정 보 보 호 학 회 지
제24권 제2호, 2014. 4

선박 네트워크를 위한 NMEA2000과 정보 보호

류 대 현*, 박 장 식**

요 약

최근 건조되고 있는 선박에는 안전 운항을 위하여 엔진제어시스템, 선박자동항법장치, 선박자동식별장치, CCTV 등의 전자장치들이 선박네트워크로 연결되어 있으며, 위성을 통하여 선박의 엔진상태 등의 선박 운항정보를 실시간으로 원격지에서 모니터링 할 수 있다. 선박의 내부와 외부통신 체계는 대체로 폐쇄적인 네트워크로 구성되어 있으나,선박고유식별번호, 선박명, 선박종류, 항로, 목적항, 입항예정일, 화물종류 등의 선박의 주요 정보를 전송하는 선박자동식별장치는 무선 VHF로 전송되고, 선원은 개인용 컴퓨터를 이용하여 인터넷에 접속이 가능하기 때문에 선박 정보의 해킹 또는 바이러스에 취약해질 수 있다. 컴퓨터 바이러스 또는 해킹 등의 외부 침입으로 인하여 선박항해시스템의 오류가 발생할 가능성이 높아지고 있다. 본 논문에서는 선박통합네트워크에서 제어네트워크의 표준화 동향과 정보보호 기술의 필요성에 대하여 기술한다.

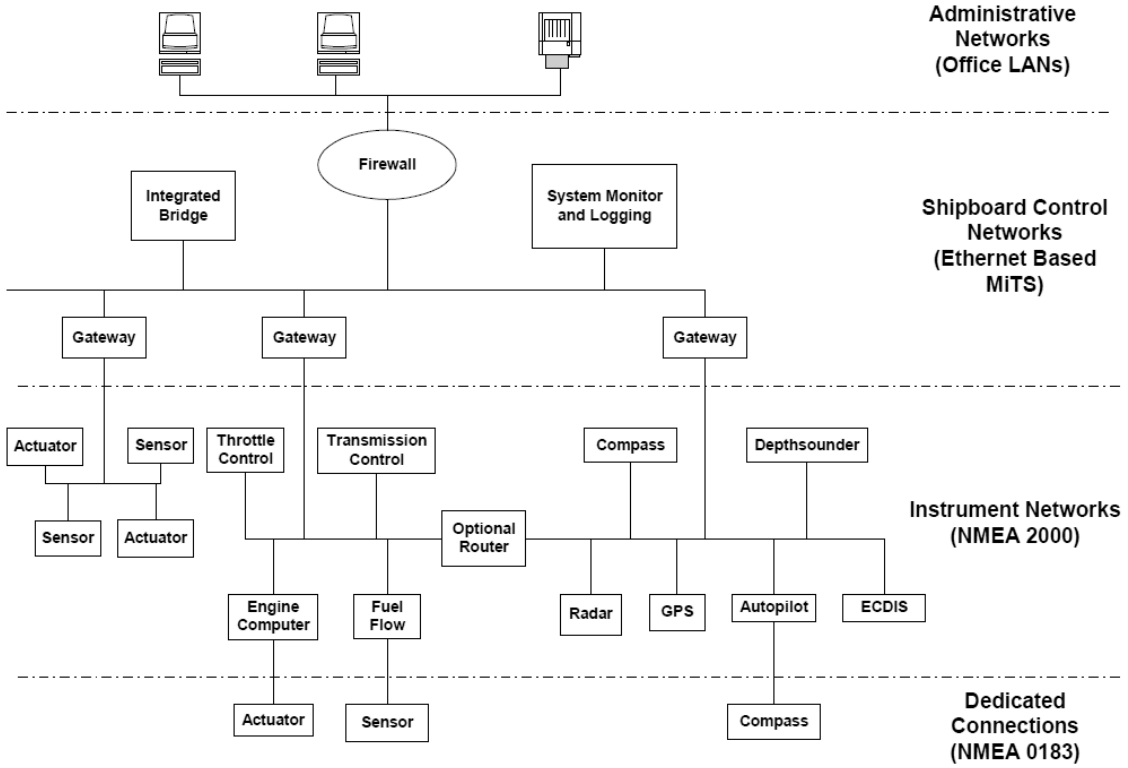
Ⅰ. 서 론

최근에 ICT 융합 기술이 산업체의 주요화두가 되면서 국내 조선 및 관련 기자재 산업에서도 ICT와 조선산업의 융합기술이 주요 이슈가 되고 있다. 특히, 2005년 12월 부터 국제해사기구(IMO, International Maritime Organization)에서 e-Navigation[1, 2]을 추진하면서 국내에서도 e-Navigation[3, 4]을 실현하기 위하여 조선산업에 ICT기술을 접목하기 위한 방안에 대한 관심과 연구 개발이 이루어지고 있다.

e-Navigation을 실현하기 위해서는 크기 3가지 영역에서의 기술 개발 및 지원이 필요하다[3]. 첫 번째는 선박내에서의 e-Navigation 지원이다. 안전한 항해를 지원하기 위하여 그 동안 독자적이고 폐쇄적으로 제공되어던 선박 장치들의 항해 정보에 대하여 종합적이고 개방적인 구조로 통합되고 관리되어야 하며 통합된 항해정보를 육상으로 제공할 수 있어야 한다. 두번째는 육상에서의 e-Navigation 지원이 필요하다. 항해자에게 최신의 기상 정보 및 전자 해도 정보를 포함하여 항해에 필요한 정보를 실시간으로 제공하기 위한 통신 인프라 구축이 필요하다. 세 번째는 선박과 육상에서 수집된 정보를 육상 또는 선박으로 전달하기 위한 4S(ship-to-ship, ship-to-shore, shore-to-ship, shore-to-shore)의 구축하는 것이다. 대양에 위치한 선박과의 통신을 위한 수 십 ~ 수 백 kbps 대역의 위성통신 기술을 사용하고 있지만, e-Navigation 을 위해서는 보다 많은 양의 통신 인프라 지원이 필요하다. 따라서, 조산산업에서의 세계 강국이 되기 위해서는 관련 통신기술 및 플랫폼 국제표준화를 선도하는 것이 필요하다. 그리고, 선박의 안전 운항에 영향을 줄 수 있는 외부에서 침입에 대한 대응과 트래픽에 의한 오류에 대한 대응 기술을 확보하는 것이 필요하다.

본 고에서는 3 가지 요소 중에서 선박네트워크에 대한 표준화 동향과 정보보호에 대하여 다루고자 한다. 선박 네트워크(SAN, Ship Area Network)는 선박 내에 설치된 장치들간에 제어명령, 상태정보, 도면정보 등을 교환할 수 있도록 구축된 선박용 백본 네트워크이다. SAN은 중앙관제실에서 선박 내 각종 장치에 대한 제어와 모니터링을 수행할 수 있도록 하기 때문에 선박 자동화에 필수적인 요소이다. 일반적으로 컨테이너선박과 같은 대형 선박도 약 30여명의 선원이 운항을 한다. 선박의 효율적인 운항을 위하여 선박 네트워크 도입되어 운용되고 있지만 바이러스 또는 해킹에 의한 선박운항 시스템이 오작동할 우려도 높아지고 있다. 자동차네트

* 한세대학교 IT학부 (dhryu@hansei.ac.kr)
** 경성대학교 전자공학과 (jsipark@ks.ac.kr)



〔그림 2〕 e-Navigation 선박 통합 네트워크 구성

워크와 동일하게 SAN에서는 제어 계통에서 CAN 기반 네트워크[5, 6]를 구축하기 때문에 선박의 각 요소 장치들이 ID에 의하여 장치 정보가 네트워크를 통하여 노출될 수 있다. 따라서 선박의 안전 운항을 위하여 선박 네트워크에 대한 정보보호 기술의 적용이 필요하다.

NMEA2000은 CAN(Controller Area Network)을 기반으로 하는 250kps 속도의 저가형 직렬 데이터 네트워크이다[7-10]. CAN은 원래 자동차 내부 네트워크를 위하여 개발되었으나 최근에는 다양한 산업분야에 적용되고 있으며, IC(Integrated circuit)제조사에서 전용 프로세서를 생산하고 있다. 선박의 안전 운항을 위하여 NMEA 2000 선박전자제어 장치들이 증가하는 추세에 있다[11-13].

Ⅱ. 선박 통합 네트워크 구조

선박 통합 네트워크에 대한 구조는 그림 1과 같다[9]. 선박 내에는 선박 위치를 추적하기 위한 선박자동식별장치, AIS(Automatic Identification System)와 GPS (Global Positioning System)장비가 있으며, 선박 내부 기기에 대한 상태 모니터링, 통보, 제어를 위한 센서 및 구동기에 해당하는 AMS(Alarm Monitoring Systme), Guage NN1 등이 있다. 그리고, 센서로부터 전달되어진 상태를 확인하는 웹페이지 생성을 위한 선박 내 웹서버 및 항해 동안 발생하는 이벤트를 기록하는 VDR (Voyage Data Recorder)이 있다. 또한 사용자에게 각 기기를 연결시켜 함교에서 모든 기기를 작동할 수 있도록 지원하는 IBS(Integratted Bridge System)과 INS (Integrated Navigation System)이 있다. 선원이 개인적인으로 사용할 수 있는 PC를 포함하는 선원 네트워크(crew network)와 외부와 통신을 위한 위성통신시스템이 있다. 그리고 모든 장치들을 연결하는 통합 게이트웨이(integrated gateway)가 네트워크의 중심에 위치한다.

Ⅲ. NMEA2000 프로토콜

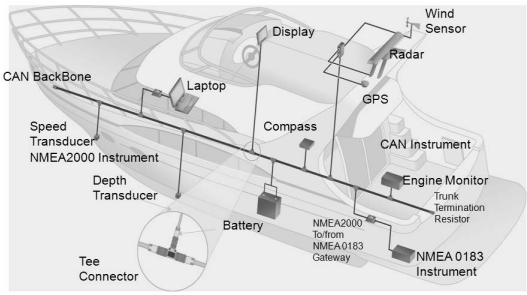
NMEA 2000은 GPS 수신기, 수심탐지기(depth finder), 전자해도(nautical chart plotter), 운항장비(navigation instruments), 엔진, 탱크레벨센서 등의 선박 내 전자 장치간의 통신과 해양 데이터 네트워크를 위한 전기 및 데이터 사양을 정한 것으로 CAN을 기반으로 한다. 선박통합네트워크에서 제어계통은 NMEA 0183과 NMEA 2000이 적용되고 있으며, NMEA 0183은 표준 비동기 직렬통신을 기반으로 4.8kbps 의 직렬 데이터 통신이다. NMEA 0183과 NMEA 2000의 차이점은 속도와 통신 네트워크 방식이 다르다. 선박의 안전 운항을 위하여 보다 효율적인 NMEA 2000으로 선박전자제어장치들이 대체되고 있다.

3.1 NMEA 0183 개요

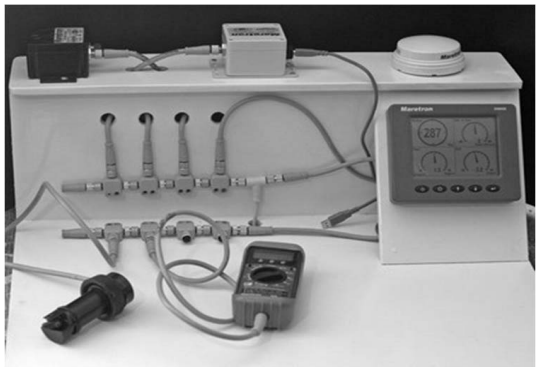
NMEA 0183 은 시간, 위치, 방위 등의 정보를 전송하기 위한 규격이다. NMEA 0183은 미국의 NMEA (National Maritime Electronics Association)에서 정의하고 데이터는 주로 자이로콤파스(gyrocompass), GPS, 나침반, 관성항법장치(INS)에 사용된다. ASCII와 직렬 방식의 통신을 사용한다. 물리계층, 데이터링크 계층, 응용 계층으로 된 3가지 레이어로 구성되어 있다. 물리계층은 RS-232, RS-422 의 전기적인 전송 규격을 따르고 데이터링크는 전송률(baud rate), 데이터비트(data bit), 패리티비트(parity bit), 정지비트(stop bit) 등을 정한다. 응용계층은 데이터를 전송하는 문장(sentence)에 대한 규약이다.

3.2 NMEA 2000 개요

NMEA 2000은 SAE J1939 상위레벨 프로토콜을 기반으로 자체 메시지를 정의하고 있어 NMEA 2000 장치와 J1939 장치는 같은 물리 네트워크 상에 공존할 수 있다. 시리얼통신버스 표준을 기반으로 하고 NMEA 0183을 계승한다. NMEA 0183이 직렬통신 기반의 단일 송신기(single-talk), 다중 수신기(multi-listener)를 요구하는 반면에 NMEA 2000은 다중 송신(multi-talk), 다중 수신기(multi-listner) 데이터 네트워크를 지향한다.



〔그림 2〕 NMEA 2000 네트워크 구성

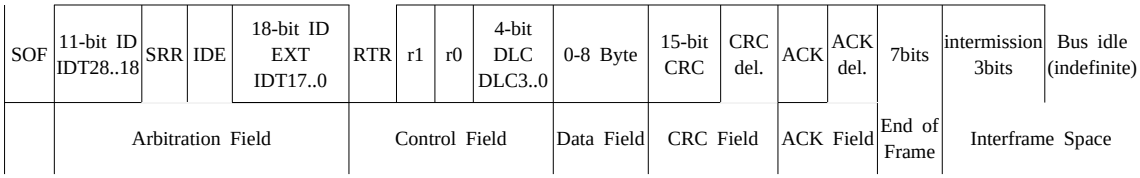


〔그림 3〕 NMEA 2000 네트워크 장치 및 네트워크 사례

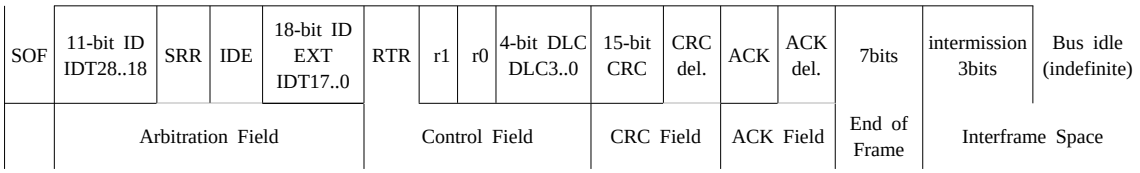
3.3 CAN 프로토콜

NMEA 2000은 자동차네트워크에 적용한 CAN을 활용한다. CAN 프로토콜은 고수준의 보안 기능을 갖춘 실시간, 직렬 브로드캐스팅 프로토콜이다. 고속통신에 대해서는 ISO 11898과 저속 통신에 대해서는 ISO 11519-2 로 정의된 국제 표준이다. CAN은 브로드캐스트(broadcast) 통신 메카니즘을 기반으로 한다. 브로드캐스트 통신은 메시지 기반의 전송 프로토콜을 사용함으로써 실현된다. 메시지는 메시지 식별자(ID, identifier)에 의하여 식별된다. 하나의 메시지 식별자는 전체 네트워크 내에서 유일하고, 식별자 내용뿐만 아니라 메시지의 우선권도 정의하고 있다.

데이터 프레임(Data Frame)



원격 프레임(Remote Frame)



〔그림 4〕 CAN 2.0B의 데이터 프레임과 원격 프레임 구조

메시지가 전송될 때 상대적으로 긴급하지 않은 다른 메시지와 비교하여 우선권이 각각의 메시지의 식별자에 의하여 명시된다. 우선권은 시스템 설계시 이진수 형태로 결정되고, 이것은 동적으로 변하지 않는다. 가장 낮은 이진수를 갖는 식별자가 가장 높은 우선권을 갖는다. 버스 접근 중재(arbitration)는 버스 레벨을 비트 단위로 관찰하고 있는 각 노드 식별자의 비트 단위 중재에 의하여 해결된다. 우세 상태(0)가 열세 상태(1)를 덮어 쓰는 와이어곱(wired AND) 메카니즘으로 처리된다.

CAN 프로토콜은 식별자의 길이에 의하여 구분되는 2 가지 메시지 프레임 포맷을 지원한다. 식별자의 길이에 따라 다음의 2 가지 포맷으로 구분된다. CAN 2.0A로 알려진 CAN 표준 프레임은 11비트 식별자를 갖고, CAN 2.0B로 알려진 CAN 확장 프레임은 29비트의 식별자를 갖는다.

CAN 통신에서 데이터는 메시지 프레임을 사용하여 송수신이 이루어진다. 메시지 프레임은 하나 또는 그 이상의 송신 노드로부터 데이터를 수신노드로 전송한다. 확장 CAN 2.0B 메시지 구조는 그림 4와 같다. 표준 메시지는 데이터 프레임과 원격 프레임이 있다. 데이터 프레임은 데이터를 전송하는 프레임이고 원격 프레임은 데이터를 요청하는 프레임이다.

SOF(Start of Frame)은 메시지 프레임의 시작을 표시한다. 메시지 프레임의 맨 앞에 위치하며 기본값(default)은 “0” 이다. 중재 필드(arbitration field)는 11비트의 표준 식별자와 확장된 18비트 그리고 원격전송요청(RTR, Remote Transmission Request) 비트로 구성된다. RTR은 기본값으로 “0”을 가지며 “0” 일때는 CAN 메시지가 데이터 프레임을 의미한다. RTR이 “1” 이면 CAN 메시지가 원격전송요청임을 의미한다.

즉, CAN 메시지가 데이터 프레임이 아닌 원격 프레임 상태임을 나타낸다. 원격 프레임은 데이터 버스 상의 어떤 노드에서 다른 노드로 데이터를 전송하여 줄 것을 요청할 때 사용된다. 데이터를 전송하기 전에 사용하는 메시지 프레임이기 때문에 데이터 필드가 없다.

제어 필드(Control Field)는 IDE(Identifier Extension) 비트와 데이터 길이 코드(DLC, data length code)로 구성된다. DLC는 데이터 필드의 바이트 수를 나타낸다. 원격 프레임에서 DLC는 요청 데이터의 바이트 수를 의미한다.

데이터 필드(Data Field)는 특정 노드에서 다른 노드로 전송하는 데이터를 포함한다. 0에서 8바이트의 데이터를 전송할 수 있다.

CRC 필드(Cyclic Redundant Check)는 15비트의 CRC 코드를 가지며 CRC 피드의 끝을 알리는 “1” 값의 비트가 이어진다.

ACK 필드(Acknowledge)는 2비트로 구성되며 첫 번째 비트는 “0”을 가지는 슬롯 비트이며, 두 번째 비트는 “1” 값을 갖는다.

프레임 종료는 7비트로 구성되어 있으며, 모두 “1” 값을 갖는다. EOF에 이어 “1” 값을 갖는 3비트의 프레임 중단 필드가 이어진다. 이 3 비트 이후에는 CAN버

스라인은 자유 상태로 인식된다.

3.4 CAN 보안 특성

현재 제조사별로 작성한 다양한 형태의 CAN 네트워크가 존재하지만, 일반적인 CAN의 취약성을 다음과 같이 정리할 수 있다.

가. 브로드캐스트

CAN 패킷은 기본적으로 자동차 내 모든 구성 컴포넌트에 브로드캐스트 된다. 따라서 CAN 네트워크상에 존재하는 악성 컴포넌트는 CAN 상의 모든 패킷을 감청할 수 있으며, 네트워크상에 존재하는 다른 노드에 공격을 위해 생성한 패킷을 전송할 수 있다. 이러한 브로드캐스트를 이용해 패킷을 감청하고, 이를 분석한 후, 분석된 결과를 바탕으로 새롭게 생성한 패킷을 다양한 목적을 위해 전송하는 공격이 가능하다.

나. 인증 필드의 부재

CAN 패킷은 인증을 위한 필드를 가지고 있지 않다. 심지어는 송신자의 식별을 위한 ID 필드도 없다. 이는 모든 컴포넌트가 타 컴포넌트에게 식별 불가능한 패킷을 전송할 수 있음을 의미한다. 따라서 방어기능이 적재되지 않은 모든 컴포넌트는 악의적으로 탑재된 하나의 컴포넌트에 의해 제어될 수 있는 가능성을 갖게 된다.

다. 접근 제어의 취약성

CAN 프로토콜 표준은 비인가 메시지로부터 ECU를 보호하기위한 질의-응답(challenge-response) 절차를 기술하고 있다. CAN 프로토콜 표준에 따르면 질의-응답 키 둘 모두 16bit로 정의되어 있고, ECU는 매 10초마다 인증 절차를 허용해야 하므로 하나의 ECU에 대한 키 획득 공격은 7일 정도면 수행될 수 있다고 알려져 있다. 따라서 공격자가 자신의 ECU를 이용해 이 정도 시간 동안 CAN에 접근할 수 있다면 데이터 갱신이 가능한 어느 ECU라도 공격가능 하다고 볼 수 있다.

3.5 NMEA 2000 프로토콜

NMEA 2000의 특징은 PGN(Parameter Group number)이며 필요한 정보는 PGN으로 구분한다. 표 1은 CAN 2.0B 확장버전의 ID와 PGN관계를 나타낸 것이다.

〔표 1〕 CAN 2.0B ID와 PGN 관계

PDU format	29 bits CAN Identifier					
	Priority 3 bit	EDP 1bit	DP 1bit	PF 8bit	PS 8bit	SA 8bit
		PGN				
PDU1	0-7	0	0	0-239	DA 0-255	SA 0-255
			1	0-239	DA 0-255	SA 0-255
PDU2	0-7	0	0	240-255	GE 0-255	SA 0-255
			1	240-255	GE 0-255	SA 0-255

우선순위(Priority)는 우선 순위 비트들은 버스를 이용한 메시지의 전송지연을 최적화하기 위한 목적으로만 사용된다. 이 비트들은 수신된 다음에는 완전히 무시된다.

확장 데이터 페이지((EDP, Extented data page)는 CAN 데이터 프레임의 CAN 식별자 구조를 결정하기 위하여 데이터 페이지 비트와 함께 사용된다. ISO 11783 메시지는 전송될 때 EDP가 0으로 설정하여 전송된다. 데이터 페이지(DP, Data page)는 CAN 데이터 프레임의 CAN 식별자의 구조를 결정하기 위하여 EDP 비트와 함께 사용된다. EDP 비트는 0으로 설정하고 DP 비트를 이용하여 PGN 명세의 페이지 0과 페이지 1을 선택할 수 있다. PDU 포맷(format) 은 PF가 결정하는 8 비트 필드이며, CAN 데이터 필드에 할당된 PGN을 결정하기 위하여 사용되는 필드 중의 하나이다. PGN은 명령, 데이터, 일부요청, ACK 또는 NACK 를 구분하거나 나타내거나 정보를 소통하기 위하여 하나 또는 그 이상의 CAN 데이터 프레임을 필요로 하는 정보를 나타내기 위하여 사용된다. PDU 특성(PS, PDU Specific)은 PDU 포맷에 따라 DA(Destination Address) 또는 GE(Group Estension) 필드로 정해지는 8 비트 필드이다.

소스 주소(SA, Source Address)는 8비트 이며, 특정 소스 주소를 갖는 제어는 네트워크에 단 하나만 존재한다.

CAN 데이터 필드는 어떤 파라미터 그룹을 표현하는데 8 바이트 이하의 데이터가 필요한 경우에는 CAN 데

이터 프레임의 8바이트 모두를 사용할 수 있다. 8바이트 보다 많은 정보가 존재하는 경우에는 멀티 패킷 메시지가 전송된다.

NMEA 2000 메시지 형식은 명령(command), 요청(request), 방송 응답(broadcast, responses), 승인(acknowledgements), 그룹 기능(group functions) 로 5가지가 있다. 메시지 형식은 메시지에 할당된 PGN에 의하여 인식된다 원격 프레임에 대한 CAN 프로토콜에서 정의하는 RTR 비트는 recessive 상태(논리적 1)로 설정되어서는 안된다. 따라서 원격전송요청(RTR=1)은 ISO 11783 네트워크에서는 사용할 수 없다.

Ⅳ. 선박통신 네트워크 보안 기술

세계 선박통신분야 국제표준을 관장하는 IEC의 해상무선통신기술위원회에서는 우리나라가 제안한 “선박통신 네트워크 보안기술”을 국제표준 초안에 채택하였다. 미국, 일본 등 등 16개국으로부터 89%의 지지를 통하여 2012년 6월 18일 국제표준안으로 선정되었다. 한국전자통신연구원이 개발한 “선박통신에 대한 안전 및 보안기술”은 2011년 우리나라가 IEC 국제표준으로 반영시킨 선박네트워크 SAN의 이미지 전송과 관련된 기술로 해킹, 바이러스 등의 외부 침입으로부터 네트워크 및 선박 항해 시스템의 안전을 보호하고 선박 내 각종 센서들의 트래픽 증가에 따른 오류 방지를 할 수 있는 기능을 포함한다. 향후 네트워크 기반 선박자동식별장치인 AIS, 전자해도 등 선박 내부 장치에 탑재될 예정이다. 선박 이더넷통신(IEC 61162-450)에 이어 국제해사기구(IMO)의 강제기준으로 채택될 가능성이 높기 때문에 국내 선박업계와 조선기자재 업계의 선행 대응에 따라 세계시장 선점의 가능성이 높아질 것으로 보인다.

Ⅴ. 결 론

선박의 안전하고 효율적인 운항을 위하여 SAN을 적용한 선박들이 최근 건조되고 있으나, 바이러스, 해킹 등의 외부 침입에 의한 선박 운항시스템의 오작동과 USB 플래시 메모리 등을 이용한 선박 정보 유출의 가능성이 높아지고 있다. 본 논문에서는 선박의 운항에 직접적으로 영향을 주는 제어네트워크 표준 기술을 살펴보고 이와 관련한 정보보호 동향에 대하여 다루었다.

참 고 문 헌

[1] A. Weintrit, R. Wawruch, C. Specht, L. Gucma and Z. Pietrzykowski, “Polish Approach to e-Navigation Concept”, International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 1, No. 3, pp. 261-269, Sept., 2007.

[2] K. Korcz, “GMDSS as a Data Communication Network for e-Navigation”, International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 2, No. 3, pp. 261-269, Sept., 2008.

[3] 이광일, 박준희, 최원석, 문경덕, “선내 통신 국제 표준화 동향”, TTA Journal No. 126, pp. 45-51, 2009.

[4] 이성형, 김재현, 문경덕, 이광일, 박준희, “선박 통합 네트워크 구조 성능 분석”, 한국통신학회논문지, 38(03), pp. 247-253, 2013

[5] ISO11898-1: Road Vehicles-Controller area network(CAN)-Part 1: Data link layer and physical signalling.

[6] 박장식, AT90CAN128을 이용한 CAN통신실무, 홍릉과학출판사, 2012년

[7] NMEA2000: Standard for Serial-Data Networking of Marine Electronic Device, Ver 1.20, Sept. 2004.

[8] ISO11783-3: Tractors and machinery for agriculture and factory-serial control and communication data network-Part3: Data link layer.

[9] Lee A. Luft, Larry Anderson, Frank Casidy, “NMEA 2000 A Digital Interface for the 21st Century”, Institute of Navigation’s 2002 National Technical Meeting, San Diego California, Jan. 2002.

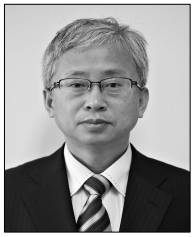
[10] 이창의, 김달용, 유영호, 신옥근, “NMEA2000을 이용한 임베디드 선박 모니터링 시스템의 개발”, 한국마린엔지니어링 학회지 제33권 제5호, pp. 746-755, 2009.

[11] T. Ming-Cheng and H. Chao-Kuang, “The Study of Ship Collision Avoidance Route Planning by Ant Colony Algorithm”, Journal of Marine Scicence and Technology, Vol. 18, No. 5, pp. 746-756, 2010.

[12] Z. Jung-dong, S. Jiang-hua, “Distributed and Redundant Design of Ship Monitoring and Control Network”, Journal of Marine Science and Application, Vol. 1, No. 2, Dec, 2002.

[13] D. Chen, L. Xia, and H. Wang, “Modelling and Simulation of Monitor-Control Network in Ship Ppwer Station”, Proceedings of the 2008 Workshop on Power Electronics and Intelligent Transportaion System, pp. 384-388, 2008

〈저 자 소 개〉



류 대 현 (Ryu, Dae-Hyun)
종신회원

1985년 2월 : 부산대학교 전자공학과 석사
1997년 2월 : 부산대학교 전자공학과 박사
1987년 3월~1998년 2월 : 한국전자통신연구원
1998년 3월~현재 : 한세대학교 IT 학부
관심분야 : 센서네트워크, 영상처리, 정보보호

박 장 식 (Park, Jangsik)
종신회원

1992년 2월 : 부산대학교 전자공학과 졸업
1994년 2월 : 부산대학교 전자공학과 석사
1999년 2월 : 부산대학교 전자공학과 박사
1997년 3월~2011년 2월 : 동의과학대학교 전자과 교수
2011년 3월~현재 : 경성대학교 전자공학과 교수
관심분야 : 신호처리, 영상처리 및 이해, 자동차 및 선박 네트워크,