가 요건을 충족하는 네트워크 노드  • 4.4.3 및 4.4.4 의 460-스위치 또는 460-포워드 요구사항을 준수하는 네트워크 인프라 구성요소  • 4.4.5의 460-게이트웨이 또는 460-무선 게이트웨이의 요구사항을 준수하는 응용 계층 게이트웨이.	
3	논리적 구성 요구사항 Logical composition requirements	4.3.3	- 460-네트워크는 460-네트워크의 모든 노드를 다루는 다음과 같은 논리적 시스템 기능 구성요소를 포함하여야 한다.  • SF(시스템 기능블록, IEC 61162-450 참조)또는 ONF (기타 네트워크 기능블록, IEC 61162-450 참조)가 4.5.1의 요구사항을 준수 할 수 있는 네트워크 모니터링 기능  • 4.5.2의 요구사항을 준수하는 SF 또는 ONF 가 될 수 있는 시스템 관리 기능.	
4.4 물리적 구성요소 요구사항				
4	450-노드 450-Node	4.4.1	- IEC 61162-450의 요건을 충족하는 네트워크 노드는 460-네트워크로 사용되기 위하여 다음의 요건 또한 충족하여야 한다.  • 외부 네트워크 또는 REDS와의 연결 금지  • IEC 61162-450:2018, 4.3.3.2에 정의된 것과 같이, 구현된 시스템로그	10.4 참조

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• 6.2.2.1에 설명된 바와 같이 제조자가 문서화한 데이터 출력 대역폭</li> <li>• 필요한 프로토콜 파라미터, 최소한 IP주소 및 포트번호를 포함하여 제조자가 지정한 ONF 서비스 구현</li> <li>• 제조사가 표시한 임시포트(사용되는 경우).</li> </ul>	
5	460-노드 460-Node	4.4.2	<p>- 다음 기능은 460-노드에서 구현해야 한다.</p> <ul style="list-style-type: none"> <li>• 5.1에 명시된 네트워크 트래픽 관리</li> <li>• 6.2.1, 6.2.2.1 및 6.2.4.1 에 명시된 보안 요구사항</li> <li>• 7.2에 명시된 이중화</li> <li>• 8.1.2.에 명시된 네트워크 모니터링</li> </ul> <p>다음 기능 중 하나가 460-노드에서 지원되는 경우, 다음에서 명시한 것과 같이 구현하여야 한다.</p> <ul style="list-style-type: none"> <li>• 외부 제어 네트워크와의 연결:                     <ul style="list-style-type: none"> <li>- 460-게이트웨이 또는 460-무선 게이트웨이 (6.3.5.1과 6.3.6 참조)를 통해 외부 제어 네트워크에서 수신된 올바른 IP주소와 포트번호를 포함한 모든 유효한 데이터 패킷을 460-노드의 응용 계층 소프트웨어에 의해 처리 및 점검 되어야 한다. 또는,</li> </ul> </li> </ul> <p>참고) MODBUS 또는 OPC(OLE for Process Control) 와 같은 네트워크 프로토콜에 대한 게이트웨이를 만드는데 사용 될 수 있다.</p> <ul style="list-style-type: none"> <li>- 만약 제어 네트워크와의 연결이 460-네트워크와 제어 네트워크 또는 다른 460-네트워크 간에 수정되지 않은 데이터그램(datagram)을 전달하기 위해 사용되는 경우, 이 전달은 460-포워더에 의해 처리 되어야 한다.</li> </ul> <ul style="list-style-type: none"> <li>• 6.2.3에 명시된 REDS에 대한 지원</li> <li>• 6.3.4에 명시된 비 제어 네트워크와의 직접 연결</li> <li>• 5.1에 명시된 VLAN 호환성</li> <li>• 필요한 프로토콜 파라미터, 최소한 IP주소 및 포트번호를 포함하여 제조자가 지정한 ONF 서비스 구현</li> <li>• 제조사가 표시한 임시포트(사용되는 경우).</li> </ul>	
6	460 스위치 460-Switch	4.4.3	<p>- 다음 기능은 460-네트워크 내의 장비를 연결하는 네트워크 인프라 구성요소에서 구현 되어야 한다.</p> <ul style="list-style-type: none"> <li>• 5.2에 명시 된 네트워크 트래픽 관리</li> <li>• 6.2.1, 6.2.2.2, 6.2.4 및 6.4에 명시된 보안 요구사항</li> </ul>	

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• 8.1.3에 명시된 네트워크 모니터링</li> <li>• 5.2.1에 명시된 VLAN 호환성(제공되는 경우)</li> </ul>	
7	460-포워더 460-Forwarder	4.4.4	<ul style="list-style-type: none"> <li>• 5.3에 명시된 네트워크 트래픽 관리</li> <li>• 6.2.1, 6.2.2.2, 6.2.4 및 6.4에 명시된 보안 요구사항</li> <li>• 8.1.4에 명시된 네트워크 모니터링</li> <li>• 5.3에 명시된 두개의 물리적 네트워크(제어 네트워크 및 다른 460 네트워크)를 논리적 네트워크로 결합하는 VLAN기능(제공되는 경우)</li> </ul>	
8	460-게이트웨이 및 460-무선 게이트웨이 460-Gateway and 460-Wireless gateway	4.4.5	<ul style="list-style-type: none"> <li>- 비 제어 네트워크에 대한 연결은 6.3.5에 명시된 460-게이트웨이 또는 6.3.6에 명시된 460-무선 게이트웨이에 대한 요구사항을 충족하는 게이트웨이로 보호 되어야 한다. 6.2, 6.3 및 6.4에 명시된 보안 요구사항이 구현 되어야 한다.</li> </ul>	
4.5 논리적 구성요소 요구사항				
9	네트워크 모니터링 기능 Network monitoring function	4.5.1	<ul style="list-style-type: none"> <li>- 네트워크 모니터링 기능은 다음 기능을 수행해야 한다.</li> <li>• 8.2.2에 명시된 네트워크 부하</li> <li>• 8.2.3에 명시된 네트워크 이중화</li> <li>• 8.2.4.1에 명시된 네트워크 토폴로지</li> <li>• 8.2.4.2에 명시된 SFI 충돌 탐지</li> </ul>	
10	시스템 관리 기능 System management function	4.5.2	<ul style="list-style-type: none"> <li>- 시스템 관리 기능은 다음 기능을 수행해야 한다.</li> <li>• 모든 네트워크 인프라 구성요소 정보를 유지하고 요청 시 이를 장비에 복원 - 관리기능은 최소한 이전의 구성기록을 유지해야 한다.</li> <li>• 460-스위치, 460-포워더, 460-게이트웨이 및 460-무선 게이트웨이에서 자동 또는 수동으로 구성 정보를 저장 및 복원</li> <li>• 인프라 구성 변경- 이 기능은 MAC 만 특정 포트에 연결 할 수 있는 460-스위치처럼 새로운 MAC 주소를 가진 장비를 교환 하는데 필요 함.</li> <li>- 시스템 관리 기능은 이중으로 사용 할 수 있어야 한다.</li> </ul>	10.12.2 참조
4.6 시스템 문서화 요구사항				
11	시스템 문서화 요구사항 System documentation requirements	4.6	<ul style="list-style-type: none"> <li>- 460-네트워크의 시스템 통합자는 네트워크 토폴로지와 그 기능 및 장치에 대한 문서를 제공해야 한다.</li> <li>- 460-네트워크의 시스템 통합자는 460-네트워크가 4.3.2에 나열된 장비만 포함되어 있음을 보여주는 문서를 제공해야 한다. 5.4 참조</li> </ul>	10.12.3.1 참조



No.	요구조건	IEC 61162-460	내용	비고
4.7 보안영역 요구사항				
12	보안영역 요구사항 Secure area requirements	4.7	- 460-스위치 및 460-포워더는 6.2.4.2에 설명된 바와 같이 보안 영역에서 MAC 주소 승인 요건을 비활성화 할 수 있다  - 460-스위치 및 460-포워더에 대한 문서에는 보안 영역에 설치할 때 보안을 완화할 수 있는 기능에 대한 설명과 보안 영역에 대한 설명이 포함되어야 한다.	10.12.3.1 참조
5 네트워크 트래픽 관리 요구사항				
13	460-노드 요구사항 460-Node requirements	5.1	- 460-노드는 네트워크 트래픽 관리 요건을 충족하기 위해 다음 사항을 준수해야 한다.  • 모든 트래픽은 IEC 61162-450을 준수하는 데이터 유형 (예: IEC 61162-1 센텐스 전송, 이진(binary) 파일 트래픽 또는 ONF) 중 하나로 지정되어야 한다.  참고 1) 차트 업데이트는 ONF의 예시이다.  • 장치의 최대 작동 데이터 출력은 제조자가 지정한 기간 동안 평균 초당 바이트로 선언되어야 한다.  참고 2) 지정된 기간은 데이터 출력의 특성에 따라 달라지며, 네트워크 트래픽 관리 목적에 적합하도록 선택된다.  • 장치의 동작은 최대 입력 데이터 속도가 초과될 때를 제조자가 지정해야 한다. 입력데이터 속도는 모든 프로토콜별 오버헤드를 포함하여 네트워크 라인에서 사용할 수 있는 초당 바이트로 표시되어야 한다.  • 노드에 의해 지정된 데이터만 노드에 의해 처리되어야 한다.  • 장치는 10분 동안 최대 0.1%의 패킷 입력 손실률로 정상 동작을 지속할 수 있어야 한다.  참고 3) 정상 동작은 인터페이스에서 어떤 것이 손실되었을 경우에도 살아남는 능력을 포함한다. 그러한 손실에 대한 정상적인 반응은 아무것도 손실되지 않은 것처럼 계속 (즉, 아무 영향 없이 계속할 수 있는 충분한 정보가 있는 경우)되거나 손실을 기반으로 표시 및 경고를 생성하는 것이다  - VLAN이 제공되면, 모든 VLAN 트래픽이 최대 전송속도에 포함되어야 한다.	10.5.1 참조

No.	요구조건	IEC 61162-460	내용	비고
			참고 4) 예를 들어, VLAN 은 별도의 세그먼트를 만드는 데 사용 된다.	
			5.2 460-스위치 요구사항	
14	리소스 할당 Resource allocation	5.2.1	<p>- 리소스 할당을 위해서는 다음 사항이 필요 하다.</p> <ul style="list-style-type: none"> <li>• 인터페이스 식별자, MAC 주소 또는 IP주소, 프로토콜 번호 및 포트번호 또는 포트번호 범위의 조합으로 식별되는 스트림 또는 네트워크 플로우를 구성하는 수단</li> <li>• 등록된 각 스트림에 대해 네트워크 대역폭 리소스를 할당하는 수단</li> <li>• 들어오고 나가는 모든 트래픽은 등록 되어야 한다.</li> <li>• 등록되지 않은 모든 트래픽은 차단되어야 한다.</li> <li>• 460-스위치에 할당된 대역폭의 양은 스위치에 연결된 네트워크에 할당된 각 트래픽 클래스의 모든 정상 트래픽 볼륨의 합계보다 커야 한다.</li> <li>• 450-노드 및 460-노드에 대한 인터페이스당 트래픽 총량은 해당 인터페이스의 네트워크 설계 값으로 제한되어야 한다. 네트워크 설계치는 포트의 물리적 용량의 0~50% 사이에서 선택 할 수 있어야 한다.</li> <li>• VLAN이 제공되는 경우, 인터페이스별로 가상 네트워크(VLAN)구성 방법이 제공 되어야 한다.</li> <li>• VLAN이 제공되는 경우, VLAN 프로토콜 IEEE 802.1Q가 지원 되어야 한다.</li> <li>• IEC 61162-450:2018 에서 요구 한 대로 IGMP 스누핑(snooping)을 통해 멀티캐스트 트래픽을 필터링하는 수단</li> <li>• IGMP 멤버십 쿼리를 다른 460-스위치, 460-포워더, 460-노드 및 450-노드로 전송하는 수단</li> </ul>	10.6.1 참조
15	루프 방지 loop prevention	5.2.2	<p>- 스위치는 예를 들어 RSTP, MSTP와 같은 루프 방지 메커니즘을 제공해야 한다. 네트워크 토폴로지 및 스위치의 구성은 5초 이내에 수렴을 지원해야 한다.</p> <p>참고) 네트워크에 루프가 있을 때 트래픽은 절대 종료 되지 않는다. 이는 네트워크 트래픽을 크게 증가 시킨다. 이 문제는 멀티캐스팅 트래픽에 스위치에 의해 증가되면 심각</p>	10.6.2 참조

No.	요구조건	IEC 61162-460	내용	비고
			<p>해 진다. 네트워크 루프는 네트워크 구성 오류로 인해 발생 할 수 있다. 또한, 네트워크 토폴로지(즉, 망사형 네트워크 토폴로지)나 네트워크 이중화에 의해 대상에 대한 경로가 여러 개 있을 때 발생한다.</p> <p>- RSTP 가 제공될 경우, 요구사항은 다음과 같다.</p> <ul style="list-style-type: none"> <li>• IEEE 802.1D-2004에 따른 RSTP 프로토콜 버전이 지원 되어야 한다.</li> <li>• 460-스위치는 모든 인터페이스에서 RSTP를 활성화 할 수 있는 기능을 제공해야 한다.</li> </ul>	
5.3 460-포워더 요구사항				
16	트래픽 분리 traffic separation	5.3.1	<p>- 트래픽 분리에 필요한 사항은 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 트래픽의 전체 또는 하위 일부 전송을 구성하는 수단</li> <li>• 최대 트래픽 플로우에 맞게 구성하는 수단</li> <li>• VLAN이 제공되는 경우, 각 인터페이스별로 가상 네트워크(VLAN)를 구성하는 수단이 제공되어야 한다.</li> <li>• VLAN이 제공되는 경우, VLAN 프로토콜 IEEE 802.1Q 가 지원되어야 한다.</li> <li>• IEC 61162-450:2018 에서 요구한 멀티캐스트 트래픽 IGMP 스누핑을 필터링 하는 수단</li> <li>• IGMP 멤버십 쿼리를 다른 460-스위치, 460-포워더, 460-노드와 450-노드로 전송하는 수단</li> </ul>	10.7.1 참조
17	리소스 할당 resource allocation	5.3.2	<p>- 리소스 할당의 요구사항은 다음과 같다:</p> <ul style="list-style-type: none"> <li>• 460-포워더는 포워더에 연결 된 네트워크에 할당된 각 트래픽 클래스의 모든 트래픽 볼륨의 합계 이상의 용량을 가져야 한다.</li> <li>• 460-포워더는 최대 트래픽 플로우에 대해 구성 할 수 있어야 한다.</li> <li>• 인터페이스 식별자, MAC 주소 또는 IP주소, 프로토콜 번호 및 포트 번호의 조합으로 식별되는 스트림 또는 네트워크 플로우를 구성하는 수단이 제공 되어야 한다.</li> <li>• 등록된 모든 스트림에 네트워크 리소스를 할당하는 수단이 제공 되어야 한다.</li> </ul>	

No.	요구조건	IEC 61162-460	내용	비고																											
18	트래픽 우선순위 지정 Traffic prioritization	5.3.3	<p>• 각 가상 네트워크에 리소스를 할당 할 수 있는 수단이 제공 되어야 한다(제공되는 경우).</p> <p>- 트래픽의 전부 또는 일부는 하나의 460-네트워크에서 제어 네트워크로의 트래픽 전송을 제어하기 위해 우선순위를 지정할 수 있다. 기본적으로 모든 트래픽은 기본 우선순위에 대한 값은 0 이어야 한다. 우선순위는 VLAN의 IP DSCP(차등화 서비스코드 포인트) 또는 CoS(서비스 클래스)가 제공하는 경우 제공될 수 있다. 0(=000)이 가장 낮고 7(=111)이 가장 높은 8가지 우선순위가 있다.</p> <p>- 각 패킷의 우선순위는 트래픽 유형에 따라 제공된다. 우선순위 정보는 IP DSCP 필드 또는 CoS 필드의 우선순위에 주어진다. 표1은 트래픽 유형과 VLAN 의 IP DSCP 및 Cos 에 지정된 트래픽 우선순위 지정 간의 관계를 보여주는 예시 이다.</p> <p>표1 - CoS 및 DSCP 를 통한 트래픽 우선순위 지정</p> <table border="1" data-bbox="646 943 1209 1227"> <thead> <tr> <th>CoS 값</th> <th>DSCP 값</th> <th>IEC 61162-450 기반 트래픽 유형</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>네트워크 제어 및 관리 트래픽을 제외한 ONF에서 제공하는 데이터</td> </tr> <tr> <td>1</td> <td>1000</td> <td>PROP, USR1 ~ USR8</td> </tr> <tr> <td>10</td> <td>10000</td> <td>MISC, 단순 이진 이미지</td> </tr> <tr> <td>11</td> <td>11000</td> <td>VDRD, TIME</td> </tr> <tr> <td>100</td> <td>100000</td> <td>RCOM, 재전송 가능한 이진 이미지</td> </tr> <tr> <td>101</td> <td>101000</td> <td>TGTD, SATD, NAVD</td> </tr> <tr> <td>110</td> <td>110000</td> <td>예약됨(reserved)</td> </tr> <tr> <td>111</td> <td>111000</td> <td>네트워크 제어 및 관리 트래픽</td> </tr> </tbody> </table> <p>- 460-포워더에서 트래픽 우선순위를 위해 다음의 수단이 제공되어야 한다.</p> <p>a) 우선순위에 기반 하여 낮은 우선순위 트래픽의 드롭을 처리하는 수단</p> <p>b) 각 물리적 포트별로 전송되는 트래픽 양이 회선의 물리적 용량의 50%를 초과하거나 460-노드 또는 450-노드의 최대입력 데이터 전송속도 용량을 초과하는 경우 드롭처리 하는 것을 의미한다. 트래픽 우선순위는 트래픽이 회선의 물리적 용량의 50% 미만 이거나, 460-노드 또는 450-노드의 설정된 최대 입력 데이터 전송속도 용량 미만일 때 까지 낮은 우선순위 트래픽을 감소시키는데 사용 되어야 한다.</p> <p>참고 1) 드롭처리 방법의 예는 우선순위가 다른 트래픽의 양을 할당 할 수 있는 설정 방법 이다.</p> <p>c) 전송되는 트래픽양이 스위치의 우선순위에 대해 설정된 최대값의 100%를 초과할 때까지 각 우선순위에서 무 손실 트래픽을 계속하는 것을 의미한다.</p>	CoS 값	DSCP 값	IEC 61162-450 기반 트래픽 유형	0	0	네트워크 제어 및 관리 트래픽을 제외한 ONF에서 제공하는 데이터	1	1000	PROP, USR1 ~ USR8	10	10000	MISC, 단순 이진 이미지	11	11000	VDRD, TIME	100	100000	RCOM, 재전송 가능한 이진 이미지	101	101000	TGTD, SATD, NAVD	110	110000	예약됨(reserved)	111	111000	네트워크 제어 및 관리 트래픽	
CoS 값	DSCP 값	IEC 61162-450 기반 트래픽 유형																													
0	0	네트워크 제어 및 관리 트래픽을 제외한 ONF에서 제공하는 데이터																													
1	1000	PROP, USR1 ~ USR8																													
10	10000	MISC, 단순 이진 이미지																													
11	11000	VDRD, TIME																													
100	100000	RCOM, 재전송 가능한 이진 이미지																													
101	101000	TGTD, SATD, NAVD																													
110	110000	예약됨(reserved)																													
111	111000	네트워크 제어 및 관리 트래픽																													

No.	요구조건	IEC 61162-460	내용	비고
			d) 드롭이 사용된 30초의 각 기간 동안 시스로그로 드롭 사용을 보고하거나 드롭 사용에 대한 SNMP 트랩방법 (즉, RMON 경고를 요청)에 응답하는 것을 의미한다. (8.2.2 참조).  참고 2) 예를 들어, SNMP-트랩방법 쿼리를 사용하여 460-포워더에 드롭 사용에 대한 네트워크 모니터링 기능	
5.4 시스템 설계 요구사항				
19	문서화 Documentation	5.4.1	- 다음 정보를 포함하는 문서가 제공되어야 한다.  <ul style="list-style-type: none"> <li>460-네트워크 트래픽 플로우 분석 및 네트워크 토폴로지 정보</li> <li>모든 스위치와 스위치, 포워더 및 게이트웨이 사이의 네트워크 트래픽 총량 및 460-네트워크에 대한 모든 트래픽의 평균 부하를 지정하는 문서</li> <li>각 460-포워더에서 하나의 460-네트워크에서 다른 460-네트워크로 전송된 최대 트래픽 플로우</li> <li>각 460-포워더에서 각 트래픽 유형의 우선순위 지정 4.6 참조</li> </ul>	10.12.3.2 참조
20	트래픽 Traffic	5.4.2	- 460-네트워크를 위한 시스템 설계는 다음 사항을 준수해야 한다.  <ul style="list-style-type: none"> <li>최대 설계 네트워크 부하가 명목상의 네트워크 용량을 초과해서는 안 된다</li> <li>460-네트워크의 모든 트래픽의 평균 부하가 1초 동안 계획된 명목상의 네트워크 용량의 95%를 초과해서는 안 되며, 10초 동안 계획된 명목상의 네트워크 용량의 80%를 초과해서는 안 된다.</li> </ul>	10.12.3.3 참조
21	보안영역과 비 보안영역간의 연결 Connections between secure and non-secure areas	5.4.3	- 보안영역에 설치된 460-네트워크와 비 보안영역에 설치된 460-네트워크 사이의 연결은 460-포워더를 사용해서 설정해야 한다. (그림 1 참조)	10.12.3.9 참조
6. 보안 요구사항				
6.1 보안 시나리오				
22	위협시나리오 Threat scenarios	6.1.1	- 그림 1에 설명된 네트워크 토폴로지의 예시와 같이, 460-네트워크는 내부적으로 450-노드에 의해 그리고 외부적으로는 다른 선박 장비나 선박 외부 (off-ship) 장비와 같은 비 제어 네트워크로부터 위협을 받는다. 따라서 460-네트워크는 내부 위협뿐 아니라 외부위협으로부터도 보호가 요구된다.	

No.	요구조건	IEC 61162-460	내용	비고
23	내부 위협 Internal threat	6.1.2	<p>- 네트워크에서 발생 할 수 있는 시나리오는 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 악성코드(malware)에 감염된 노트북과 같은 460-네트워크의 다른 장비에서 악성코드 복제</li> <li>• 예를 들어, (인가 또는 비인가) 유지보수 및 지원 관련하여 460-네트워크 내에서 사용 중인 손상된 대용량 저장장치(예:USB 플래시 드라이브) 또는 이동식 미디어 드라이브(CD/DVD)로 인한 감염</li> <li>• 시스템 권한을 얻기 위해 장비 중 하나에 백도어 설치, 그다음 다른 장비가 공격 받음</li> <li>• 실수(오동작)에 의한 시스템 파일 삭제 또는 구성 파일의 변경</li> <li>• 장비의 정상 작동을 막는 불법 접근</li> <li>• 장비의 정상 작동을 막는 잘못된 데이터 생성</li> <li>• 460-네트워크로 쉽게 전파되는 제어 네트워크의 보안 위협</li> <li>• 460-네트워크로 쉽게 전파되는 다른 460-네트워크의 보안 위협</li> <li>• 대량의 브로드캐스트 트래픽과 ICMP 및 IGMP 패킷으로 인한 네트워크 서비스 중단.</li> </ul> <p>- 내부 위협에 대한 보안 요건은 6.2에 설명되어 있다</p>	
24	외부 위협 External threat	6.1.3	<p>- 외부 네트워크에서 발생 할 수 있는 시나리오는 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 보안 되지 않은 무선 네트워크로부터의 위협</li> <li>• 460-네트워크 장비의 일부가 다른 선박 네트워크의 악성코드에 의해 감염</li> <li>• 선박 네트워크 사용자가 460-네트워크에 원격 로그인하여 중요한 파일을 삭제 하거나 구성을 변경하는 실수(오동작)</li> <li>• 선박 장비에 백도어를 설치하여 공격용으로 사용; 스위치 또는 라우터와 같은 네트워크 인프라를 통해</li> </ul>	

No.	요구조건	IEC 61162-460	내용	비고
			<p>장비에 대한 직접 공격</p> <ul style="list-style-type: none"> <li>• 스캐닝 공격 - 공격자는 먼저 포트를 검색하여 공격용 포트를 찾는다. 포트가 발견되면, 포트로 서비스를 스캔한다. 예를 들어, 웹서비스를 위한 포트 번호 80이 열려 있는 경우, 공격자는 웹서버 유형 및 버전 정보를 수집한다.</li> <li>• 다른 선박 네트워크와 같은 비 제어 네트워크를 통해 460-네트워크에 대한 간접 공격</li> <li>• 외부장치 및 시스템과 통신하는 동안 데이터 스니핑(sniffing) 및 수정공격 - 460-네트워크 장비가 선박 외부(off-ship) 네트워크 시스템과 통신할 때, 공격은 스니핑을 통해 데이터를 추출하고 수정한다. 예를 들어, 항해경로 정보는 해적과 테러리스트에 의해 노출되고 수정 될 수 있다</li> <li>• 460-네트워크로 들어오는 과도한 데이터 트래픽 및 SYN 플로딩(flooding) 공격을 포함한 프로토콜 기능 공격.</li> </ul> <p>- 외부위협에 대한 보안 요건은 6.3에 설명되어 있다.</p>	
6.2 내부 보안 요구사항				
25	일반사항 General	6.2.1	<p>- 460-노드, 460-스위치 및 460-포워더는 무선 LAN 인터페이스 및 무선 액세스 포인트(AP) 기능을 사용하지 않아야 한다.</p> <p>- 모든 VLAN 터널링 프로토콜은 460-노드, 460-스위치 및 460-포워더에서 비활성화 되어야 한다.</p>	10.5.2.1, 10.6.3.1, 10.7.4.1 참조
6.2.2 서비스 보호 거부				
26	460-노드 460-node	6.2.2.1	<p>- 장치에 대한 최대 작동 입력 및 출력 대역폭은 제조사에서 지정한 기간 동안 평균으로 선언해야 한다.</p> <p>- 이더넷 포트에서 수신되는 과도한 수신 트래픽 하에서 노드의 정상 작동을 보장하기 위한 수단이 제공되어야 한다.</p>	10.5.2.2 참조
26	460-스위치, 460-포워더, 460-게이트웨이 및 460 - 무선 게이트웨이 460-Switch, 460-Forwarder, 460-Gateway and	6.2.2.2	<p>- ICMP 및 IGMP 프로토콜을 사용하는 DoS 공격으로부터 보호해야 한다. 추가 DoS 예방 방법을 제공될 수 있다.</p>	10.6.3.2, 10.7.4.1 10.8.1 참조

No.	요구조건	IEC 61162-460	내용	비고
	460-Wireless gateway			
6.2.3 REDS 보안				
27	물리적 보호 Physical protection	6.2.3.1	<ul style="list-style-type: none"> <li>- 연결 포인트(USB 포트, 디스크드라이브 등) 수는 시스템 작동과 시스템 수명유지 및 지원에 필요한 최소값으로 제한되어야 한다.</li> <li>- 다른 모든 포인트는 도구나 키가 없는 사용자가 쉽게 접근할 수 없도록 물리적으로 차단해야 한다.</li> </ul>	10.5.2.3 참조
28	운영적 보호 Operational protection	6.2.3.2	<ul style="list-style-type: none"> <li>- 연결 포인트는 데이터 소스에 대한 연결만 허용하도록 작동을 제한해야 한다.</li> <li>- USB기반 장치의 경우, REDS에는 USB 장치 클래스 08h (USB 대용량 저장장치)만 허용된다. 다른 장치의 경우, 제조자는 사용된 기술과 연결 포인트가 데이터 소스로만 연결을 제한하는 요건을 충족하는 방법에 대한 정보를 제공해야 한다.</li> <li>- 키보드, 프린터 등에 사용되는 USB 연결 포인트는 기기 설정에서 도구(Tool) 또는 키(Key) 또는 암호보호(사용 안함 / 사용 함)를 통해 사용자가 쉽게 접근할 수 없도록 차단해야 한다.</li> </ul>	
29	실행프로그램 파일검증 Executable program file verification	6.2.3.3	<ul style="list-style-type: none"> <li>- USB 자동실행을 포함하여 REDS의 460노드에서 모든 자동실행은 금지되어야 한다.</li> <li>- REDS 에서 모든 형식의 파일을 수동 실행은 REDS의 실행 가능한 콘텐츠에 접근하기 위한 인증을 통과한 후에만 가능하다. 수동 실행은 디지털 서명 또는 특수키를 사용하여 실행 전에 확인된 파일에 대해서만 가능해야 한다.</li> </ul> <p>참고 1) 디지털 서명 방법은 개인/공용키 쌍을 기반으로 한다. 일반적으로 SHA-2 군(family) (MD5 및 SHA-1의 사용이 중지 됨, ISO/IEC 10118-3 참조)와 같은 해쉬 함수(Hash function)가 사용된다.</p> <p>참고 2) 특수키는 지정된 기능을 사용하여 전달된 데이터에서 계산한 값일 수 있으며, 알려진 예상 값과 신뢰할 수 있는 소스 또는 송신자가 지정하는 기능과 값과 비교한 것이 될 수 있다.</p>	
30	실행 불가능 데이터 검증 Non-executable program file verification	6.2.3.4	<ul style="list-style-type: none"> <li>- REDS의 실행 불가능한 모든 데이터는 장비에서 사용하기 전에 확인되어야 한다.</li> </ul>	
6.2.4 접근 제어				
31	장치 접근 제어 Device access control	6.2.4.1	<ul style="list-style-type: none"> <li>- 460-노드, 460-스위치, 460-포워더, 460-게이트웨이 및 460-무선 게이트웨이 장비의 구성을 변경하기 위한 접근은 사용자 인증에 따라야 한다.</li> </ul>	10.5.2.4, 10.6.3.3, 10.7.4.3,



No.	요구조건	IEC 61162-460	내용	비고
			<p>- 사용자 인증에는 로그인 정보가 제공되어야 한다. 기기 접근 제어 프로세스에 필요한 사항은 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 장치 설정을 변경하기 전에 사용자 인증 메커니즘을 제공해야 한다. 인증의 예로는 암호와 키 카드가 있다:</li> <li>• 로그인 시 암호가 필요한 경우, 8자 이상의 암호를 제공해야 한다. 가능한 경우 더 긴 암호 및 RSA 키 등과 같은 기타 인증 토큰이 지원될 수 있다.</li> <li>• 사용자 설명서는 “암호는 사용자 이름 또는 사용자 전체 이름의 일부를 포함해서는 안 된다. 예를 들어, 이름, 회사 이름, 제품이름 등”, “사전 단어를 사용 하면 안 된다.”, “임의의 무의미한 암호를 사용해야 한다.” 와 같은 지침을 포함해야 한다.</li> <li>• 암호는 소문자, 대문자, 숫자 및 특수문자의 네 가지 문자유형 중 세 가지를 사용해야 한다.</li> </ul>	10.8.2 참조
32	네트워크 접근 제어 Network access control	6.2.4.2	<p>- 네트워크 접근 제어는 460-네트워크 리소스에 대한 접근을 허용하거나 거부하기 위한 것이다. 460-스위치 또는 460-포워더는 네트워크 접근 제어를 통해 승인 되지 않은 장비 및 승인되지 않은 트래픽의 접근을 거부해야 한다.</p> <p>- 460-네트워크에 연결된 각 450-노드와 460-노드는 보안영역 외부에 설치된 경우 MAC주소로 승인되어야 하며 460-스위치 또는 460-포워더의 포트에 물리적으로 연결되어야 한다.</p> <p>연결된 노드를 보안 영역에 설치하려는 경우 MAC 주소에 의한 승인을 활성화하거나 비활성화 할 수 있는 수단이 제공되어야 한다.</p> <p>- 460-스위치 및 460-포워더에서 모든 우회 및 발신 트래픽은 IP주소, 프로토콜 번호 및 포트번호로 승인되어야 한다.</p> <p>참고) 일반적으로 네트워크 접근 제어 기능은 장비 제조사에서 ACL(Access Control List)이라는 이름으로 제공한다.</p>	10.6.3.4 10.7.4.4 참조
6.3 외부 보안 요구사항				
6.3.2 방화벽				
33	외부 방화벽 External firewall	6.3.2.1	<p>- 외부 방화벽은 DMZ 내의 장비에만 등록되고 지정되지 않은 모든 트래픽을 차단 한다. 이는 원칙적으로 460-네트워크에 대한 모든 직접통신이 허용되지 않는 것을 의미한다.</p>	

No.	요구조건	IEC 61162-460	내용	비고
34	내부 방화벽 Internal firewall	6.3.2.2	<p>- 내부 방화벽은 460-네트워크 장비로 향하고, DMZ의 장비에서 비롯되지 않은 한, 모든 트래픽을 차단한다. 내부방화벽을 통과하는 모든 트래픽은 사전에 등록된다.</p>	
35	직접 통신 Direct communication	6.3.3	<p>- 460-네트워크 장비에 직접 통신이 필요한 경우 전체 통신 기간 동안 모니터링과 함께 관리자 또는 감독자의 허가가 필요하다. (6.3.5 및 부속서 A 참조).</p> <p>- 비제어 네트워크와 460-네트워크 간의 직접 연결은 460-게이트웨이 또는 460-무선 게이트웨이에서만 가능하다. 직접연결은 외부 네트워크를 통한 원격 활성화로부터 보호된다. 직접 연결이 설정되면 460-노드는 이 연결을 사용하여 비 제어 네트워크와의 통신에 사용할 수 있다. 상세는 6.3.4를 참조한다.</p> <p>- 비제어 네트워크와 460-네트워크 사이의 모든 직접 연결은 460-게이트웨이 또는 460-무선 게이트웨이를 통해 VPN을 사용하여야한다. 비 제어 네트워크와 교환되는 모든 데이터는 보안 공격으로부터 보호하기 위해 암호화되어야한다. VPN은 460-게이트웨이 또는 460-무선 게이트웨이에서 비 제어 네트워크를 통해 460-네트워크를 연결하는데 사용될 수 있다. 460-게이트웨이 또는 460-무선 게이트웨이 또한 460-노드가 VPN을 통해 다른 대상으로 직접 통신할 수 있도록 허용할 수 있다. 이 경우 460-게이트웨이 또는 460-무선 게이트웨이는 VPN 연결을 설정해야 하며, 460-게이트웨이 또는 460-무선게이트웨이는 내부 460-네트워크 내의 연결을 위한 네트워크 기능을 제공해야 한다.</p> <p>참고) 암호화는 승인되지 않은 읽기를 방지 하고 서명/인증 시 승인되지 않은 수정을 방지 하며 발신자를 식별한다. 둘의 조합도 가능 하다.</p> <p>- 보안 암호화 알고리즘은 다음과 같은 키 길이를 가진 비대칭 또는 대칭 알고리즘을 사용해야 한다.</p> <ul style="list-style-type: none"> <li>•비대칭 암호화 알고리즘은 최소 RSA 만큼 강력한 암호화 강도로 최소 2048비트의 키 길이(256 바이트)를 제공해야 한다.</li> <li>•대칭 암호화 알고리즘은 최소 AES 만큼 강력한 암호화 강도로 최소 256비트 키 길이(32바이트)를 제공해야 한다.</li> </ul>	10.8.3 참조

No.	요구조건	IEC 61162-460	내용	비고
			- 키는 신뢰 체인(chain of trust)을 사용하거나 개인 키가 관련된 경우 안전한 수동 방식으로 교환하거나 수동(예: 전화통화) 및 메시지(예: 보안/암호화된 이메일 전송)의 조합을 사용하여 전달해야 한다.	
36	460-노드 460-Node	6.3.4	- 460-노드는 필요한 경우 DMZ를 우회하는 460-게이트웨이를 통해서 비제어 네트워크에서 다른 장비와 직접 정보를 교환 할 수 있다. 직접 연결을 제공할 때 다음 요건을 만족해야 한다. <ul style="list-style-type: none"> <li>• 비제어 네트워크로부터의 직접 연결은 기본적으로 제조사에 의해 “허용되지 않음”으로 설정 되어야 한다.</li> <li>• 비제어 네트워크에서 460-노드에 대한 직접 연결은 460-노드의 운영자에 의해서만 활성화 되어야 한다. 전제조건은 비제어 네트워크와 460-네트워크 사이의 직접연결이 460-게이트웨이 또는 460-무선 게이트웨이에서 이미 활성화 되어야 한다.</li> <li>• 비제어 네트워크와의 직접 연결이 활성화 될 때 460-노드는 영구적인 표시를 가져야 한다.</li> </ul> 참고) 표시의 예로는 위치, 램프, 디스플레이 등이 있다. <ul style="list-style-type: none"> <li>• “비제어 네트워크에 연결”이라는 ‘주의’가 생성되어야 하며, 8.2.7에서 설명한 인터페이스는 직접 연결이 활성화 된 경우 사용되어야 한다.</li> <li>• 미리 정의된 시간 이후, ‘주의’는 ‘경계로 대체될 수 있다.</li> <li>• 비제어 네트워크와 460노드 사이의 모든 연결은 통신 보안 요구사항(6.3.3, 참고)을 만족해야 한다.</li> </ul> 6.3.5 460-게이트웨이	10.5.2.5 참조
37	방화벽 Firewall	6.3.5.1	- 다음은 460-게이트웨이에 대한 요구사항이다. <ul style="list-style-type: none"> <li>• 비제어 네트워크로부터의 직접연결은 제조사에 의해 “허용되지 않음”으로 설정 되어야한다.</li> <li>• 출발지/목적지 IP 주소, 프로토콜 및 포트 번호의 조합으로 구성된 내부 및 외부 방화벽이 제공 되어야한다.</li> <li>• 비제어 네트워크와 460-네트워크 사이의 모든 연결은 등록되어야 한다.</li> </ul>	10.8.4 참조

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• 비제어 네트워크에서 460-네트워크로의 모든 연결은 외부 통신 보안 요건을 충족해야 한다.(6.3.3 참조)</li> <li>• 460-게이트웨이는 460-네트워크와 비제어 네트워크 사이의 활성화된 직접 연결을 표시 하거나 “ 비제어 네트워크에 연결됨”이라는 주의를 생성해야한다. 그리고 주의를 8.2.7에 설명된 인터페이스를 사용해야 한다.</li> <li>• 460-게이트웨이는 460-네트워크와 비제어 네트워크 사이의 모든 활성화 된 직접 연결 목록을 제공해야 한다. 이 목록은 지난 12개월 동안의 변경을 포함하여 게이트웨이 또는 외부 장치에 의해 기록되어야 하며, 목록을 볼 수 있는 방법이 제공 되어야 한다. 사용이 가능한 경우, 활성화 된 직접 연결마다 최소한 다음 정보가 기록되어야 한다. IP 주소 소스, 대상 IP주소, 연결 시작시간 및 종료 시간, 프로토콜 및 포트번호.</li> <li>• 비제어 네트워크에서 460-노드와 직접 연결은 설치 사이트 또는 방화벽의 460-네트워크 측에서의 작동에 의해서만 활성화 되어야 한다. 이것은 비제어 네트워크에서 활성화 될 수 없어야 한다. 운영은 관리자 또는 감독자의 허가를 받아야만 수행 할 수 있도록 하는 수단을 제공해야 한다.</li> <li>• 모든 직접 연결은 사용자가 시간을 연장하기 위해 개입하지 않는 한 4시간 이하의 사전에 정해진 시간 후에 자동으로 종료 되어야 한다.</li> <li>• 직접 연결을 위한 모든 트래픽은 연결동안 트래픽이 없는 미리 정의된 10분 이내의 시간이 지나면 자동으로 전달을 중지 하여야한다.</li> </ul>	
38	응용 서버 Application server	6.3.5.2	<p>- 응용 서버는 비제어 네트워크와 460-네트워크에 의해 공통데이터 접근을 볼 수 있도록 한다. 응용 서버는 비제어 네트워크에서 클라이언트에 대한 암호와 같은 응용 수준 인증 매커니즘을 제공해야 한다(제공되는 경우).</p> <p>다음은 460-게이트웨이의 DMZ에 위치한 모든 서버에 대한 요구사항 이다.</p> <ul style="list-style-type: none"> <li>• 패킷의 라우팅은 허용 되지 않는다.</li> <li>• 460-노드 요건을 준수해야 한다.</li> </ul>	10.8.5 참조

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• 컴퓨터 플랫폼에 적합한 악성코드로부터 보호하기 위한 수단이 제공 되어야 한다.</li> </ul>	
39	DMZ의 파일저장소에 대한 상호 운영 접근 Interoperable access to file storage of DMZ	6.3.5.3	<p>- DMZ 내의 파일저장소에 접근하기 위해 DMZ와 비제어 네트워크 또는 460-네트워크 간에 파일을 다운로드/업로드 할 수 있는 방법이 제공될 수 있다. DMZ 내의 파일 저장소에 대한 접근이 제공되는 경우, SMB 네트워크 프로토콜(예:samba) 또는 SFTP(Secure Shell(SSH)파일전송 프로토콜)과 같은 프로토콜을 구현해야 한다. SMB 네트워크 프로토콜이 구현된 경우, 보안 취약점 때문에 버전 1을 사용할 수 없다.</p>	10.8.6 참조
40	460-무선 게이트웨이 460-Wireless gateway	6.3.6	<p>- 460-무선 게이트웨이에 대한 요구사항은 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 무선 액세스 포인트(AP)기능은 허용되지 않아야 한다. 즉, 무선 게이트웨이는 클라이언트로만 운영 되어야 한다.</li> <li>• 무선 네트워크에서 460-네트워크로의 트래픽 전달은 허용되지 않는다.</li> <li>• IEC 61162-450에 정의된 해당 SF 또는 ONF가 제공되어야 한다. 무선 게이트웨이는 460-게이트웨이의 모든 요건을 충족해야 한다. 무선 인터페이스를 통해 교환되는 모든 데이터는 6.3.3의 암호화 요구사항을 충족해야 한다.</li> <li>• 무선연결은 인증을 통해 등록된 무선 AP에만 설정 되어야 한다.</li> </ul>	10.9.2 참조
41	추가 보안 문제 Additional security issues	6.4	<p>- 460-스위치, 460-포워더, 460-게이트웨이 및 460-무선 게이트웨이에 대해 다음과 같은 관리 기능이 필요하다.</p> <ul style="list-style-type: none"> <li>• 구성은 스위치를 끄거나 전원 이상 후에도 유지 되어야 하며, 장비는 전원 복구 시 정상 작동으로 복귀해야 한다.</li> <li>• 구성이 변경 될 경우 시스템 관리 기능에 의해 이전 구성이 저장 되어야 한다. 시스템 관리 기능에서 이전 구성으로 되돌릴 수 있는 기능이 제공 되어야 한다(4.5.2 참조).</li> <li>• 460-스위치, 460-포워더, 460-게이트웨이 및 460-무선 게이트웨이에 대한 물리적 접근을 제한해야 함을 설치 지침에서 알려야 한다.</li> </ul>	10.6.3.5, 10.7.4.5, 10.8.7 참조

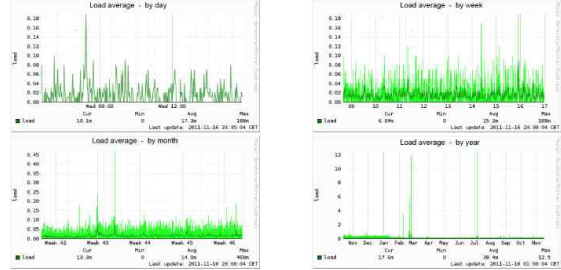
No.	요구조건	IEC 61162-460	내용	비고
7. 이중화 요구사항				
42	일반 General	7.1.1	<p>- 단일 구성 품 고장(케이블, 460-스위치, 460-포워더, 460-게이트웨이 또는 460-무선 게이트웨이)은 460-네트워크에서 노드의 기능에 중요한 영향을 미치지 않아야 한다.</p> <p>- 시스템 구성 문서는 노드의 중요도를 식별해두어야 한다.</p> <p>참고 1) IEC 62439-1 에는 세 가지 유형의 고장이 정의되어 있다. : 일시적 고장, 구성요소 고장, 체계의 고장(부속서 B 참조)</p> <p>- 460-네트워크에서 문제가 발생할 경우(네트워크 모니터링에 의해 감지), 고장 이벤트에서 이중화 방법의 활성화까지의 복구 시간은 5초를 넘지 않아야 한다.</p> <p>참고 2) 5초 보다 짧은 복구시간이 필요한 시스템은 ISO 16425참조</p> <p>- 이중화 인터페이스는 이중화(7.1.2 참조)또는 장치 이중화(7.1.3 참조)에 의해 제공되어야 한다. 그림3은 이 문서에 지정된 이중화 네트워크구성의 예를 보여준다.</p> <div data-bbox="657 1234 1198 1451" style="text-align: center;"> <p>The diagram illustrates three types of redundancy in a network setup. On the left, '장치 및 인터페이스 이중화' (Device and Interface Redundancy) shows two parallel paths, each with a GPS device (GPS 1 and GPS 2) connected to a switch. In the middle, '장치 이중화' (Device Redundancy) shows two parallel paths, each with an AIS device (AIS 1 and AIS 2) connected to a switch. On the right, '인터페이스 이중화' (Interface Redundancy) shows a single path with an INS device connected to a switch. All paths are connected to a central network backbone.</p> </div> <p style="text-align: center;">그림 3 이중화 예시</p>	
43	인터페이스 이중화 Interface redundancy	7.1.2	<p>- 인터페이스 이중화는 장치에 하나 이상의 IEC 61162-450 인터페이스가 있으며 인터페이스가 두 개 이상의 다른 460-스위치에 연결되어 있음을 의미한다.</p> <p>- 장비는 아래 방법 중 하나를 통해 인터페이스 이중화를 구현해야 한다.</p> <ul style="list-style-type: none"> <li>• 데이터 스트림 이중화</li> </ul> <p>데이터 스트림 이중화가 있는 장비는 두 인터페이스에서 동일한 데이터를 송수신해야 한다. 장비가 중복된 메시지를 수신할 때, 중복된 메시지는 네트워크 계층 또는 전송 계층 위에서 처리되어야 한다.</p> <p>참고 1) 수신 장비가 처리로 인하여 메시지를 사용하지나</p>	

No.	요구조건	IEC 61162-460	내용	비고
			<p>사용하지 않을 수 있다.</p> <ul style="list-style-type: none"> <li>• 링크기반 이중화</li> </ul> <p>링크 기반 이중화가 있는 장비는 두 번째 인터페이스가 대기상태일 때 첫 번째 인터페이스에서만 데이터를 송수신해야 한다. 첫 번째 인터페이스가 실패일 경우, 두 번째 인터페이스는 5초 이내에 연결되어야 한다. 두 인터페이스는 두 개의 개별 IP 주소 또는 하나의 공통 IP 주소로 구성될 수 있다.</p> <p>참고 2) 이 기술은 스위치 내결함성, 백업 본딩 또는 이중호밍으로 알려져 있다. 인터페이스 스위칭은 운영체제에 의해 관리된다. 어플리케이션 계층은 두 인터페이스를 단일 인터페이스로 간주하여 중복된 메시지를 처리할 필요가 없다. 이를 통해 CARP(공통 주소 이중화 프로토콜)와 같은 이중화 프로토콜을 사용할 수 있다.</p> <p>참고 3) 인터페이스 이중화 구현은 LAN 토폴로지에 따른다.</p>	
44	장치의 이중화 Device redundancy	7.1.3	<p>- 장치 이중화는 기능이 동일한 장치를 동시에 두 개 이상 활성화 하는 것을 의미한다.</p> <p>- 장치 이중화가 있는 장비는 고유한 장치 식별자(예 : 태그 블록 및 SFI)를 가져야하며 다른 460-스위치에 연결되어야 한다. 추가적인 안전을 위해, 장치 이중화를 인터페이스 이중화와 함께 사용할 수 있다.</p>	
45	460-노드 요구사항 460-Node requirements	7.2	<p>- 높은 중요도로 정의된 각 460-노드는 최소 인터페이스 이중화 또는 장치 이중화를 제공해야 한다.</p> <p>참고) 460-노드 제조자는 장비를 중요하거나 중요하지 않은 것으로 정의한다.</p> <p>- 이중화 기능을 설명하는 문서가 제공되어야 한다.</p>	10.5.3 참조
46	460-스위치 요구사항 460-Switch requirements	7.3	<p>- 460-스위치에 장애가 발생하거나 460-스위치 사이의 케이블 연결이 끊긴 경우, 460-네트워크의 다른 460-스위치에서 발생하는 주요 네트워크 트래픽은 링, 백업 인터페이스 또는 유사한 아키텍처에 의해 중요하다고 정의된 460-노드로 다시 라우팅되어야 한다.</p>	10.5.3 참조
47	460-포워더 요구사항 460-Forwarder requirements	7.4	<p>- 이중화가 제공되는 경우 460-스위치의 이중화 요구사항을 적용해야 한다.</p>	
48	460-게이트웨이와 460-무선 게이트웨이 요구사항	7.5	<p>- 이중화가 제공되는 경우, 460-스위치 이중화 요구사항을 적용해야 한다.</p>	

No.	요구조건	IEC 61162-460	내용	비고
	460-Gateway and 460-Wireless gateway requirements			
49	네트워크 모니터링 기능 요구사항 Network monitoring function requirements	7.6	- 네트워크 모니터링 기능은 이중화로 사용 할 수 있어야 한다.	8.2.6 참조
50	시스템 설계 요구사항 System design requirements	7.7	- 시스템 문서에는 이중화 기능에 대한 FMEA 또 는 FEMCA가 포함 되어야 한다.  - 460 네트워크의 시스템 통합자는 연결 된 모든 장 비를 포함한 460-네트워크가 단일 구성요소 고장 요 건을 충족함을 입증하는 문서를 제공해야 한다. 케 이블, 460-스위치, 460-포워더, 460-게이트웨이 또는 460-무선 게이트웨이의 고장은 460-네트워크의 중요 노드의 기능에 영향을 미치지 않아야 한다. 문서는 중요한 노드를 식별해야 한다.	10.12.3.10 참조
8. 네트워크 모니터링 요구사항				
8.1 네트워크 상태 모니터링				
51	460-네트워크 460-Network	8.1.1	- 460-네트워크의 구성과 트래픽의 흐름은 8.1. 2~8.1.4. 에 설명된 바와 같이 보고 및 모니터링 되 어야 한다.	
52	460-노드 460-Node	8.1.2	- 460-노드에서 모니터링 하는데 필요한 구성 정보 는 다음과 같다.  • 인터페이스 수 • 트래픽의 플로우 목록 및 최대트래픽 속도 설계치 • 플로우의 변경 - 추가, 삭제 또는 수정 • 각 인터페이스에 할당된 플로우의 목록  - 정보는 460-노드에서 30분마다 주기적으로 시스 로그에 의해 제공 되어야 한다(IEC 61162-450 참조). 또한 노드의 플로우가 추가 또는 삭제 등 구성이 변 경 될 때마다 정보가 기록 되어야 한다. 구성정보는 분당 1회 이상 보고되지 않아야 한다.	10.5.4 참조
53	460-스위치 460-Switch	8.1.3	- 460-스위치에서 모니터링 하는데 필요한 구성 정 보는 다음과 같다.  • 인터페이스 정보 • 각 인터페이스 당 인접 MAC 주소 목록 • 인접 MAC 주소 변경  - 정보는 SNMP 쿼리 요청 메시지를 수신할 때 460-스위치에서 보고되어야 한다. (8.2.3 및 8.2.4참 조). 또한 인접 MAC 주소의 변경과 같이 구성이 변경 될 때 마다 SNMP-트랩 또는 시스로그를 사용	10.6.4 참조



No.	요구조건	IEC 61162-460	내용	비고
			<p>하여 변경 사항을 보고 해야 한다. 시스로그를 사용한 구성 정보는 분당 1회 이상 보고되지 않아야 한다.</p> <ul style="list-style-type: none"> <li>- 460-스위치에서 모니터링에 필요한 트래픽 플로우 정보는 인터페이스 입력 및 출력 링크 사용률 (평균 5 분 이상)이다.</li> <li>- 정보는 SNMP 쿼리 요청 메시지를 수신 할 때 460-스위치에서 보고되어야 한다(8.2.2참조). 또한 중대한 변경(트래픽이 네트워크 용량 0~100% 범위에 사전 정의된 한계 이상)이 발생할 때마다 SNMP-트랩 또는 시스로그를 사용하여 변경사항을 보고해야 한다. 시스로그를 사용한 트래픽 플로우 정보는 3초에 1회 이상 보고되지 않아야 한다.</li> </ul> <p>참고) 460스위치가 네트워크 모니터링에 보낸 SNMP 응답은 직접 경보를 발생 시키지 않고 네트워크 모니터링 기능이 경고를 발생 시키는 통계기반 역할을 한다.</p>	
54	460-포워더 460-Forwarder	8.1.4	<ul style="list-style-type: none"> <li>- 460-포워더는 SNMP 쿼리 요청 메시지를 수신할 때 스위치(8.1.3 참조)에 필요한 구성정보를 제공해야 한다(8.2.3 및 8.2.4 참조). VLAN이 제공된 경우 현재 VLAN 구성 정보를 제공해야 한다. 또한 변경사항이 있을 때 마다 SNMP-트랩 또는 시스로그를 사용하여 변경사항을 보고해야 한다. 시스로그를 사용한 경우 구성정보는 분당 1회 이상 보고되지 않아야 한다.</li> <li>- 460-포워더는 인터페이스 당 유효한 입력 및 출력 패킷수 (평균 5분 이상)와 함께 스위치에 필요한 트래픽 플로우 정보를 제공해야 한다(8.1.3 참조).</li> <li>- 이 정보는 460-스위치와 동일한 방식으로 460-포워더에 의해 보고되어야 한다(8.1.3참조).</li> </ul>	10.7.5 참조
8.2 네트워크 모니터링 기능				
55	일반사항 General	8.2.1	<ul style="list-style-type: none"> <li>- 네트워크 모니터링 기능은 네트워크 부하, 이중화 및 토폴로지를 모니터링 하고 위반사항을 탐지 하고 경고를 생성하여 네트워크 운영을 유지하도록 돕는다. 네트워크 모니터링 기능은 적어도 하나의 460-노드 또는 460-네트워크의 일부 인 하나의 460-스위치에서 사용할 수 있어야 한다.</li> <li>- 시료(Equipment Under Test)가 네트워크 모니터링 기능을 제공하지 않는 경우 설치 문서에는 다른 장비가 네트워크 모니터링 기능을 제공하는 네트워크에만 EUT를 연결할 수 있음을 명시해야 한다.</li> </ul>	10.11.1 참조

No.	요구조건	IEC 61162-460	내용	비고
			<p>- 네트워크 모니터링 기능은 경고관리의 기능을 제공해야 하며 경고관리 기능에 접근 할 수 있는 HMI (Human Machine Interface)를 제공해야 한다(8.2.7 참조).</p> <p>- 로컬 HMI가 제공되고 시스템이 선교에 설치 되도록 설계된 경우 경고(8.2.7참조)를 위한 인터페이스를 제공해야 한다. 선교 설치를 위한 호환성은 제조자가 지정해야 한다.</p> <p>- 네트워크 모니터링 기능은 필요할 때 이용할 수 있는 기록을 유지해야 한다. 기록은 최소 마지막 3개월 또는 마지막 10,000개 이벤트 중 더 작은 것을 저장 할 수 있어야 한다. 최소한 다음과 같은 이벤트 기록이 저장 되어야 한다.</p> <p>a) 네트워크 모니터링 기능의 모든 경고</p> <p>b) SNMP 또는 시스로그를 사용하는 460스위치 또는 460-포워더의 이벤트 또는 보고서(8.2.2, 8.2.3 및 8.2.4참조).</p> <p>- 기록은 사용자가 보기에 적합한 형식으로 표시 될 수 있어야 한다. 그림 4의 예시 참조.</p>  <p>그림 4 - 네트워크 상태 기록 정보 예시</p>	
56	네트워크 부하 모니터링 기능 Network load monitoring function	8.2.2	<p>- 시스템 문서는 시스템이 460-네트워크로 생성되는 모든 플로우의 총 최대 트래픽 속도를 제조자의 정의에 기초한 최대 네트워크 부하에 대한 모든 스위치와 스위치, 포워더 및 게이트웨이에 대한 분석을 포함해야 한다.</p> <p>- 네트워크 모니터링 기능은 8.1.3 및 8.1.4 에 명시된 바와 같이 460-스위치 및 460-포워더에서 정보를 수집하기 위해 아래 방법 중 하나 이상을 사용해야 한다.</p> <p>a) SNMP 쿼리를 사용하여 30초 주기</p> <p>b) 15분마다 SNMP-트랩 방법 (예: RMON 통계 요청)과 주기적인 SNMP 쿼리 조합사용</p>	10.11.2 참조

No.	요구조건	IEC 61162-460	내용	비고
			<p>c) 분당 1회 이하의 보고서와 함께 시스로그방법 사용.</p> <p>- 네트워크 모니터링 기능은 다음 경고를 생성해야 한다.</p> <ul style="list-style-type: none"> <li>• 주의: 네트워크 트래픽 용량 초과 될 수 있음 - 관측된 네트워크 부하가 10분 이내에 3회 이상 30초 동안 460-스위치 또는 460-포워더에서 어떤 포트의 물리적 용량의 80% 한계를 초과하는 경우</li> <li>• 경계: 네트워크 트래픽 용량 초과 - 관측된 네트워크 부하가 10분 이내에 10회 이상 30초 동안 460-스위치 또는 460-포워더에서 어떤 포트의 물리적 용량 80%제한을 초과 한 경우</li> </ul>	
57	<p>이중화 모니터링 기능 Redundancy monitoring function</p>	8.2.3	<p>- 시스템 문서에는 인터페이스 이중화(7.1.2 참조) 또는 장치 이중화(7.1.3 참조)에 의해 이중으로 사용할 수 있는 데이터 소스 목록이 포함 되어야 한다. 인터페이스 이중화를 위한 목록에는 460-스위치에서 사용할 수 있는 MAC 주소, 인터페이스 번호 및 인터페이스가 포함 되어야 한다. 장치 이중화를 위한 목록에는 이중으로 사용할 수 있는 각 장치의 MAC 주소가 포함 되어야 한다.</p> <p>- 네트워크 모니터링 기능은 8.1.3 및 8.1.4 에 명시된 바와 같이 460-스위치 및 460-포워더에서 정보를 수집하기 위해 아래 방법 중 하나 이상을 사용해야 한다.</p> <p>a) SNMP 쿼리를 사용 하여 30초 주기 b) 15분마다 SNMP-트랩 방법 (예: RMON 변경 알림 요청)과 주기적인 SNMP 쿼리 조합사용 c) 분당 1회 이하의 보고서와 함께 시스로그 방법 사용</p> <p>- 목록에는 다음 정보가 포함 되어야한다.</p> <ul style="list-style-type: none"> <li>• 데이터 소스 이름: 최대 8자 문자열</li> <li>• 데이터를 사용 할 수 있는 각 이중 네트워크 주소에 대해 2개 이상의 MAC주소, 인터페이스 번호 및 인터페이스 사용 가능한 대안</li> </ul> <p>- 두개의 MAC 주소 또는 데이터 소스에 사용 가능한 인터페이스가 두개 미만인 하나의 MAC 주소가 2분 동안 손실 된 경우, 네트워크 이중화 모니터링</p>	10.11.3 참조

No.	요구조건	IEC 61162-460	내용	비고
			기능은 다음과 같은 경고를 생성해야한다.  주의: xxxx 에 대한 네트워크 이중화가 손실. 여기서 xxxx 은 데이터 소스의 이름	
8.2.4 네트워크 토폴로지 모니터링 기능				
58	토폴로지 모니터링 Topology monitoring	8.2.4.1	<ul style="list-style-type: none"> <li>- 시스템 문서에는 MAC 주소와 함께 460-네트워크에 대해 승인된 장치 목록이 포함 되어야 한다. 보안 영역에서 승인된 장치의 경우, 승인 해제를 위해 장치가 선택된 경우 목록에 MAC 주소 대신 “해당 없음”이 포함 될 수 있다(6.2.4.2 참조).</li> <li>- 네트워크 토폴로지를 유지하기 위하여 네트워크 토폴리지를 모니터링하고 승인된 장치 목록에서 사용할 수 없는 것으로 감지된 추가 장치를 기반으로 경고를 생성해야 한다. 네트워크 모니터링 기능은 8.1.3 및 8.1.4에 명시 된 바와 같이 460-스위치 및 460-포워더에서 정보를 수집하기 위해 아래 방법 중 하나 이상을 사용해야 한다.                         <ul style="list-style-type: none"> <li>a) SNMP 쿼리를 사용 하여 30분 주기</li> <li>b) 2시간마다 SNMP-트랩 방법 (예: RMON 변경 알림 요청)과 주기적인 SNMP 쿼리 조합사용</li> <li>c) 분당 1회 이하의 보고서와 함께 시스로그 방법 사용</li> </ul> </li> <li>- SNMP 요청에서 승인 된 장치 목록에 포함되지 않은 MAC 주소가 발견되면, 네트워크 토폴로지 모니터링 기능은 다음 경보를 생성해야 한다.</li> </ul> <p style="margin-left: 20px;">주의: 네트워크에서 새로운 장치가 발견되었음.</p>	10.11.4 참조
59	SFI 충돌 모니터링 SFI collision monitoring	8.2.4.2	<ul style="list-style-type: none"> <li>- 선박의 460-네트워크 구축 시, SFI(System Function ID)의 할당을 명확하게 정의 할 수 있다. 그러나 선박의 장비가 수정, 교체, 수리 및 점검됨에 따라 SFI 의 할당이 명확하지 않을 수 있다.</li> <li>- SFI의 고유성을 유지하기 위하여 SFI 충돌을 모니터링 하고 동일한 SFI의 여러 인스턴스 간에 감지된 충돌을 기반으로 경고를 생성해야 한다. SFI 충돌 모니터링은 450-노드와 460-노드가 보낸 SRP-센텐스를 기반으로 한다(IEC 61162-450 참조). SFI 충돌 모니터링은 서비스 기관의 SFI 의 고유성을 유지 하고 사용 중인 시스템의 설정 구성에 이상이 있을 경우 사용자에게 알릴 수 있도록 지원한다.</li> <li>- 다음 규칙은 SFI 충돌 모니터링에 적용 된다.</li> </ul>	

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• SFI 충돌 모니터링은 수신된 SRP 센텐스에서 사용할 수 있는 모든 필드에 기반 하여 SFI 표를 유지해야 한다. SRP-센텐스의 새로운 조합은 SFI표에 새로운 입력을 생성 한다.</li> <li>• SFI 충돌 모니터링은 SFI 표의 내용을 볼 수 있는 가능성을 제공해야 한다. 보기는 최소한 SFI 충돌과 이중화로 이용 가능한 SFI를 표시해야 한다. 보기는 SFI 충돌 모니터링이 구현된 장비에서 내부적으로 사용할 수 있거나 SFI 충돌 모니터링이 필요한 정보를 제공하는 다른 장비에서 사용할 수 있다.</li> <li>• SFI 충돌 모니터링은 SFI 충돌 모니터링을 부팅할 때 및 사용자의 요구에 따라 SFI 표를 재설정 할 수 있다.</li> <li>• SFI표를 기반으로 비 충돌 SFI를 식별 할 수 있다. 다른 SFI와 결합된 동일한 MAC 주소 또는 다른 SFI와 결합된 동일한 IP 주소는 SFI 충돌을 일으키지 않는다.</li> <li>• SFI 표에 근거하여 이중화로 이용 가능한 SFI는 SRP 센텐스의 “이중 대체 인스턴스 수”필드의 차이로부터 확인 할 수 있다. 이중화로 이용 가능한 SFI는 SFI의 충돌을 일으키지 않는다.</li> <li>• SFI 표에 근거하여 아래의 모든 조건이 충족될 때 충돌이 감지된다.             <ul style="list-style-type: none"> <li>· 동일한 SFI를 여러SRP 센텐스에서 사용할 수 있다</li> <li>· SRP센텐스 중 하나 이상의 “이중 대체 인스턴스 수” 필드에 널(null) 또는 두개의 SRP 센텐스가 동일한 값을 포함</li> <li>· 그리고 SRP 센텐스의 “MAC 주소” 필드의 차이 또는 “IP주소”필드의 차이가 있다.</li> </ul> </li> <li>- SFI충돌이 감지될 경우, SFI 충돌 감시 기능은 다음과 같은 경고를 생성해야 한다.</li> </ul> <p>주의: 네트워크에서 SFI cxxxx 충돌. 여기서 cxxxx 는 SFI의 식별자 문자열이다.</p>	
60	시스템 기록 기능	8.2.5	<ul style="list-style-type: none"> <li>- 네트워크 모니터링 기능은 시스템 메시지의 수신기(receiver) 및 기록기(recorder) 역할을 해야 한다.</li> </ul>	10.11.5 참조

No.	요구조건	IEC 61162-460	내용	비고																																																																								
	Syslog recording function		- 네트워크 모니터링 기능은 450-노드, 460-노드, 460-게이트웨이 및 460-무선 게이트웨이가 제공한 시스로그 정보의 기록 및 보기를 제공해야 한다. - 기록의 최소 용량은 20,000개 메시지여야 한다. 기록 된 시스로그 메시지는 최소 90일 동안 사용할 수 있어야 한다.																																																																									
61	네트워크 모니터링 기능 이중화 Redundancy of network monitoring function	8.2.6	- 네트워크 모니터링 기능은 이중화가 가능해야 한다.	10.12.7.3 참조																																																																								
8.2.7 경고 관리																																																																												
62	경고 및 표시 Alerts and indication	8.2.7.1	- 경고 및 표시는 IEC 62288에 지정된 표시 요구 사항을 준수해야 한다. 표 2 는 이 기준서에 정의된 모든 경보의 요약 이다. 표 2 - 네트워크 감시경고 요약 <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>소스</th> <th>원인</th> <th>경보</th> <th>경계</th> <th>주의</th> <th>카테고리A</th> <th>카테고리B</th> <th>경고소스의 특수식별자</th> </tr> </thead> <tbody> <tr> <td>460 노드</td> <td>경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3109</td> </tr> <tr> <td>460 노드</td> <td>경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)</td> <td></td> <td>X</td> <td></td> <td></td> <td>X</td> <td>3108</td> </tr> <tr> <td>460 게이트웨이</td> <td>통제되지 않는 네트워크와 연결(6.3.5.1 참고)</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3113</td> </tr> <tr> <td>네트워크 감시기능</td> <td>네트워크 트래픽 용량 초과될 가능성이 있는 경우 (8.2.2 참고)</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3116</td> </tr> <tr> <td>네트워크 감시기능</td> <td>네트워크 트래픽 용량 초과된 경우 (8.2.2 참고)</td> <td></td> <td>X</td> <td></td> <td></td> <td>X</td> <td>3118</td> </tr> <tr> <td>네트워크 감시기능</td> <td>xxxxx의 네트워크 이중화 상실</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3123</td> </tr> <tr> <td>네트워크 감시기능</td> <td>네트워크에 새로운 장비가 감지된 경우(8.2.4 참고)</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3126</td> </tr> <tr> <td>네트워크 감시기능</td> <td>SFI 중환이 감지된 경우 (8.2.4 참고)</td> <td></td> <td></td> <td>X</td> <td></td> <td>X</td> <td>3129</td> </tr> </tbody> </table>	소스	원인	경보	경계	주의	카테고리A	카테고리B	경고소스의 특수식별자	460 노드	경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)			X		X	3109	460 노드	경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)		X			X	3108	460 게이트웨이	통제되지 않는 네트워크와 연결(6.3.5.1 참고)			X		X	3113	네트워크 감시기능	네트워크 트래픽 용량 초과될 가능성이 있는 경우 (8.2.2 참고)			X		X	3116	네트워크 감시기능	네트워크 트래픽 용량 초과된 경우 (8.2.2 참고)		X			X	3118	네트워크 감시기능	xxxxx의 네트워크 이중화 상실			X		X	3123	네트워크 감시기능	네트워크에 새로운 장비가 감지된 경우(8.2.4 참고)			X		X	3126	네트워크 감시기능	SFI 중환이 감지된 경우 (8.2.4 참고)			X		X	3129	10.11.6.1 참조
소스	원인	경보	경계	주의	카테고리A	카테고리B	경고소스의 특수식별자																																																																					
460 노드	경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)			X		X	3109																																																																					
460 노드	경고로서 통제되지 않는 네트워크와의 직접연결( 6.3.4 참고)		X			X	3108																																																																					
460 게이트웨이	통제되지 않는 네트워크와 연결(6.3.5.1 참고)			X		X	3113																																																																					
네트워크 감시기능	네트워크 트래픽 용량 초과될 가능성이 있는 경우 (8.2.2 참고)			X		X	3116																																																																					
네트워크 감시기능	네트워크 트래픽 용량 초과된 경우 (8.2.2 참고)		X			X	3118																																																																					
네트워크 감시기능	xxxxx의 네트워크 이중화 상실			X		X	3123																																																																					
네트워크 감시기능	네트워크에 새로운 장비가 감지된 경우(8.2.4 참고)			X		X	3126																																																																					
네트워크 감시기능	SFI 중환이 감지된 경우 (8.2.4 참고)			X		X	3129																																																																					
63	경고 관리 인터페이스 Alert management interface	8.2.7.2	- 양방향 인터페이스는 외부 시스템으로 경고가 전달 될 수 있도록 통신을 용이하게 하고, 가청 경보 (제공된 경우)를 음소거 또는 외부 시스템에서 확인 (Ack) 할 수 있도록 한다. - 경고관리 인터페이스는 제공된 경우 부속서 E 의 요구사항 및 IEC61924-2:2012, 부속서 J의 상태 다이어그램을 준수해야 한다. 경고 관리 요구사항 <ul style="list-style-type: none"> <li>• 경고 분류</li> <li>• 경고의 표시</li> <li>• 경고의 보고</li> <li>• 확인되지 않은 경계의 취급</li> <li>• 원격 확인 및 원격 음소거 기능</li> </ul>	10.11.6.2 참조																																																																								
64	확인되지 않은 경계 Unacknowledged warnings	8.2.7.3	- 확인되지 않은 경계는 다음과 같다. <ul style="list-style-type: none"> <li>• 5분을 초과하지 않는 제한된 시간 후에 경계로 반복 됨 또는</li> <li>• 5분을 초과하지 않는 제한된 시간 후에 경보 우선 순위로 변경 됨 또는</li> </ul>	10.11.6.3 참조																																																																								

No.	요구조건	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>• 사용자가 선택할 수 있는 시간이 5분을 넘지 않으면 경보 우선순위가 변경</li> <li>- 사용자가 선택한 기간의 기본시간은 60초이어야 한다.</li> </ul>	
65	원격 확인 및 경고의 음소거 Remote acknowledgments and silencing of alerts	8.2.7.4	<ul style="list-style-type: none"> <li>- 카테고리 B 경고에 대해서만 원격 확인이 가능해야 한다. (IEC 61924-2:2012, 부속서 C 참고).</li> <li>- 네트워크 모니터링 기능에 가칭 경보의 원격 음소거가 제공될 경우 언제든지 가능해야 한다.</li> </ul>	10.11.6.4 참조
66	제어 네트워크 요구사항 Controlled network requirements	9	<ul style="list-style-type: none"> <li>- 제어 네트워크는 연결된 네트워크 노드에 어떠한 보안 위험도 초래하지 않고 작동하도록 설계된 네트워크이다. 이는 다음의 최소 요건을 충족해야 한다.                     <ul style="list-style-type: none"> <li>• 물리적 인프라에 직접 접근하거나 무선 인터페이스를 통해 허가되지 않은 트래픽을 네트워크에 삽입하는 데 사용할 수 있는 장치를 네트워크에 연결할 수 없어야 한다.</li> <li>• 네트워크 노드는 사용자가 이러한 작업을 수행할 수 있는 권한이 없는 한, 사용자가 승인되지 않은 트래픽을 네트워크에 삽입하는데 사용할 수 있는 운영 시스템 또는 기능에 직접 접근할 수 있도록 허용해서는 안 된다.</li> <li>• 승인되지 않은 REDS 또는 승인되지 않은 콘텐츠가 있는 REDS 또는 REDS에서 네트워크의 어떤 노드나 장치로 데이터를 전송할 수 없어야 한다.</li> </ul> </li> <li>- 대부분의 제어 네트워크는 네트워크에서 승인되지 않은 데이터 읽기를 막고 네트워크 토폴로지 변경을 막기 위한 규정을 포함할 수 있다. 그러나 460-네트워크에 연결된 제어 네트워크에 대해서는 그러한 규정이 필요하지 않다.</li> <li>- 시스템 통합 관리자는 이러한 요구사항이 충족된다는 문서화된 근거를 제공해야 한다.</li> </ul>	10.10 참조

## 제 3 장 형식시험

### 제 1 절 일반사항

#### 101. 형식시험 시료(EUT)의 구성

1. 시료(EUT)는 IEC 61162-460에 정의된 개별 네트워크/시스템 구성요소 또는 IEC 61162-460에 기반한 시스템일 수 있다.

#### 102. 시험 장소 및 구성(Test configuration)

1. 시험 장소는 제조자의 선택에 따라 실험실 시험대 또는 시험 시설 내 설치 일 수 있다.

참고 : 실험실 시험대는 일반적으로 개별 네트워크/시스템 구성요소에 대해 선택된다. 시험 시설에 전체 시스템을 설치하는 것은 복잡한 시스템에 더 적합하다.

2. 네트워크 프로토콜 분석기가 필요하다.

(예 : Wireshark)

3. 다음의 특성을 가진 시뮬레이터가 필요하다.

- (1) IEC 61162-450에 호환하는 데이터 및 IEC 61162-450을 준수하지 않는 데이터를 전송 및 수신할 수 있음.
- (2) 유효하지 않은 데이터를 생성할 수 있음.
- (3) 시료에 적합한 이더넷 (Ethernet) 인터페이스를 지원할 수 있음.
- (4) SNMP 및 시스로그 클라이언트-서버 데이터 제공이 가능함.
- (5) SNMP를 통해 네트워크 구성 및 상태 정보를 모니터링 할 수 있음.
- (6) 시스로그를 통해 네트워크 구성 및 상태 정보를 모니터링 할 수 있음.
- (7) ICMP 패킷 (packets) 제공이 가능함.
- (8) IEC 61162-450에 호환하는 데이터 및 IEC 61162-450을 준수하지 않는 데이터를 사용하여 0% ~ 100%의 네트워크 부하를 제공할 수 있음. (예: TCP/IP, UDP/IP, multicast and broadcast)
- (9) IEC 61162-450에 호환하는 데이터를 IEC 61162-460의 표 1에 명시된 우선순위에 따라 제공할 수 있음 (시료가 이 기능을 지원하는 경우)
- (10) VLAN 및 서브넷 (subnets)을 포함한 여러 네트워크에 IEC 61162-450에 호환하는 데이터를 제공할 수 있음.

4. 다음의 특성을 가진 보안 시험을 위한 시뮬레이터도 필요하다.

- (1) 클라이언트-서버 연결을 제공할 수 있음.
- (2) DoS 공격 패킷 (packet) 생성이 가능함.





그림 1 시험 구성 (예시)

### 103. 시험의 순서

1. IEC 기준에 시험의 순서가 규정되어 있다면 그 순서를 따라야 한다. 단, 별도로 규정되어 있지 않은 사항의 경우 KR과 협의 하에 진행하여야 한다.

## 제 2 절 시험 항목 및 결과

### 201. 시험 항목

아래 Table의 항목에 대한 성능 시험이 실시되어야 한다.

No.	시험 항목	IEC 61162-460	내용	비고
1	일반 요구사항 General requirements	10.3	<ul style="list-style-type: none"> <li>- 각 460-네트워크 구성요소가 IEC 60945에 따른 선박 향해 무선통신장비에 대한 일반 요건을 준수하는지 확인하여야 한다.</li> <li>- 각 460-네트워크 구성요소가 IEC 61162-450:2018의 조항 4 및 5에 따른 일반 요건을 준수하는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 적용가능한 모든 MAC 주소 목록이 460-네트워크용으로 제공되는지 확인하여야 한다.</li> <li>- 참조된 IEC 표준에 따라 이전에 수행된 시험의 시험데이터 및 시험성적서는 시험문서의 검사에 의해 적합성을 확인 할 수 있어야 한다.</li> </ul>	
2	450-노드 450-Node	10.4	<ul style="list-style-type: none"> <li>- 분석 평가를 통해 정상 작동 시 외부 네트워크 또는 REDS에 연결할 수 없음을 확인하여야 한다.</li> <li>- 분석 평가를 통해 시스로그가 IEC 61162-450:2018 4.3.3.2에 정의된 대로 구현되는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 노드의 데이터 출력이 IEC 61162-460:2018 6.2.2.1에 기술된 바와 같이 문서화 되어 있는지 확인하여야 한다.</li> <li>- ONF 서비스가 제공되는 경우, 제조자의 문서를 검사하여 필요한 프로토콜 매개변수 (예: IP 주소 및 포트 번호)를 포함하는지 확인하여야 한다.</li> </ul>	
10.5 460-노드				
3	네트워크 트래픽 관리 Network traffic management	10.5.1	<ul style="list-style-type: none"> <li>- 문서화된 증거의 분석 평가를 통해 460-노드가 IEC 61162-450 준수하지 않는 트래픽을 생성하지 않는 것을 확인하여야 한다.</li> </ul> <p>비고) 트래픽에 대한 대부분의 사용 사례는 ONF로 설명할 수 있으며, 이 경우 IEC 61162-450 준수 트래픽이다. 명확한 비 준수 사례는 일반적으로 IEC61162-450에서 허용된 것 이외의 목적으로 예약된 IP주소 또는 포트 번호 (예: 239.192.0.1 비디오 서비스 브로드캐스트)를 사용하는 것을 기반으로 한다.</p>	

No.	시험 항목	IEC 61162-460	내용	비고
			<ul style="list-style-type: none"> <li>- 제조자의 문서를 참조하여 지원되는 모든 서비스에 대한 최대 전송속도가 명시되어 있는지 문서화된 증거를 검사하여 확인하고 문서화된 증거를 분석 평가를 통해 모든 IEC61162-450 준수 데이터가 최대 전송속도를 충족하는지 확인하여야 한다.</li> <li>- 분석 평가를 통해 장치가 10분 동안 최대 0.1% 패킷 손실률로 장비 성능 요구사항을 충족하는지 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 최대 입력 데이터 속도를 초과한 경우 제조자가 장치 동작을 지정하였음을 확인하여야 한다.</li> <li>- 460-노드의 문서화된 증거를 검사하여 지원되는 데이터를 제외한 다른 모든 수신 데이터를 삭제하는지 확인하여야 한다.</li> <li>- 제공되는 경우, 제조자의 문서를 참조하여 지원되는 모든 VLAN 서비스에 대한 최대 전송 속도가 지정되어 있는지 문서화된 증거를 검사하여 확인하고 각 VLAN의 모든 IEC 61162-450 호환 데이터가 최대 전송 속도를 충족하는지 문서화된 증거를 분석 평가를 통해 확인하여야 한다.</li> <li>- VLAN이 제공되는 경우, 문서화된 증거를 검사하여 460-노드가 VLAN IEEE 802.1Q를 지원하는지 확인하여야 한다.</li> </ul>	
10.5.2 보안				
4	일반 보안 Security in general	10.5.2.1	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 시료가 무선 LAN 인터페이스 또는 무선 AP 기능을 사용하지 않는지 확인하여야 한다.</li> <li>- VLAN이 제공되는 경우, 분석 평가를 통해 사용 중인 VLAN 터널링 프로토콜이 없는지 확인하여야 한다.</li> </ul>	
5	서비스 거부 Denial of service behaviour	10.5.2.2	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 최대 작동 입력 대역폭이 선언되어 있는지 확인하여야 한다.</li> <li>- 제조자가 선언한 최대 트래픽을 생성하기 위하여 시뮬레이션 방식을 사용한다. 시료가 성능요구사항을 만족하는지 관찰하여 확인하여야 한다.</li> <li>- 최소 10분 동안 제조자가 선언한 최대 트래픽의 200%를 생성하기 위하여 시뮬레이션 방식을 사용한다. 10분 후 100% 트래픽으로 돌아간다. 분석 평가</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			<p>를 통해 제조자의 문서에 기술된 대로 460-노드가 트래픽 변경 중 및 변경 후 동작하는지 확인하여야 한다.</p> <ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 최대 작동 출력 대역폭이 선언되어 있는지 확인하여야 한다.</li> <li>- 문서화된 증거에 대한 분석 평가로 확인하거나 시료 자체의 분석 평가로 시료가 선언된 최대 작동 출력 대역폭을 초과하지 않는지 확인하여야 한다.</li> </ul>	
6	REDS 보안 Security for REDS	10.5.2.3	<ul style="list-style-type: none"> <li>- 제조자의 문서를 참조하여 REDS (USB 포트, 디스크 드라이브 등)에 대한 연결 지점 수가 시스템 작동 및 수명 유지 관리 및 지원에 필요한 절대 최소값으로 제한되어 있는지 문서화된 증거를 검사하여 확인한다. 도구나 키 없이 사용자가 쉽게 접근할 수 없도록 다른 연결 지점이 차단되었는지 관찰하여 확인하여야 한다.</li> <li>- REDS용 USB 기반 연결 포인트의 경우, 키보드나 마우스 장치 (즉, 08h 이외의 USB 장치 클래스)를 하나씩 포트에 연결하고 시료가 연결된 장치의 인식을 거부하고 연결된 장치와의 기능 수행을 거부하는지 분석 평가를 통해 확인하여야 한다.</li> <li>- 데이터 소스 이외의 다른 목적을 위한 USB 기반 포트의 경우, 사용자가 쉽게 접근하는 것을 차단하는지 관찰하여 확인하여야 한다.</li> <li>- USB 기반 REDS 이외의 다른 연결 포인트의 경우, 기술적으로 가능한 REDS의 역할에 대해 제조자가 제공한 정보를 사용한다. 이러한 REDS가 기술적으로 역할 변경이 가능한 경우, 비 데이터 저장 장치의 예를 하나씩 포트에 연결하고 시료가 연결된 장치의 인식을 거부하고 연결된 장치와의 기능 수행을 거부하는지 분석 평가를 통해 확인한다.</li> <li>- 장치를 REDS용 연결 포인트에 하나씩 연결하거나 매체를 REDS (디스크 드라이브 등)에 삽입하고 시료에서의 모든 자동 실행이 금지되는지 분석 평가를 통해 확인하여야 한다.</li> <li>- 시료가 REDS로부터 모든 유형의 파일의 수동 실행을 제공하는 경우, 분석 평가를 통해 디지털 서명 또는 특수키로 검증된 파일에 대해서만 수동 실행이 가능함을 확인하여야 한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			- 시료에서 사용할 수 있는 실행 불가능한 파일에 대한 제조자의 문서를 사용한다. 분석 평가를 통해 시료에서 사용하기 전에 제조자의 문서에 기술된 대로 실행 불가능한 파일이 검증되는지 확인하여야 한다.	
7	구성 설정에 대한 접근 제어 Access control to configuration setup	10.5.2.4	- 제조자의 문서를 검사하여 시료의 구성을 변경하기 위한 접근은 사용자 인증을 받는지 확인하여야 한다.  - 분석 평가를 통해 장치 설정을 변경하기 전에 사용자 인증이 8자 이상의 긴 암호, RSA 키 또는 다른 적절한 방법에 기반 하는지 확인하여야 한다.  - 암호는 소문자, 대문자, 숫자, 특수 문자의 네 가지 문자 유형 중 세 가지 이상이 없으면 허용되지 않는지 관찰하여 확인하여야 한다.  - 제조자의 문서를 검사하여 사용자 설명서에 강력한 암호 사용에 대한 지침이 포함되어 있는지 확인하여야 한다.	
8	비 제어 네트워크에 대한 직접 접근 Direct access to uncontrolled network	10.5.2.5	- 다음 시험은 460-노드가 비 제어 네트워크에 연결된 다른 장비와 정보를 교환하기 위해 직접 연결된 경우 적용되어야 한다.  - 분석 평가를 통해 시료의 제조 기본 설정이 비 제어 네트워크와 직접 연결될 수 없게 하는지 확인하여야 한다.  - 구성된 각각의 직접 데이터 교환에 대해 직접 연결을 활성화하기 위한 전제 조건으로 460-게이트웨이 또는 460-무선 게이트웨이에서 VPN이 설정되었으며 460-노드의 운영자만 직접 연결을 활성화 할 수 있는지 분석 평가를 통해 확인하여야 한다.  - 각각의 직접 데이터 교환에 대해 다음을 관찰하여 확인하여야 한다. <ul style="list-style-type: none"> <li>• 직접 연결이 활성화되면 영구적으로 표시된다.</li> <li>• 직접 연결이 활성화되면 주의가 생성된다.</li> <li>• 제공되는 경우, 사전 정의된 기간이 지난 후 주의가 경계로 대체된다.</li> <li>• 주의 및 경계는 직접 연결 종료 후 제거된다.</li> </ul> - 제조자의 문서를 검사하여 VPN에 사용되는 암호화 알고리즘이 6.3.3에 명시된 암호화 강도 요구사항을 충족하는지 확인하여야 한다.	
9	이중화 Redundancy	10.5.3	- 제조자의 문서를 참조하여 시료의 이중화 기능을 위해 제공된 수단을 문서화된 증거를 검사하여 확인하여야 한다.	

No.	시험 항목	IEC 61162-460	내용	비고
10	모니터링 Monitoring	10.5.4	- 시스로그에 대한 모니터링 정보는 구성정보를 분당 1회 이하로 30분마다 주기적으로 시료에 의해 제공되는지 관찰하여 확인하여야 한다.	
10.6 460-스위치				
11	리소스 할당 Resource allocation	10.6.1	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 인터페이스 식별자, MAC 주소 또는 IP 주소, 프로토콜 번호 및 포트 번호의 조합으로 식별되는 스트림 또는 네트워크 플로우를 구성할 수 있는 수단이 제공되는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 등록된 모든 스트림에 대해 네트워크 리소스를 할당하기 위한 수단이 제공되는지 확인하여야 한다.</li> <li>- 들어오고 나가는 모든 트래픽을 등록한다. 시뮬레이션을 사용하여 등록된 트래픽과 등록되지 않은 트래픽을 모두 생성한다. 분석 평가를 통해 들어오고 나가는 트래픽만 통과하고 등록되지 않은 트래픽은 모두 차단되는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 리소스 할당을 사용하여 각 인터페이스의 총 트래픽 양을 450-노드 및 460-노드로 제한하는 수단이 제공되는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 두 개의 460-노드를 시료에 연결하고 설정된 최대 트래픽을 사용하여 서로 통신하도록 노드를 설정한다. 분석 평가를 통해 모든 트래픽이 시료를 통과하는지 확인하여야 한다. 10분 동안 설정된 최대 트래픽에 보다 트래픽을 50% 증가시킨다. 과도한 트래픽이 차단되는지 분석 평가를 통해 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 VLAN이 제공되는 경우 각 인터페이스에 대해 가상네트워크(VLAN)를 구성할 수 있는 수단이 제공되는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 VLAN이 제공되는 경우 VLAN 프로토콜 IEEE 802.1Q가 지원되는지 확인하여야 한다.</li> <li>- 문서를 검사하여 시료가 IGMP 스누핑(snooping)을 통해 멀티캐스트(multicast) 트래픽을 필터링할 수단을 가지고 있는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 시료를 병렬로 연결하거나 460-스위치, 460-포워드, 460-노드 및 450-노드에 하</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			<p>나씩 연결한다. IGMP 스누핑으로 네트워크 트래픽을 필터링하기 위해 시료에 멀티캐스팅 그룹을 설정한다. 시료가 이 멀티캐스팅 그룹에 대한 IGMP 멤버십 쿼리(query)를 전송하는지 관찰하여 확인하여야 한다.</p>	
12	루프 방지 Loop prevention	10.6.2	<ul style="list-style-type: none"> <li>- 시료가 루프 방지 메커니즘을 제공하는지 문서화된 증거로 확인하여야 한다.</li> <li>- RSTP가 제공되는 경우, 제조자의 문서를 검사하여 RSTP 프로토콜 버전 IEEE 802.1D-2004가 지원되는지 확인하여야 한다.</li> <li>- 예를 들면 유니캐스트(unicast)를 사용하여 루프 토폴로지용 3개의 460-스위치를 각 스위치에서 하나 이상의 460-노드와 연결되도록 한다. 분석 평가를 통해 스위치에서 데이터가 중복되지 않는지 확인하여야 한다.</li> <li>- 예를 들면 유니캐스트(unicast)를 사용하여 루프 토폴로지용 3개의 460-스위치를 각 스위치에서 하나 이상의 460-노드와 연결되도록 한다. 인접한 각 460-스위치 사이의 케이블을 하나씩 분리한다. 분석 평가를 통해 5초 이내에 460-노드 간에 데이터가 도달할 수 있는지 확인하여야 한다.</li> </ul>	
10.6.3 보안				
13	일반 보안 Security general	10.6.3.1	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 시료가 무선 LAN 인터페이스 또는 무선 AP 기능을 사용하지 않는지 확인하여야 한다.</li> <li>- VLAN이 제공되는 경우, 사용 중인 VLAN 터널링 프로토콜이 없는지 분석 평가를 통해 확인하여야 한다.</li> </ul>	
14	서비스 거부 행동 Denial of service behaviour	10.6.3.2	<ul style="list-style-type: none"> <li>- 문서화된 증거를 검사하여 시료가 ICMP 및 IGMP DoS 방지를 제공하는지 확인하여야 한다.</li> </ul>	
15	구성 설정에 대한 접근 제어 Access control to configuration setup	10.6.3.3	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 시료의 구성을 변경하기 위한 접근은 사용자 인증을 받는지 확인하여야 한다.</li> <li>- 분석 평가를 통해 장치 설정을 변경하기 전에 사용자 인증이 8자 이상의 긴 암호, RSA 키 또는 다른 적절한 방법에 기반 하는지 확인하여야 한다.</li> <li>- 암호는 소문자, 대문자, 숫자, 특수 문자의 네 가지 문자 유형 중 세 가지 이상이 없으면 허용되지 않는지 관찰하여 확인하여야 한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			- 제조자의 문서를 검사하여 사용자 설명서에 강력한 암호 사용에 대한 지침이 포함되어 있는지 확인하여야 한다.	
16	네트워크에 대한 접근 제어 Access control for network	10.6.3.4	- 제조자의 문서를 검사하여 각 물리적 포트의 IP 주소, 프로토콜 번호 및 포트 번호를 기반으로 플로우를 허용하거나 거부할 수 있는 수단이 제공되는지 확인하여야 한다.  - 분석 평가를 통해 각 물리적 포트에 대한 MAC 주소를 기반으로 장치를 허용하거나 거부할 수 있는 수단이 제공되는지 확인하여야 한다. 시료가 보안구역에 설치를 지원하는 경우, 분석 평가를 통해 MAC 주소에 의한 인증을 활성화 또는 비활성화 하도록 수단을 구성할 수 있는지 확인하여야 한다.	
17	추가 보안 문제 Additional security issues	10.6.3.5	- 분석 평가를 통해 스위치 Off 또는 전원 고장 후 전원이 다시 공급될 때 이전 구성으로 시료가 정상 작동을 계속하는지 확인하여야 한다.  - 분석 평가를 통해 시스템 관리 기능에 이전에 저장된 구성으로 되돌리기 위한 수단이 제공되는지 확인하여야 한다.  - 문서화된 증거를 검사하여 물리적으로 보호된 위치에 시료를 설치하기 위한 지침이 제공되는지 확인하여야 한다.	
18	모니터링 Monitoring	10.6.4	- 다음 모니터링 정보가 시료에 의해 제공되는지 관찰하여 확인하여야 한다. <ul style="list-style-type: none"> <li>• 인터페이스 정보</li> <li>• 인터페이스 당 인접 MAC 주소 목록</li> <li>• 인접 MAC 주소 변경</li> </ul> - 네트워크 모니터링 기능의 SNMP 쿼리(query)에 대한 응답으로 네트워크 구성 정보가 시료에 의해 전송되는지 관찰하여 확인하여야 한다. 분석 평가를 통해 인접 MAC 주소 변경과 같은 구성 변경이 발생할 때마다 최소한 시스로그 (비 조건부 송신) 또는 SNMP-트랩 (네트워크 모니터링 기능에 의해 요청된 경우)에 의해 정보가 보고되는지 확인하여야 한다. 시스로그를 사용하는 구성 정보가 분당 한 번 이상 보고되지 않는지 관찰하여 확인하여야 한다.  - 네트워크 모니터링 기능의 SNMP 쿼리(query)에 대한 응답으로 시료가 인터페이스 입/출력 링크 활용률 (평균 5분 이상)을 전송하는지 관찰하여 확인하여야 한다. 중요한 변경사항 (트래픽이 네트워크 용량의 0% ~100% 범위에서 미리 정의된 한계를 초과함)이 있을 때마다 정보가 최소한 시스로그 (비 조건부 전송) 또는 SNMP 트랩 (네트워크 모니터링	



No.	시험 항목	IEC 61162-460	내용	비고
			기능에 의해 요청된 경우)에 의해 보고되는지 관찰하여 확인하여야 한다. 시스로그를 사용하는 정보가 3초에 한 번 이상 보고되지 않는지 관찰하여 확인하여야 한다.	
10.7 460-포워더				
19	트래픽 분리 Traffic separation	10.7.1	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 460-네트워크와 제어된 네트워크 또는 기타 460-네트워크 간에 트래픽의 전부 또는 하위 일부를 전송하기 위한 수단이 제공되는지 확인하여야 한다.</li> <li>- 제조자의 지침을 따르고 460-네트워크와 제어된 네트워크 또는 기타 460-네트워크 간에 최대 트래픽 플로우를 제한하도록 시료를 설정한다. 분석 평가를 통해 전송된 총 트래픽이 설정된 최대값을 초과하지 않는지 확인하여야 한다.</li> <li>- VLAN 기능이 제공되는 경우, 제조자의 문서를 검사하여 460-네트워크와 제어된 네트워크 또는 시료에서 VLAN이 있는 기타 460-네트워크 간의 전송/연결 해제 구성을 위한 수단이 제공되는지 확인하여야 한다.</li> <li>- VLAN 기능이 제공되는 경우, 제조사 문서를 검사하여 460-포워더가 VLAN 프로토콜 IEEE 802.1Q를 구현하는지 확인하여야 한다.</li> <li>- 문서를 검사하여 시료가 IGMP 스누핑에 의해 멀티캐스트 트래픽을 필터링할 수단을 가지고 있는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 시료를 병렬로 연결하거나 460-스위치, 460-포워더, 460-노드 및 450-노드에 하나씩 연결한다. IGMP 스누핑으로 네트워크 트래픽을 필터링하기 위해 시료에 멀티캐스팅 그룹을 설정한다. 시료가 이 멀티캐스팅 그룹에 대한 IGMP 멤버십 쿼리를 전송하는지 관찰하여 확인하여야 한다.</li> </ul>	
20	리소스 할당 Resource allocation	10.7.2	<ul style="list-style-type: none"> <li>- 들어오고 나가는 모든 트래픽을 등록한다. 시뮬레이션을 사용하여 등록된 트래픽과 등록되지 않은 트래픽을 모두 생성한다. 분석 평가를 통해 들어오고 나가는 트래픽만 통과하고 등록되지 않은 트래픽은 모두 차단되는지 확인하여야 한다.</li> <li>- 분석 평가를 통해 리소스 할당을 사용하여 각 인터페이스의 총 트래픽 양을 450-노드 및 460-노드로 제한하는 수단이 제공되는지 확인하여야 한다.</li> <li>- 두 개의 460-노드를 시료에 연결하고 설정된 최대 트래픽을 사용하여 서로 통신하도록 노드를 설정한</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			<p>다. 모든 트래픽이 시료를 통과하는지 관찰하여 확인하여야 한다. 설정된 최대 트래픽 이상으로 트래픽을 증가시킨다. 분석 평가를 통해 과도한 트래픽이 차단되는지 확인하여야 한다.</p> <ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 인터페이스 식별자, MAC 주소 또는 IP 주소, 프로토콜 번호 및 포트 번호의 조합으로 식별되는 스트림 또는 네트워크 플로우를 구성하기 위한 수단이 제공되는지 확인하여야 한다. 등록된 모든 스트림에 네트워크 리소스를 할당하기 위한 수단이 제공되는지 관찰하여 확인하여야 한다.</li> <li>- VLAN 기능이 제공되는 경우, 분석 평가를 통해 자원 할당을 사용하여 주어진 값에 대해 제어된 네트워크 또는 460-네트워크에 대한 각 VLAN의 총 트래픽 양을 제한하는 수단이 제공되는지 확인하여야 한다.</li> </ul>	
21	트래픽 우선순위 Traffic prioritisation	10.7.3	<ul style="list-style-type: none"> <li>- 시뮬레이션을 사용하여 가장 낮은 우선순위를 포함하는 다른 우선순위를 가진 세 가지 다른 트래픽 유형을 설정한다. 트래픽 한도를 가장 우선순위가 높은 트래픽에 대해서만 충분하도록 설정한다. 데이터 손실이 발생할 때까지 우선순위가 가장 낮은 트래픽을 증가시켜야 한다.</li> <li>- 분석 평가를 통해 우선순위가 가장 높은 트래픽의 손실률이 가장 낮고 우선순위가 가장 낮은 트래픽의 손실률이 가장 높은 지 확인하여야 한다.</li> <li>- 각 포트에 대해 회선의 물리적 용량의 50%보다 높거나 30초 동안 포트에 설정된 최대 입력 데이터 속도보다 높은 증가된 트래픽을 생성하고 회선의 물리적 용량의 50% 미만 및 포트에 설정된 최대 입력 데이터 속도 미만으로 되돌린다. 분석 평가를 통해 트래픽이 회선의 물리적 용량의 50% 미만이고 포트에 설정된 최대 입력 데이터 속도 미만이 될 때까지 우선순위가 낮은 트래픽이 감소했는지 확인한다.</li> <li>- 분석 평가를 통해 각 포트에 대하여 지난 30초 동안 전송된 트래픽의 양이 포트에 설정된 최대 입력 데이터 속도보다 높을 때까지 최고 우선순위 트래픽이 무손실 상태로 계속 유지되고, 그 후에는 최고 우선순위 트래픽의 일부가 드롭 될 수 있음을 확인하여야 한다.</li> <li>- 분석 평가를 통해 드롭이 사용된 각 30초 동안 시스로그에 의해 보고되거나 또는 SNMP 트랩 방법에 대한 응답으로 드롭 사용이 보고되는지 확인한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
10.7.4 보안				
22	일반 General	10.7.4.1	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 시료가 무선 LAN 인터페이스 또는 무선 AP 기능을 사용하지 않는지 확인하여야 한다.</li> <li>- VLAN이 제공되는 경우, 사용 중인 VLAN 터널링 프로토콜이 없는지 분석 평가를 통해 확인하여야 한다.</li> </ul>	
23	서비스 거부 행동 Denial of service behaviour	10.7.4.2	<ul style="list-style-type: none"> <li>- 문서화된 증거를 검사하여 시료가 ICMP 및 IGMP DoS 방지를 제공하는지 확인하여야 한다.</li> </ul>	
24	구성 설정에 대한 접근 제어 Access control to configuration setup	10.7.4.3	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 시료의 구성을 변경하기 위한 접근은 사용자 인증을 받는지 확인하여야 한다.</li> <li>- 분석 평가를 통해 장치 설정을 변경하기 전에 사용자 인증이 8자 이상의 긴 암호, RSA 키 또는 다른 적절한 방법에 기반 하는지 확인하여야 한다.</li> <li>- 암호는 소문자, 대문자, 숫자, 특수 문자의 네 가지 문자 유형 중 세 가지 이상이 없으면 허용되지 않는지 관찰하여 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 사용자 설명서에 강력한 암호 사용에 대한 지침이 포함되어 있는지 확인하여야 한다.</li> </ul>	
25	네트워크에 대한 접근 제어 Access control for network	10.7.4.4	<ul style="list-style-type: none"> <li>- 제조자의 문서를 검사하여 각 물리적 포트의 IP 주소, 프로토콜 번호 및 포트 번호를 기반으로 플로우를 허용하거나 거부할 수 있는 수단이 제공되는지 확인하여야 한다.</li> <li>- 분석 평가를 통해 각 물리적 포트에 대한 MAC 주소를 기반으로 장치를 허용하거나 거부할 수 있는 수단이 제공되는지 확인하여야 한다. 시료가 보안구역에 설치를 지원하는 경우, 분석 평가를 통해 MAC 주소에 의한 인증을 활성화 또는 비활성화 하도록 수단을 구성할 수 있는지 확인하여야 한다.</li> </ul>	
26	추가 보안 Additional security	10.7.4.5	<ul style="list-style-type: none"> <li>- 스위치 Off 또는 전원 차단 후 전원이 다시 공급될 때 이전 구성으로 시료가 정상 작동을 계속하는지 관찰하여 확인하여야 한다.</li> <li>- 분석 평가를 통해 시스템 관리 기능에 이전에 저장된 구성으로 되돌리기 위한 수단이 제공되는지 확인하여야 한다.</li> <li>- 제조자의 문서를 검사하여 물리적 접근이 제한된 위치에 시료를 설치하기 위한 지침이 제공되는지 확인하여야 한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
27	모니터링 Monitoring	10.7.5	<p>- 다음 모니터링 정보가 시료에 의해 제공되는지 관찰하여 확인하여야 한다.</p> <ul style="list-style-type: none"> <li>• 인터페이스 정보</li> <li>• 인터페이스 당 인접 MAC 주소 목록</li> <li>• 인접 MAC 주소 변경</li> </ul> <p>- 네트워크 모니터링 기능의 SNMP 쿼리(query)에 대한 응답으로 네트워크 구성 정보가 시료에 의해 전송되는지 관찰하여 확인하여야 한다. VLAN이 제공되는 경우 현재 VLAN 구성 정보가 SNMP 쿼리에 대한 응답으로 전송되는지 관찰하여 확인하여야 한다. 분석 평가를 통해 인접 MAC 주소 변경과 같은 구성 변경이 발생할 때마다 최소한 시스로그 (비조건부 송신) 또는 SNMP-트랩 (네트워크 모니터링 기능에 의해 요청된 경우)에 의해 정보가 보고되는지 확인하여야 한다. 시스로그를 사용하는 구성 정보가 분당 한 번 이상 보고되지 않는지 관찰하여 확인하여야 한다.</p> <p>- 네트워크 모니터링 기능의 SNMP 쿼리(query)에 대한 응답으로 시료가 인터페이스 입/출력 링크 활용률 (평균 5분 이상)을 전송하는지 관찰하여 확인하여야 한다. 중요한 변경사항 (트래픽이 네트워크 용량의 0% ~100% 범위에서 미리 정의된 한계를 초과함)이 있을 때마다 정보가 최소한 시스로그 (비조건부 전송) 또는 SNMP 트랩 (네트워크 모니터링 기능에 의해 요청된 경우)에 의해 보고되는지 관찰하여 확인하여야 한다. 시스로그를 사용하는 정보가 3초에 한 번 이상 보고되지 않는지 관찰하여 확인하여야 한다.</p>	
10.8 460-게이트웨이				
28	서비스 거부 행동 Denial of service behaviour	10.8.1	<p>- 문서화된 증거를 검사하여 시료가 ICMP 및 IGMP DoS 방지를 제공하는지 확인하여야 한다.</p>	
29	구성 설정에 대한 접근 제어 Access control to configuration setup	10.8.2	<p>- 제조자의 문서를 검사하여 시료의 구성을 변경하기 위한 접근은 사용자 인증을 받는지 확인하여야 한다.</p> <p>- 분석 평가를 통해 장치 설정을 변경하기 전에 사용자 인증이 8자 이상의 긴 암호, RSA 키 또는 다른 적절한 방법에 기반 하는지 확인하여야 한다.</p> <p>- 암호는 소문자, 대문자, 숫자, 특수 문자의 네 가지 문자 유형 중 세 가지 이상이 없으면 허용되지 않는지 관찰하여 확인하여야 한다.</p> <p>- 제조자의 문서를 검사하여 사용자 설명서에 강력</p>	

No.	시험 항목	IEC 61162-460	내용	비고
30	통신 보안 Communication security	10.8.3	<p>한 암호 사용에 대한 지침이 포함되어 있는지 확인하여야 한다.</p> <ul style="list-style-type: none"> <li>- 제조자 문서를 통해 비제어 네트워크와 460-네트워크 사이의 직접연결이 460-게이트웨이나 460-무선 게이트웨이에서만 활성화 될 수 있음을 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 460-네트워크와 비제어 네트워크 간에 시료에서 시작되는 VPN 연결을 설정한다. 분석 평가를 통해 VPN이 제공되는지 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 VPN에 사용되는 암호화 알고리즘이 다음과 같은 암호화 강도 요구사항을 충족하는지 확인하여야 한다. <ul style="list-style-type: none"> <li>• 최소 2048비트 키 길이(256바이트)이상의 비대칭 암호화 알고리즘</li> <li>• 최소 256비트 키 길이(32바이트)의 대칭 암호화 알고리즘</li> </ul> </li> <li>- 문서화된 증거를 검사하여 인증서 전달이 신뢰 체인에 기반 하거나 또는 개인 키/인증서가 안전한 수동 방식으로 교환되거나 또는 수동 방법 및 메시지의 조합을 사용하는지 확인하여야 한다.</li> </ul>	
31	방화벽 Firewall	10.8.4	<ul style="list-style-type: none"> <li>- 분석적 평가를 통해 460-네트워크에 대한 모든 직접 연결이 제조자의 기본 구성에서 비활성화 되어 있는지 확인하여야 한다.</li> <li>- 460-네트워크와 비제어 네트워크 사이에 시료를 설정한다. 비제어 네트워크, 460-네트워크 및 DMZ의 주소 범위에 대해 핑 발생기(Ping Generator)를 20개의 다른 IP주소로 설정한다. 분석적 평가를 통해 다음 패킷이 시료를 통과하지 않는지 확인하여야 한다. <ul style="list-style-type: none"> <li>• 460-네트워크의 내부 주소범위에 대한 핑 테스트</li> <li>• EUT의 DMZ 주소범위에 대한 핑 테스트</li> <li>• 비제어 네트워크 주소범위에 대한 핑 테스트</li> </ul> </li> <li>- 관찰을 통해 시료가 출발지 및 목적지 IP 주소, 프로토콜 및 포트 번호로 구성된 외부/내부 방화벽 규칙으로 트래픽을 등록하는지 확인하여야 한다.</li> <li>- 관찰을 통해 시료가 지난 12개월 동안 모든 직접 연결에 대한 목록을 제공하는지 확인하여야 한다.</li> <li>- 분석적 평가를 통해 시료가 출발지 IP 주소, 목적지 IP 주소, 연결 시작시간 및 종료시간, 프로토콜</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
			<p>및 포트번호를 포함한 각 연결에 대한 상태정보와 함께 460-네트워크와 비제어 네트워크 사이에 활성화된 직접 연결에 대한 목록을 제공하는지 확인하여야 한다.</p> <ul style="list-style-type: none"> <li>- 분석적 평가를 통해 비제어 네트워크에서 460-노드와의 직접연결을 허용하기 위해 제공된 수단이 방화벽의 460-네트워크 측에서의 작업에 의해서만 활성화 될 수 있음을 확인하여야 한다. 제조사의 문서를 검사하여 비제어 네트워크에서 활성화 할 수 없음을 확인하여야 한다. 예를 들어 선교의 선원의 허가를 받은 후에만 작업을 수행 할 수 있도록 하는 방법이 제공되는지 확인하여야 한다.</li> <li>- 관찰을 통해 시료가 시간 연장을 위한 사용자 개입이 없는 한 4시간을 초과하지 않는 사전 정의된 시간 후에 모든 직접 연결을 자동으로 종료하는지 확인하여야 한다.</li> <li>- 관찰을 통해 시료가 연결이 10분을 초과하지 않는 사전 정의된 시간 동안 유휴 상태일 때 모든 직접 연결을 자동으로 종료하는지 확인하여야 한다.</li> <li>- 460-네트워크와 비제어 네트워크 사이의 직접연결이 제공되는 경우, 관찰을 통해 활성화상태가 표시되는지 확인하거나, 분석적 평가를 통해 활성화 상태가 '주의'를 발생시키는지 확인하여야 한다.</li> </ul> <p>참고) 주의의 생성 및 표시는 네트워크 모니터링에 대한 경고를 표시하는 장치에서 수행될 수 있다.</p>	
32	응용 서버 Application server	10.8.5	<ul style="list-style-type: none"> <li>- 제조사의 문서를 검사하여 응용 서버가 비제어 네트워크를 통해 연결된 클라이언트를 인증할 수 있는 수단(예: 암호)을 제공하는지 확인하여야 한다.</li> <li>- 분석적 평가를 통해 3번 계층으로 전달 또는 라우팅이 비활성화 되었는지 확인하여야 한다(즉, 패킷 라우팅이 허용되지 않음).</li> <li>- 10.5.에 따라 460-노드 요구사항을 준수하는지 확인하여야 한다.</li> <li>- 제조사의 문서를 검사하여 악성코드로부터 보호하기 위한 수단이 컴퓨터 플랫폼에 적절하다고 명시되어 있는지 확인하여야 한다.</li> </ul>	
33	DMZ 파일 저장소에 상호 운용 접근	10.8.6	<ul style="list-style-type: none"> <li>- 관찰을 통해 DMZ와 비제어 네트워크 사이에 파일을 다운로드하고 업로드 할 수 있는지 확인하여야 한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
	Interoperable access to file storage of DMZ		- 관찰을 통해 DMZ와 460-네트워크 간의 파일을 다운로드하고 업로드 할 수 있는지 확인하여야 한다 (제공되는 경우). - DMZ내의 파일저장소에 대한 접근이 제공되는 경우 제조자 문서를 검사하여 SMB 또는 SFTP와 같은 프로토콜이 제공되었는지 확인하여야 한다. - 문서화된 증거를 검사하여 파일저장소 및 DMZ의 관련 데이터 트래픽 대한 시료 접근이 IEC 61162-450 및 460-노드에 명시된 ONF, NF에 대한 요구사항을 충족하는지 확인하여야 한다(구현된 경우).	
34	추가 보안 Additional security	10.8.7	- 스위치 Off 또는 전원 차단 후 전원이 다시 공급 될 때 이전 구성으로 시료가 정상 작동을 계속하는 지 관찰하여 확인하여야 한다. - 분석 평가를 통해 시스템 관리 기능에 이전에 저장된 구성으로 되돌리기 위한 수단이 제공되는지 확인하여야 한다. - 제조자의 문서를 검사하여 물리적 접근이 제한된 위치에 시료를 설치하기 위한 지침이 제공되는지 확인하여야 한다.	
10.9 460-무선 게이트웨이				
35	일반 General	10.9.1	- 문서화된 증거를 검사하여 시료가 460-게이트웨이 요건을 충족하는지 확인하여야 한다(10.8 참조).	
36	보안 Security	10.9.2	- 관찰을 통해 무선 액세스 포인트(AP) 기능이 활성화 되지 않았는지 확인하여야 한다. - 관찰을 통해 전달(forwarding)기능이 허용되지 않는지 확인하여야 한다. - 제조자 문서를 통해 460-네트워크에 대한 모든 트래픽이 IEC 61162-450 트래픽을 준수 하는지 확인하여야 한다. - 문서화된 증거를 검사하여 VPN에 사용되는 암호화 알고리즘이 다음과 같은 암호화 강도 요구사항을 충족하는지 확인하여야 한다. <ul style="list-style-type: none"> <li>• 최소 2048비트 키 길이(256바이트)이상의 비대칭 암호화 알고리즘</li> <li>• 최소 256비트 키 길이(32바이트)의 대칭 암호화 알고리즘</li> </ul> - 무선 AP를 활성화 하고 관찰을 통해 무선 AP에 대한 모든 연결이 인증만으로 설정 되었는지 확인하여야 한다.	

No.	시험 항목	IEC 61162-460	내용	비고
37	제어 네트워크 Controlled network	10.10	<ul style="list-style-type: none"> <li>- 문서화된 증거를 검사하여 제어 네트워크가 물리적 인프라에 직접 접근하거나 예를 들어 무선 인터페이스를 통해 승인되지 않은 트래픽을 네트워크에 삽입할 수 없음을 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 사용자가 특별히 작업을 수행하도록 허가되지 않은 한, 제어 네트워크가 승인되지 않은 트래픽을 네트워크에 삽입하는데 사용할 수 있는 운영 시스템이나 기능에 직접 접근하는 것을 방지하기 위한 수단을 제공하는지 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 제어 네트워크가 승인되지 않은 REDS 또는 승인되지 않은 콘텐츠가 있는 REDS에서 네트워크의 모든 노드나 장치로 데이터를 전송하는 것을 방지하는 수단을 제공하는지 확인하여야 한다.</li> </ul>	
10.11 네트워크 모니터링 기능				
38	일반 General	10.11.1	<ul style="list-style-type: none"> <li>- 시료가 네트워크 모니터링 기능을 제공하지 않는 경우 설치문서를 검사하여 시료는 다른 장비가 네트워크 모니터링 기능을 제공하는 네트워크에만 연결되어야함을 확인하여야 한다.</li> <li>- 관찰을 통해 시료가 로컬 HMI 또는 경고관리 인터페이스를 통해 모니터링을 제공하는지 확인하여야 한다.</li> <li>- 제조자가 선교에 설치를 위한 적합성을 선언한 경우, 관찰을 통해 시료가 경고관리 인터페이스를 제공하는지 확인하여야 한다.</li> <li>- 주의 및 경계를 발생시키도록 시뮬레이션을 설정한다. 관찰을 통해 시료가 모든 알림을 보고하고 경고관리 인터페이스를 제공하는 경우 이전된 책임, 원격 확인(Ack) 및 원격 음소거 명령을 수용할 수 있는지 확인하여야 한다.</li> <li>- 주의 및 경계를 발생시키고 460-스위치 및 460-포워더에서 이벤트와 보고서를 생성하도록 시뮬레이션을 설정한다. 관찰을 통해 네트워크 모니터링 기능 및 460-스위치와 460-포워더의 이벤트 및 보고서의 모든 경고가 시료에 기록되었는지 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 시료가 지난 3개월 또는 최근 10,000개 이벤트 중 더 작은 이벤트와 함께 정보를 표시하는 기능을 가지고 있는지 확인하여야 한다.</li> </ul>	



No.	시험 항목	IEC 61162-460	내용	비고
39	네트워크 부하 모니터링 기능  Network load monitoring function	10.11.2	<p>- 관찰을 통해 시스템 문서에 최대 네트워크 부하의 모든 스위치와 스위치, 파워더 및 게이트웨이 사이의 분석이 포함되어 있는지 확인하여야 한다.</p> <p>- 시뮬레이션을 사용하여 관찰을 통해 시료가 30초마다 SNMP-쿼리를 사용하거나 15분마다 SNMP-트랩방법과 SMNP-쿼리를 조합을 사용하여 모든460-스위치와 460-파워더의 트래픽 플로우 정보를 요청하는지 확인하여야 한다.</p> <p>- 시뮬레이션을 사용하고 시료가 다음 기능을 위해 SNMP 또는 시스로그의 정보 또는 두 가지 모두의 조합을 사용할 수 있는지 관찰을 통해 확인하여야한다.</p> <ul style="list-style-type: none"> <li>• 관측된 네트워크 부하가 10분 이내에 3회 이상 30초 동안 최대 네트워크 용량의 80% 제한을 초과할 경우 '주의'를 발생한다.</li> <li>• 관측된 네트워크 부하가 10분 이내에 10회 이상 30초 동안 최대 네트워크 용량의 80% 한계를 초과할 경우 '경계'를 발생한다.</li> </ul>	
40	이중화 모니터링 기능 Redundancy monitoring function	10.11.3	<p>- 관찰을 통해 시스템 문서에 이중으로 사용할 수 있는 데이터 소스 목록이 포함 되어 있는지 확인하여야 한다.</p> <p>- 관찰을 통해 목록은 이 데이터를 사용할 수 있는 각 중복 네트워크 주소에 대해 데이터 소스의 이름, 두 개 이상의 MAC주소, 인터페이스 번호 및 사용 가능한 인터페이스 대안을 제공 하는지 확인하여야 한다.</p> <p>- 시뮬레이션을 사용하여 관찰을 통해 시료가 30초마다 SNMP-쿼리를 사용하거나 15분마다 SNMP-트랩방법과 SMNP-쿼리를 조합을 사용하여 모든460-스위치와 460-파워더에서 네트워크 구성 정보를 요청하는지 확인하여야 한다.</p> <p>- 시뮬레이션을 사용하여 관찰을 통해 시료가 두 개 미만의 MAC주소 또는 목록의 데이터 소스에 사용할 수 있는 인터페이스가 2개 미만인 MAC주소 하나가 시료에서 30초마다 수행되는 모든 SNMP 요청에 대해 2분 동안 손실 되는 경우 SNMP와 시스로그의 정보를 사용하여 '주의'를 생성 하는지 확인하여야 한다.</p> <p>- 관찰을 통해 '주의'는 요구사항을 준수 하는지 확인하여야 한다.</p>	

No.	시험 항목	IEC 61162-460	내용	비고
41	네트워크 토폴로지 모니터링 기능 Network topology monitoring function	10.11.4	<ul style="list-style-type: none"> <li>- 관찰을 통해 시스템 설명서에 승인된 장치목록이 포함되어 있는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 관찰을 통해 시료가 30분마다 SNMP-쿼리를 사용하거나 15분마다 SNMP-트랩방법과 SMNP-쿼리를 조합을 사용하여 모든460-스위치와 460-포워더에서 네트워크 토폴로지 구성 정보를 요청하는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 관찰을 통해 시료가 SNMP 또는 시스로그 또는 두 가지 모두의 조합을 사용하여 승인된 장치 목록에 포함되지 않은 MAC 주소가 '주의'를 생성할 수 있는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하고 관찰을 통해 시료가 수신된 SRP 문장을 기반으로 SFI 표를 생성하는지 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 "이중 대체의 인스턴스 번호", MAC 주소 또는 SRP 문장으로 보고된 IP주소와 같은 값을 가진 최소 2개의 다른 SFI를 포함 시키고 시료가 '주의'를 발생시키지 않음을 관찰을 통해 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 SRP 센텐스의 "이중 대체의 인스턴스 번호" 필드를 다른 값으로 설정하고 SRP 센텐스로 보고된 동일한IP 주소를 가진 두 개의 동일한 SFI를 포함시키고 시료가 '주의'를 생성시키지 않음을 관찰을 통해 확인하여야 한다.</li> <li>- 시뮬레이션을 사용하여 SRP 센텐스의 "이중 대체의 인스턴스 번호" 필드가 널(null) 또는 동일한 숫자로 설정되고 SRP 센텐스에서 보고된 MAC주소가 서로 다른 두 개의 동일한 SFI를 포함시키고 시료가 주의를 생성하는지 관찰을 통해 확인하여야 한다.</li> <li>- 관찰을 통해 '주의'는 요구사항을 준수 하는지 확인하여야 한다.</li> </ul>	
42	시스로그 기록 기능 Syslog recording function	10.11.5	<ul style="list-style-type: none"> <li>- 시스로그 메시지를 발생 시키도록 시뮬레이션을 설정 한다. 관찰을 통해 네트워크 모니터링 기능이 460-네트워크의 450-노드, 460-노드, 460-게이트웨이 및 460-무선 게이트웨이에서 시스로그 정보를 볼 수 있는 기록 및 내부 또는 외부 가능성을 제공하는지 확인하여야 한다.</li> <li>- 문서화된 증거를 검사하여 기록된 최소 용량이 100,000개의 메시지이고 기록된 시스로그 메시지가 지난 30일 동안 사용할 수 있는지 확인하여야 한다.</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
10.11.6 경고 관리				
43	경고 및 표시 Alerts and indications	10.11.6.1	- 분석적 평가를 통해 경고가 표2의 요구사항을 준수하는지 확인하여야 한다.	
44	경고 관리 인터페이스 Alert management interface	10.11.6.2	- 제조사의 문서를 검사하여 제조자가 정의한 경고가 IEC 61924-2:2012, 8.2에 정의된 경고의 분류기준과 카테고리에 부합하는지 확인하여야 한다.  - 경고의 통신 및 표시를 시험하기 위해 제조사의 문서를 참조하여 무작위로 선택할 수 있는 사용가능한 '경계' 중 적어도 1개와 무작위로 선택할 수 있는 사용가능한 '주의' 중 2개를 확인한다. 그리고 BAM용 시뮬레이터를 사용하여 다음 시험을 수행하여야 한다. • 분석적 평가를 통해 경고 통신이 부속서E에 열거된 센텐스 및 IEC 61924-2:2012, 부속서 J의 상태 다이어그램을 준수하는지 확인하여야 한다.  • 분석적 평가를 통해 중앙 경고 관리시스템에 인터페이스 할 수 있는 수단이 제공되는 경우, HBT 센텐스의 주기적인 수신에 중단될 때 '주의' 경고를 제공하는 것을 확인하여야 한다.	
45	승인 되지 않은 경고 Unacknowledged warnings	10.11.6.3	- 제조사의 문서를 검사하여 경고 확대의 기본 값이 60초인지 확인하여야 한다.  - 관찰을 통해 사용자가 선택할 수 있는 경고의 확대 기간이 5분 미만인지 확인하여야 한다.  - 제조사의 문서를 검사하여 제조자가 아래 정보를 제공하는지 확인하여야 한다. • 경계로 반복되는 경계 • 사용자가 선택할 수 있는 시간 후 경보로 변경되는 경계 • 제조자의 정해진 시간 후 경보로 변경되는 경계  - 제조사 문서를 참조하여 경계로 반복되는 경우 무작위로 선택할 수 있는 최소 두 가지 사례를 식별한다. 관찰을 통해 반복 시간이 사용자가 선택한 시간인지 확인하여야 한다.  - 제조사 문서를 참조하여 경계가 경보로 변경되는 경우 무작위로 선택할 수 있는 최소 두 가지 사례를 식별한다. 관찰을 통해 우선순위 변경 전 시간이 사용자가 선택한 시간인지 확인하여야 한다.	
46	원격 확인 및 경고의 음소거	10.11.6.4	- 카테고리 B의 하나 이상의 2개의 경고를 생성한다. 관찰을 통해 ALF, ALC 및 HBT(시료가 '책임 이전'을 지원하는 경우)센텐스가 시료에서 경고 관리 인터페이스로 전송되는지 확인하여야 한다.	

No.	시험 항목	IEC 61162-460	내용	비고
	Remote acknowledgments and silencing of alerts		<p>- 시뮬레이터를 사용하여 ACN 센텐스를 시료로 전송하여 경고 중 하나를 음소거 한다. 관찰을 통해 ALF, ALC 및 HBT(제공된 경우) 센텐스가 경고의 새로운 상태를 올바르게 보고하는지 확인하여야 한다.</p> <p>- 시뮬레이터를 사용하여 ACN 센텐스를 전송하여 카테고리 B 경고를 확인(Ack)한다. 관찰을 통해 ALF, ALC 및 HBT(제공된 경우) 센텐스가 경고의 새로운 상태를 올바르게 보고하는지 확인하여야 한다.</p>	
10.12 시스템 수준				
47	일반 General	10.12.1	<p>- 10.12 하위 조항은 요구 사항의 시스템 수준 확인을 위한 시험 방법 및 필요한 결과를 포함한다. 시스템 수준 확인은 다음에 대해 수행 될 수 있다.</p> <ul style="list-style-type: none"> <li>• 적합성 시험 신청자가 설명한 일반적인 시스템 설정 또는</li> <li>• 적합성 시험 신청자가 설명한 실제 선상 설치.</li> </ul> <p>- 시스템 수준 적합성 시험은 시뮬레이션 대신에 실제 장비를 기반으로 한다. 시스템 수준 적합성 시험의 목표는 네트워크 인프라와 장비(예 : 레이다, ECDIS, 자이로 컴파스와 같은 항해기기)로 구성된 실제 시스템이 이 기준의 시스템 요건을 충족한다는 것을 입증하는 것을 말한다.</p> <p>- 시스템 수준 적합성의 기본은 각 개별 구성 품이 개별 기능에 대하여 이 기준에 따라 사전에 별도로 시험이 되었다는 것을 말한다(10.4 ~ 10.9항 참고).</p> <p>- 시스템 수준 적합성 시험을 위한 최소 시스템은 최소한 다음 기능으로 구성된다.</p> <ul style="list-style-type: none"> <li>• 2개의 460-스위치</li> <li>• 2개의 450-노드 또는 460-노드</li> <li>• 네트워크 모니터링 기능</li> </ul> <p>- 시험장의 요건은 다음과 같다.</p> <ul style="list-style-type: none"> <li>• 트래픽 모니터링을 위한 프로토콜 분석기 (예: Wireshark)</li> <li>• IEC 61162-450 호환데이터와 비 IEC 61162-450 호환 데이터 (예: TCP/IP, UDP/IP, 멀티캐스트 및 브로드캐스트)를 사용하여 460-스위치에 더 많은 네트워크 트래픽을 주입하여 정상적인 네트워크 부하 수준에서 100%까지 네트워크 회선 부하를 증가시킬 수 있는 구성</li> <li>• 460-스위치에 Dos 공격을 할 수 있는 구성</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
48	시스템 관리 기능 System management function	10.12.2	- 관찰을 통해 460-스위치의 구성 정보가 시스템에 저장될 수 있는지 확인하여야 한다. 460-스위치를 구성되지 않은 다른 460-스위치로 교체한다. 시스템 관리 기능을 사용하여 관찰을 통해 원래 구성을 새로운 460-스위치로 복원할 수 있는지 확인하여야 한다. 이 시험은 모든 460-스위치 및 460-포워더에 대해 반복 되어야한다.  - 하나의 460-노드 제거하고 MAC 주소가 다른 동등한 장치로 교체한다. 시스템 관리 기능을 사용하여 관찰을 통해 새 장치를 수용하도록 원래 구성을 변경할 수 있는지 확인하여야 한다.  - 첫 번째 시스템 관리 기능을 끄거나 시료에 인터페이스 이중화가 있는 경우 케이블 하나를 분리한다. 관찰을 통해 두 번째 시스템 관리기능을 사용할 수 있는지 확인하여야 한다.	
10.12.3 시스템 설계				
49	일반 General	10.12.3.1	- 문서화된 증거를 검사하여 다음 정보가 제공되는지 확인하여야 한다. <ul style="list-style-type: none"> <li>• 네트워크의 토폴로지 및 장치 (제공되는 경우, 보안 영역의 네트워크를 포함)</li> <li>• 네트워크가 460-네트워크 물리적 구성 요소, 460-네트워크 노드 및 네트워크 인프라 구성 요소로만 구성</li> <li>• 460-포워더와 연결된 모든 네트워크가 제어 네트워크 또는 다른 460-네트워크</li> </ul> - 문서화된 증거를 검사하여 네트워크 모니터링 기능과 시스템 관리 기능을 모두 네트워크에서 사용할 수 있는지 확인하여야 한다.	
50	문서화 Documentation	10.12.3.2	- 문서화된 증거를 검사하여 다음 정보가 제공되는지 확인하여야 한다. <ul style="list-style-type: none"> <li>• 460-네트워크 트래픽 플로우 분석 및 네트워크 토폴로지</li> <li>• 460-네트워크에 대한 총 네트워크 트래픽의 양과 모든 트래픽의 평균 부하</li> <li>• 제공되는 경우, 각 460-포워더에서 하나의 460-네트워크에서 다른 460-네트워크로 전송 되는 최대 트래픽 플로우</li> <li>• 제공되는 경우, 각 460-포워더에서 각 트래픽 유형의 우선순위 지정</li> <li>• 최대 네트워크 부하분석</li> <li>• 이중 사용 가능한 데이터 소스 목록</li> <li>• 허용된 장치 목록</li> </ul>	

No.	시험 항목	IEC 61162-460	내용	비고
51	네트워크 트래픽 설계 Network traffic design	10.12.3.3	<p>- 문서화된 증거를 검사하여 각 460-스위치에서 할당된 대역폭의 양이 스위치에 연결된 네트워크에 할당된 각 트래픽 클래스의 모든 트래픽 볼륨의 합보다 크거나 같음을 확인하여야 한다.</p> <p>- 네트워크 설계 문서를 사용하고 3개의 포트를 선택하여 관찰을 통해 측정된 트래픽이 정의된 트래픽 부하 합계의 값보다 낮거나 같은지 확인하여야 한다. 관찰을 통해 460-네트워크에서 모든 트래픽의 평균 부하가 1초 동안 계획된 명목상의 네트워크 용량의 95%를 초과하지 않으며 10초 동안 계획된 명목상의 네트워크 용량의 80%를 초과하지 않는지 확인하여야 한다.</p>	
52	루프 방지 Loop prevention	10.12.3.4	<p>- 네트워크 설계 문서를 사용하고 예를 들어 유니캐스트를 사용하여 각 스위치에서 하나 이상의 460-노드와 연결하는 루프 토폴로지를 위하여 최소 2개의 460-스위치를 선택한다. 분석적 평가를 통해 스위치의 데이터가 중복되지 않는지 확인하여야 한다.</p>	
53	리소스 할당 Resource allocation	10.12.3.5	<p>- 문서화된 증거를 검사하여 460-포워더에 할당된 대역폭의 양이 460-포워더에 연결된 네트워크에 할당된 각 트래픽 클래스의 모든 트래픽 볼륨의 합보다 크거나 같음을 확인하여야 한다.</p> <p>- 네트워크 설계 문서를 사용하고 2개의 포트를 선택하여 관찰을 통해 측정된 트래픽이 정의된 트래픽 부하 합계의 값보다 낮거나 같은지 확인하여야 한다.</p>	
54	트래픽 우선순위 Traffic prioritisation	10.12.3.6	<p>- 시험 대상 시스템에서 사용할 수 있는 경우, 연결된 460-노드 기반 장치가 작동을 표시하는 우선 순위가 다른 두 트래픽 플로우를 선택한다. 시뮬레이션을 사용하여 최대 회선 부하까지 선택한 두 가지 우선 순위사이에 우선순위 수준의 추가 트래픽을 가한다. 관찰을 통해 우선순위가 가장 높은 트래픽 플로우를 사용하는 장치가 지속적으로 작동 표시하고, 우선순위가 가장 낮은 트래픽을 사용하는 장치가 왜곡됨을 확인하여야 한다.</p>	
55	서비스 거부 행위 Denial of service behaviour	10.12.3.7	<p>- 네트워크 설계 문서를 사용하여 3개의 460-노드를 선택하여 1시간 동안 회선 부하까지 추가 트래픽을 가한다. 460-노드 수가 3개 미만일 경우 460-노드를 모두 선택한다. 관찰을 통해 460-노드가 독립형 장치로 정상 작동을 지속 하는지 확인하여야 한다. 추가된 트래픽을 제거하고 관찰을 통해 460-노드가 460-네트워크로부터 수신된 정보를 기반으로 작동을 재개하는지 확인하여야 한다.</p>	
56	비제어 네트워크 보안 Uncontrolled network security	10.12.3.8	<p>- 시험 대상 시스템에 460-게이트웨이가 포함된 경우, 10.8에 명시된 모든 시험을 반복하여야 한다.</p> <p>- 시험 대상 시스템에 460-무선게이트웨이가 포함된 경우, 10.9에 명시된 모든 시험을 반복하여야 한다.</p>	

No.	시험 항목	IEC 61162-460	내용	비고
57	보안 영역과 비 보안 영역 간의 연결 Connections between secure and non-secure areas	10.12.3.9	- 시험 대상 시스템이 보안영역에 설치된 460-네트워크와 비 보안 영역에 설치된 460-네트워크사이의 연결을 포함하는 경우, 10.7에 명시된 모든 시험을 반복하여야 한다.	
58	이중화 Redundancy	10.12.3.10	- 문서화된 증거를 검사하여 이중화 기능의 FMEA 또는 FMECA를 사용할 수 있고 중요 노드가 식별되며 단일 고장 지점이 중요 노드의 기능에 영향을 미치지 않음을 확인하여야 한다.  - FMEA 또는 FMECA 문서를 사용하고 중요 장치의 20% 또는 최소 3개의 장치를 대표 장치로 선택한다. 각 대표 장치에 하나씩 단일 고장을 일으키고 분석 평가를 통해 이중화 장치가 5초 이내에 정상 작동을 지속하는지 확인하여야 한다.  - 연결된 460-노드 기반 장치에 대하여 두 개의 트래픽 플로우를 선택하고 작동을 표시한다. 두 개의 460-스위치 사이의 케이블을 분리하고 분석 평가를 통해 데이터 전송 중단이 5초 이하인지 확인하여야 한다.	
59	네트워크 모니터링 기능 Network monitoring function	10.12.4	- 네트워크 모니터링 기능의 경우 10.11.1에 명시된 모든 시험을 반복하여야 한다.	
60	네트워크 부하 모니터링 기능 Network load monitoring function	10.12.5	- 네트워크 부하 모니터링 기능의 경우 10.11.2에 명시된 모든 시험을 반복하여야 한다.	
61	이중화 모니터링 기능 Redundancy monitoring function	10.12.6	- 네트워크 이중화 모니터링 기능의 경우 10.11.3에 명시된 모든 시험을 반복하여야 한다.	
10.12.7 네트워크 토폴로지 모니터링 기능				
62	일반 General	10.12.7.1	- 네트워크 토폴로지 모니터링 기능의 경우 10.11.4에 명시된 모든 시험을 반복하여야 한다.	
63	시스로그 기록 기능 Syslog recording function	10.12.7.2	- 시스로그 기록 기능의 경우 10.11.5에 명시된 모든 시험을 반복하여야 한다.	

No.	시험 항목	IEC 61162-460	내용	비고
64	네트워크 모니터링 기능의 이중화 Redundancy of network monitoring function	10.12.7.3	- 첫 번째 네트워크 모니터링 기능을 끄거나 시료에 인터페이스 이중화가 있는 경우, 케이블 하나를 분리한다. 관찰을 통해 두 번째 네트워크 모니터링 기능을 사용할 수 있는지 확인하여야 한다.	