http://dx.doi.org/10.7236/JIWIT.2012.12.2.251
JIWIT 2012-2-31

생산자동화설비의 종단보안 시스템 구조

Edge Security System for Factory Automation Devices

황호영*, 김승천**, 노광현***

Hoyoung Hwang, Seung-Cheon Kim, Kwanghyun Ro

요 약 기존의 공장 자동화 및 각종 생산설비 시스템의 전통적인 보안 개념은 네트워크의 경계선, 즉 내부와 외부 네트워크의 접점에 집중되어 있었으나, 최근 외부뿐 아니라 네트워크의 경계선을 우회하여 내부에서 침입할 수 있는 소위 신종 Day-zero공격이 증가하고 있다. 본 논문에서는 최근 대두되고 있는 NAC(Network Access Control)의 문제점인 1) 표준화 지연 및 복잡성으로 인한 설치와 운영의 어려움, 2) 인증 위주의 제품특성상 내, 외부 사용자에게 사용상의 불편함 초래, 3) 높은 구축 비용으로 인한 부담 등을 보완할 수 있는 저가형의 자동화설비 보안 솔루션으로서 내/외부의 다양한 경로로 유입되는 위협이나 유해트래픽을 차단하기 위한 사전 방역체계(Proactive Security) 구조를 제안하고, 생산설비에 특화된 밀착된 보안, 환경설정, 시스템 관리의 통합적 기능을 제공할 수 있는 신개념의 종단보안(Edge Security)시스템을 설계하고자 한다.

Abstract The conventional network security solutions for manufacturing or factory automation devices are concentrated on protecting the internal networks from the attacks of external networks. Recently, however, so called Day-zero attacks are increased; the threat from internal devices such as notebooks, USB devices are as critical as attacks from external networks. Thus a new security solution is needed to protect manufacturing devices from both external and internal threat. To this purpose, we propose an edge-security system to provide cost effective, integrated, and simple end-point security solution specialized for automated manufacturing devices, which may avoid the shortcomings of NAC.

Key Words : 종단보안, 패킷제어, 방화벽, 접근제어, 설비보안

Ⅰ. 서 론

오늘날 사용되고 있는 대다수 공장 자동화 및 각종 생산설비 시스템은, 보안에 대한 관심이 낮았던 시대에 설계되었다. 이러한 시스템은 비교적 격리된 환경에서 운용되며 주로 독점 소프트웨어와 하드웨어, 통신기술에 의존하였다.

그러나 오늘날에는 생산설비 제어시스템 기반구조의 확장, 시장경쟁 체제 도입 등으로 인하여 생산설비 제어 시스템과 경영 시스템간 상호 연동 필요성 및 제어 시스템간 연계를 위한 상호운용성이 강조되고 있다. 그 결과, 윈도우나 UNIX와 같은 표준 운영체제의 사용, 인터넷이나 공중 전화망, 유·무선 네트워크와 같은 일반 통신 기술이 널리 사용되고 있다.

*정회원, 한성대학교 멀티미디어공학과
**정회원, 한성대학교 정보통신공학과
***정회원, 한성대학교 산업경영공학과
접수일자 2012.2.29, 수정완료 2012년 3월 29일
게재확정일자 2012년 4월 13일

Received: 29 February 2012, Revised: 29 March 2012
Accepted: 13 April 2012
**Corresponding Author: kimsc@hansung.ac.kr,
Dept. of Information and Communication Engineering,
Hansung University, Korea

이와 같이 각종 공장 및 생산설비의 제어 시스템 환경이 급변하고 있지만 아직까지 각종 생산설비 제어시스템의 보안적 측면은 배제되거나 무시되고 있는 실정이다. 기존의 공장 자동화 및 각종 생산설비 시스템의 전통적인 보안 개념은 네트워크의 경계선, 즉 내부 네트워크와 외부 네트워크의 접점에 집중되어 있었다. 네트워크의 경계선에 대한 보안과 외부 트래픽의 차단만 분명히 하면 시스템이 안전하다고 생각하였던 것이다. 그러나 유무선 통신 기술의 발달과 시스템간 상호연동성의 강화로 네트워크의 경계선은 예전과 달리 다양해지고 불분명해졌으며 따라서 특별히 한 지점만 보호하면 된다는 의미의 접점은 사라져가고 있다. 네트워크의 경계선을 우회하여 침입할 수 있는 새로운 기술들이 등장하고 있으며 소위 Day-zero(신종) 공격이 증가하고 있다[1].

변화된 환경에서 외부에서 내부로의 공격은 방화벽 또는 IPS와 같은 보안장비가 담당한다고 하더라도 내부에서의 내부로 향하는 공격에는 거의 무방비상태라 할 수 있다. 이와 같은 결과로 격리된 환경(예: 사설망)에서 작동하고 있는 각종 공장 자동화 기기라하여도 사용자 또는 관리자의 이동저장매체(USB Storage)나 노트북등에 의하여 웜에 감염되거나 바이러스에 감염되어 생산설비가 정지하거나 다른 생산설비로 감염되어 공장 자동화 기기전체가 멈추는 사례가 발생하곤 한다.

실례로 몇 년 전 구미에 있는 한 대기업 계열 전자회사의 공장자동화 프로그램이 들어있는 생산설비가 CIH 바이러스에 감염돼 결국 하루 동안 공장 가동이 중단되는 일이 벌어졌다. 또한 반도체를 생산하는 굴지의 대기업계열 공장에서는 이와 같은 사고가 매년 1회 이상 발생하며 생산중단에 따른 수억원의 피해가 발생하고 있다. 이외에도 보고되지 않은 사고가 수시로 발생하고 있으며 이에 대한 대비책은 아직까지도 미비할 뿐이다.

이와 같이 무정지자동화설비(반도체 제조, 철강 제조, 금융권 장비 등)의 경우 한 번의 동작정지 발생 시 적게는 수백만 원에서 많게는 수십억 원의 금전적 피해가 발행하므로 이러한 무정지자동화설비에서의 기기당 밀착보안(Man to Man Security)을 위한 종단보안(Edge Security)시스템 구성은 필수라고 할 수 있다.

현재 이러한 문제를 해결하기 위한 종단보안(Edge Security) 및 단독보안(Strand alone Security)을 구현할 수 있는 제품으로는 방화벽(Firewall), NAC(Network Access Control), UTM(Unified Threat Management) 등의 장비가 대두되고 있다. 특히 최근에 NAC을 이용한 인증이 종단보안을 위한 방법으로 주목받고 있다[2-6]. 그러나 NAC은 1) 표준화 지연 및 복잡성으로 인한 설치와 운영의 어려움, 2) 인증 위주의 제품특성상 내, 외부 사용자에게 사용상의 불편함 초래, 3) 높은 구축 비용으로 인한 부담 등의 문제점을 가지고 있다. 특히 중소중견기업(SMB: Small Medium Business)에서 NAC등을 이용해 종단보안(Edge Security)을 구현하기에는 단가가 높아 투자 대비 효율성 면에서 적합하지 않은 경우가 대부분이다.

따라서 특화된 공장자동화 생산설비 환경에 맞추어 설치 및 운영 단가가 낮으며 중앙관리가 가능하고 제어가 쉬운 종단보안 시스템의 개발이 필요하다. 현재 생산설비에 특화된 관련 국내외 보안장비나 기술은 전무한 편이며, 일반적인 보안기술보다는 종단설비를 위한 밀착형 보안기술이 적용되어야 한다.

이에 본 논문에서는 저가형의 자동화설비 보안 솔루션으로서 내/외부의 다양한 경로로 유입되는 위협이나 유해 트래픽을 차단하기 위한 사전 방역체계를 구축하고, 생산설비에 밀착된 보안, 환경설정, 시스템 관리의 통합적 기능을 제공할 수 있는 신개념의 종단보안 시스템을 제안하고자 한다. 제안하는 시스템에서는 각 생산설비 기기별로 임베디드 시스템에 기반한 종단보안시스템을 설치하여 공장자동화 설비의 내부보안위협을 차단하고, 종단시스템을 관리하는 중앙관리 서버를 설치하여 원활한 관리를 지원하도록 한다. 본 시스템을 통하여 이상 트래픽 감지 및 미허가된 네트워크 접속 방지, 비인가된 데이터 유출방지, 그리고 설비관리자에 의한 보안위협 발생시 타 기기로의 웜 및 바이러스 전염을 사전에 방지하여 생산설비 전체에 미치는 영향을 최소화 할 수 있을 것이다.

II. 본 론

1. 관련 기술 동향

국내 보안솔루션 동향을 살펴보자면, 1세대와 2세대를 거쳐 현재 보안시장은 3세대로 발전하고 있다. 1세대와 2세대의 보안 장비들이 외부 트래픽을 차단하는데 중점을 둔 네트워크 경계 보안에 주력했다면 3세대 보안은 내/외부의 위협에 모두 대처할 수 있는 엔드포인트 시큐리

티(End Point Security)에 주력할 것으로 예상된다.

외부로부터의 각종 위협을 차단했다고 하더라도, 내부에서 웜이나 바이러스가 존재할 경우 이에 대한 대비책은 각각의 PC나 서버에 설치된 안티바이러스 프로그램이 전부라고 할 수 있다. 하지만 기업의 규모가 커지면 커질수록 이 같은 각 사용자 PC에 대한 관리는 어려운 문제가 된다. 수백 혹은 수천의 사용자들에게 일일이 각종 보안 프로그램 설치를 강요하거나 기업의 보안 정책을 숙지, 교육시키는 등의 작업은 보안 담당자들에게 과중한 업무가 될 수 있으며, 그렇다고 항상 안전한 환경을 유지할 수 있다는 보장도 없다.

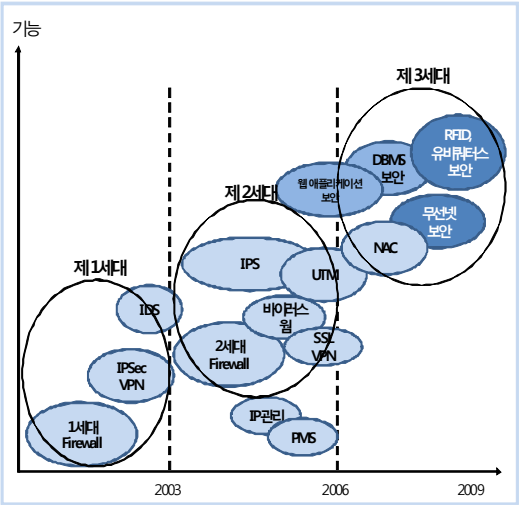

그림 1. 보안솔루션 기술 동향
Fig. 1. Security Solution Trends

같은 문제에 대응하기 위해 최근 부각되고 있는 것이 NAC(Network Access Control)이다[2-5]. 수 년 전에 처음 등장한 NAC 개념은 기업의 보안 정책에 따라 네트워크와 보안 솔루션이 유기적으로 결합해, 엔드포인트에 대한 보안을 강화한다는 점에서 기존의 보안 솔루션과 차별화를 이루며, 최근 관련 업체들의 솔루션 출시 등과 맞물려 급성장하고 있다. 하지만 NAC의 도입은 앞에서 언급한 바와 같이 몇 가지 문제점을 가지고 있다.

- 표준화 지연 및 복잡성으로 인한 설치와 운영의 어려움: NAC의 표준화를 선점하기 위해 각축하며 프레임워크를 추진하고 있는 참여 기업 및 기관은 30여개가 넘으며 이들 중 진정한 리더는 아직 확연히 부각되지 않고 있다. 크게 시스코시스템즈의 NAC (Network Admission Control), 마이크로소프트의 NAP (Network Access Protection), TCG (Trusted Computing Group)의 TNC (Trusted Network Connect) 등이 경쟁을 하고 있으며, 동시에 합종, 연횡이 이루어지고 있다. NAC 방식 면에서도 Agent-based, Agent-less 등 다양한 방법과 많은 옵션 사항이 혼재하며, IETF등의 표준화 기구도 아직 확실한 방향을 정하지 못하고 있다. 따라서 NAC 도입을 검토하는 기관에서는 시스템의 불안정성을 가져올 수 있다.
- 인증 위주의 제품특성상 내, 외부 사용자에게 사용상의 불편함 초래: NAC을 이용한 보안솔루션은 관리자에게는 강력한 기능을 제공하지만 사용자에게는 잦은 서비스 차단으로 인한 고통과 피곤함을 가져올 수 있다. 협력사의 직원이 접근을 할 경우에 사용자 인증을 받아야 하며 사용하는 노트북이나 저장 매체도 단말기 인증을 받아야 하고, 작업중 이상 트래픽이 발생하게 되면 해당 단말기는 네트워크로부터 격리되어야 한다. 이는 외부 직원뿐만 아니라 보안시스템에 익숙하지 않은 내부직원에게도 피곤함을 줄 수 있으며 자동화 설비관리자 역시 네트워크에 대한 인식자체가 부족하여 운영이 쉽지 않을 것이다. 이는 사업장에서 NAC의 많은 옵션을 off 시켜놓고 사용하게 되는 이유가 되며, 따라서 고가의 유휴설비로 전락할 위험성도 있다.
- 높은 구축비용으로 인한 부담: NAC 자체가 워낙 고가이며 NAC 솔루션의 도입은 고가의 전용솔루션을 도입한다는 것 외에도 운영비용, Help Desk 비용 등을 모두 고려해야 한다. 또한 기존에 사용하고 있는 스위치 및 장비와의 인터페이스 및 연동 방식이 맞지 않아 전체 네트워크를 재구성하거나 장비를 교체해야 하는 상황이 발생할 수도 있다. 따라서 투자비용 대비 효율성이 떨어질 수 있다. 특히 중소중견기업(SMB: Small Medium Business)에서 NAC등을 이용해 종단보안(Edge Security)을 구현하기에는 단가가 높아 투자 대비 효율성 면에서 적합하지 않은 경우가 대부분이다.

이러한 상황을 종합해 봤을 때 내/외부의 위협에 모두 대처할 수 있는 제3세대 보안솔루션으로서 NAC의 미래를 밝게 보면서도, 그 문제점을 극복할 수 있는 신개념의

엔드포인트 시큐리티(End Point Security) 구현 기술이 필요하다.

2. 개발 시스템 특성

네트워크 환경의 변화에 따라 내/외부의 위협에 모두 대처할 수 있는 보안솔루션으로서 자동화 기기에 대한 보안 밀착성과 사용 및 관리의 편리성을 갖춘 시스템을 개발한다. 개발 시스템은 신뢰성 있는 패킷제어를 통하여 공장자동화 기기와 같은 생산설비의 보안위협을 원천적으로 차단하며, 능동적인 패킷 분석으로 손쉬운 보안정책 구현을 실현할 수 있도록 한다.

1) 시스템 설계의 기술적 목표

- 패킷 노멀라이제이션(Pachket Normalization)을 기반으로 IP Fragment rebuild, TCP Stream reassembly, TCP state inspection 기술을 적용한다.
- 비정상 패킷 및 유해 트래픽에 대한 세션 킬(kill) 및 블록(block) 기능을 제공한다.
- 비즈니스 트래픽에 대한 트래픽 대역폭 보장 및 제한 기술을 적용한다.
- 프로토콜별 제어가 가능한 정책수립(TCP, UDP, ICMP etc) 기능을 제공한다.
- 하드웨어 장애와 같은 예기치 못한 장애를 대비하여 Bypass모듈을 내장하여 통신망 가용성 극대화를 추구한다.
- 손쉬운 정책수립 및 운영을 위한 윈도우 클라이언트 프로그램을 사용한다.
- 해당 종단에 위치한 생산자동화설비의 정책수립을 위한 네트워크 트래픽 분석기를 내장한다.
- 일별/주별/월별/년별 종단보안(Edge Security)시스템의 CPU사용량 및 in/out bps, pps 리포트를 제공한다.
- 관리자별 정책 수립 권한 부여 및 제어 권한 분리로 체계적이고 제한적인 운영을 가능하게 한다.
- 관리가 쉽고 자체적으로 트래픽분석이 가능하여 손쉬운 정책설계가 가능하도록 설계한다.
- 일별/주별/월별/년별 리포트를 활용한 통계적 관리 기능을 제공한다.
- 운영체제 저장공간으로 HDD를 사용하지 않고 CF 메모리를 이용하여 발열의 최소화 및 장비의 소형화를 구현한다.
- 손쉬운 관리를 위한 중앙관리 시스템을 도입하나, 중앙관리 시스템 없이 단독으로도 동작 및 제어가 가능하도록 설계한다.

2) 시스템 구성 및 기능

전체 시스템은 종단(Edge) 시스템, 중앙관리 시스템, 관리용 콘솔 프로그램의 세 부분으로 구성된다.

표 1. 시스템 구조 및 기능
Table 1. System Elements and Functions

A. 종단(Edge) 시스템
- 외부 유입 패킷에 대한 차단 - 대상 설비 감염시 외부로 확산되는 패밋을 차단하여 설비 고립화 - 장애시 Bypass mode로 네트워크 가용성 보장 - Server 없이도 Console과 1:1 관리가 가능토록 구현
B. 관리서버(Server) 시스템
- 모든 종단(Edge)시스템에 대한 정책관리 수행 - 그룹별로 보안 정책을 차별화시켜 적용할 수 있도록 구현 - 실시간 모니터링을 통한 네트워크 안정성 확보 - 사용자별 인증을 통한 독립적인 관리 권한 부여
C. 매니지먼트 콘솔(Console)
- Windows GUI 환경의 손쉬운 관리 인터페이스 제공 - 각종 보안리포트 제공 기능 - 관리자별 권한별 기능 및 화면 제공 - 직관적이고 쉬운 인터페이스 화면 제공

A. 종단(Edge)시스템 기능

- Contents Blocking 및 Pattern Matching 이 가능한 Inline Packet Analyzing 모듈
- 관리자 정책에 따라 패킷 제어(allow, drop)가 가능한 커널 모듈
- 관리자와의 통신을 위한 TCP 통신 모듈및 파일 전송기능
- 시스템의 상태를 주기적으로 저장할 Database 및 Table 설계
- 설치된 곳의 IP 및 port현황을 파악할 수 있는 Traffic Analyze 기능
- 정책을 손쉽게 생성/수정 하기위한 ip및 port단위의 item화 방법
- 중앙관리 시스템과의 통신을 위한 통신모듈

- 수동 Bypass전환기능
- 시스템 상태의 주기적 파악 및 저장
- 패킷허용정책의 Create/Load/Save 기능

B. 중앙관리 시스템 기능
- 매니지먼트 프로그램과의 통신을 위한 TCP통신 모듈
- 종단보안(Edge Security)시스템과의 통신을 위한 TCP통신 모듈
- 관리자 id와 password 및 정책 그리고 각종 데이터를 저장할 Database시스템 구축
- 관리자 Log 기능(접속/명령/정책설정) 및 리포트(일별/주별/월별/년별) 기능

C. 관리용 콘솔 프로그램 기능
- 중앙관리 시스템과의 통신을 위한 TCP 통신 모듈
- GUI 기반의 관리 프로그램

3. 시스템 구조 설계

종단보안(Edge Security)시스템을 개발하기 전에 가장 먼저 해야 할 일은 개발전략에 맞는 하드웨어를 개발 또는 구성하는 것이다. 최근 네트워크 관련 하드웨어 장비들은 여러 가지 다재다능한 기능을 겸비한 고성능장비로 출시되고 있지만 고가라는 단점이 있다. 이에 적절한 성능과 적절한 가격을 갖춘 장비를 갖추는 것이 중요하다. 종단보안(Edge Security)시스템은 1:1 보안이라는 신개념의 기기로써 고성능을 요하지 않으며 다재다능한 기능보다는 안정된 기능을 요하기 때문에 하드웨어의 안정성 확보가 최우선시 될 것이다. 이에 우선적으로 기출시되어있는 여러 네트워크 장비 및 보드를 선정하여 스트레스 테스트 및 Throughput 테스트, Bypass테스트, 무정지 테스트 등 여러 테스트 항목을 설정하여 적합한 장비를 선정하였다. 하드웨어 선정 후에는 3가지 부분으로 구성된 시스템 설계를 진행하였다. 종단보안(Edge Security)시스템의 패킷제어 커널 모듈과 관리 프로세서 부분, 중앙관리 시스템의 제어 부분, 관리용 콘솔 프로그램 부분의 3가지 요소로 나뉘어 각각 설계 및 통합을 수행하였다.

종단보안(Edge Security)시스템의 패킷제어 커널모듈은 허가된 패킷이외에는 모든 패킷을 Drop해야 하므로 다양한 트래픽을 수용하는 테스트환경에 노출시켜 제품의 신뢰성을 테스트 받게 된다.

중앙관리시스템은 분산설치된 각 종단보안 (Edge Security) 시스템의 중앙통제서버로써 각종 정책을 데이터베이스화하여 저장하고 배포하며 관리자 인증 및 권한 설정 등등의 역할을 수행하게 된다. 이에 중앙관리 시스템은 관리자의 의한 정책의 생성/저장/삭제를 테스트 하게 된다.

정책 적용시 관리자 실수에 의한 정책 에러가 발생할 수도 있는 바, 이러한 경우를 최소화하기 위하여 패킷제어 커널모듈은 drop시킨 IP 패킷의 일부분을 항시 유지하게 된다. 유지할 정보로는 source IP address와 port 그리고 destination IP address와 port로써 정책설정의 근간을 이루는 부분이라 할 수 있다. 대략적으로 300~500개의 마지막으로 drop된 패킷정보를 원형버퍼 형식으로 저장하게 되며 정책에러로 설비와의 통신이 되지 않을 경우 관리자는 이러한 정보를 통하여 정책 적용의 실수를 조기에 발견, 수정할 수 있게 된다.

일반적으로 정책 설정 에러는 생산설비라인의 네트워크가 잘못 파악되거나 누락되어 발생하는데 이러한 실수를 방지하고자 Traffic Analyze기능을 탑재하게 된다. 이 기능은 네트워크에 흘러다니는 IP를 캡쳐하여 source IP address, port 그리고 destination IP address, port 및 direction 을 파악하여 관리자에게 리포팅하는 기능을 수행하게 된다.

매니지먼트 프로그램은 관리자가 보다 편하게 종단보안(Edge Security)시스템을 운영하기위한 콘솔(Console)로써 사용되는데 일반적인 네트워크 지식으로도 충분히 정책설정을 할 수 있도록 직관적이고 다양한 도움말을 제공하게 되며 중앙관리시스템으로 접속할 수 있으며 종단보안(Edge Security)시스템에 직접 1:1로 접속할 수도 있다. 이때 사용자 별로 id와 password인증을 실시하게 되며 권한 별로 실행할 수 있는 명령아이콘이 구분되게 된다.

그림 2는 종단보안시스템의 구조에 대한 예시를 보여주고 있으며, 그림 3은 종단보안 시스템의 관리 프로세스 흐름도를 나타낸다. 기술의 성능 검증을 위하여 인위적인 정책 설정 에러 및 사용자 인증에러, 관리자 인증 에러 상황 등을 재연 가능하도록 구현한 테스트 툴을 개발하여 반복적인 테스트 결과 안정적인 동작을 보이는 지 검증하도록 한다.

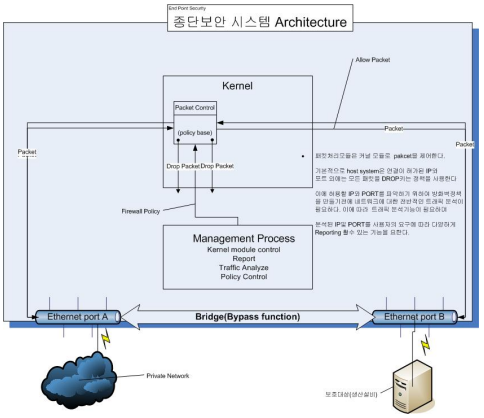

그림 2. 종단(Edge) 보안시스템 구조 예시
Fig. 2. Edge Security System Architecture Exa mple

1) 종단보안 시스템 동작

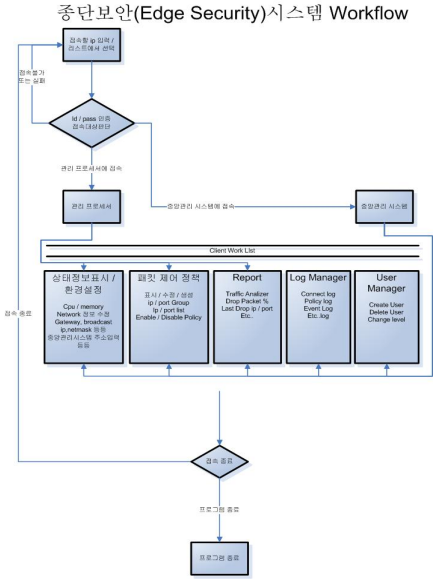

그림 3. 종단보안시스템 작업 흐름도
Fig. 3. Edge Security System Workflow example

- 패킷의 제어는 커널의 모듈형태로 제작하여 처리속도를 향상
- 사용자 정책에 따라 해당 패킷을 allow또는 Drop
- 전반적인 시스템의 제어를 위하여 별도의 프로세서가 동작
- 두 개의 Ethernet Port 를 Bridge 로 사용하여 패킷을 Inline형태로 제어
- Port A와 B는 Bypass기능내장으로 정전과 같은 사고시 Bypass모드로 자동전환
- IP 만을 통제하게 되며 TCP, UDP, ICMP를 제외한 모든 패킷은 허용
- 각 보호 시스템은 주기적으로 중앙관리시스템과 정책에 관한 변경사항을 체크.

2) 종단보안 시스템 구성도

본 시스템은 다음과 같은 시스템 사양을 적용하여 설계 및 개발되었으며, 실제 현장에의 적용시에는 설비 및 대상 환경에 따라 동적으로 구성하도록 한다.

* 종단보안(Edge Security)시스템 : ASIC Appliance
- cpu : 펜티엄4 400MHz 이상, 전용 ASIC 보드 사용
- Ram : 512M
- Storage : 512M 이상 Comfact Flash Memory Card
- OS : Linux or Embedded System
- 2~4 Ehternet Lan Port(Bypass function 내장)

* 중앙 관리(Central Management) 시스템
- cpu: 펜티엄 4 1GHz 이상
- Ram : 1G
- Storage : 60G
- OS : Linux
- 사용자 및 정책 저장을 위한 Database
- 1 Ethernet Lan Port

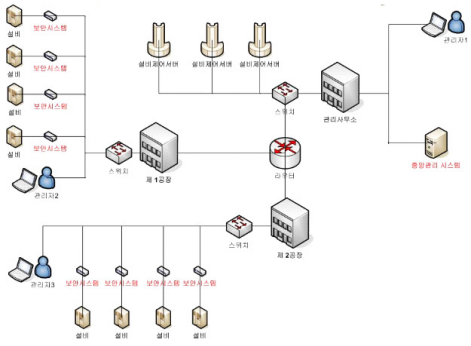

그림 4. 자동화 설비보안 전체 시스템 구성
Fig. 4. Organization of Edge Security Systems.

4. 시스템 개발 효과

현재 네트워크는 끝없이 넓어지고 진화하며 빨라져만 가고 있다. 이와 동시에 각 산업의 네트워크 의존도 역시 높아져만 가고 있는 실정이다. 이러한 네트워크의 대형화 및 고속화가 진행될수록 네트워크의 위협도 기하급수적으

로 늘어나게 마련이다. 전 세계가 하나의 Open Network로 구성될 날도 멀지 않았으며 이와 함께 노트북, 스마트폰, 각종 이동식 저장매체의 급속한 보급으로 인하여 세계 어느 곳에서도 보안위협이 존재할 수 있게 되었다.

산업화 역시 거대해지고 공장자동화를 이룬지 오래지만 보안에 대한 인식은 낮기만 하며 현재 지속적인 보안위협에 노출되고 있다. 자동화 설비가 커질수록 위험요소는 다양하며 그 피해가 다른 기기로 전파될 가능성이 높다. 이러한 보안위협에 대비하여 중/대형 자동화 설비 체제를 갖춘 사업장이라면 반드시 생산설비 종단보안(Edge Security)시스템을 설치하여 각종 네트워크 위협을 최소화 하는 것이 공장자동화의 기본이 될 수도 있다.

이러한 사업장의 예로는 중소기업의 공장자동화 라인 또는 반도체, 철강, 자동차, 금융권 등등 대형설비에 적용할 수 있으며 국내외 시장규모로 살펴볼 때 이미 거대한 규모의 잠재적 자동화 생산설비 종단보안(Edge Security) 시스템 시장이 형성되어 있다고 할 수 있다.

앞으로 생산설비에 적용될 보안기술은 기존의 보안기술과 크게 다르지 않지만 단독보안(Stand alone Security) 기술과 종단보안(Edge Security) 개념을 통합 수용하며, 생산설비에 밀착된 보안, 환경설정과 시스템 관리의 통합적 기능을 제공할 수 있는 신개념의 장비라고 설명할 수 있다. 보안 솔루션은 보안문제가 생겼을 때 동작하는 것으로 문제가 생기지 않는 상태에서는 만약의 경우에 대비하여 설치하는 Overhead 비용이 된다. 따라서 특히 보안 장비 및 기술에 익숙하지 않은 생산자동화 설비의 운영 기관에서는 설치 및 사용상의 복잡도와 불확실성, 어려움을 극복하고 보다 낮은 구축비용과 사용의 편리성을 제공해주는, 투자 대비 효율성이 높은 솔루션이 필요하다. 따라서 이러한 목적에 적합한 보안시스템을 개발함으로써 시장에서 요구하는 Needs를 만족시키고 기술이전을 통한 제품화, 사업화를 통해 관련 산업 발전에 기여하리라 생각된다.

1) 기술적 기대효과

- 자동화 생산설비에 특화된 밀착된 보안, 환경설정, 시스템 관리의 통합적 기능을 제공할 수 있는 신개념의 보안(Edge Security)시스템 제공
- 일반적인 단말 보안이나 Network 보안과는 달리 생산설비에 특화된, 외부 및 내부 위협을 모두 차단할 수 있는 신개념의 보안솔루션 제공
- 내/외부의 다양한 경로로 유입되는 위협이나 유해 트래픽을 모두 차단할 수 있는 단순하고 안정적인 보안솔루션 제공
- 고비용 NAC 솔루션에 비하여 가격대비 효율성이 높은 보안솔루션 제공
- 반도체 라인, 자동차 등 무중단 생산 라인, 제철 고로 생산 라인, 금융권 등 생산 자동화 설비 및 무중단 설비에 대한 적용이 가능
- 생산자동화 설비의 보안정책 중앙관리 시스템 제공하며, 자동화 생산 설비의 모니터링 기능 제공
- 개별 생산설비의 기기당 밀착형 보안시스템 구축하며, Bypass기능을 탑재하여 보안기능의 에러 발생 시에도 Network 가용성을 최대한 보장
- 패킷 제어기능을 종단시스템별로 구현하여 유해트래픽 차단하고, 감염시스템의 격리 및 차단을 통한 확산 방지와 취약지점 격리기능

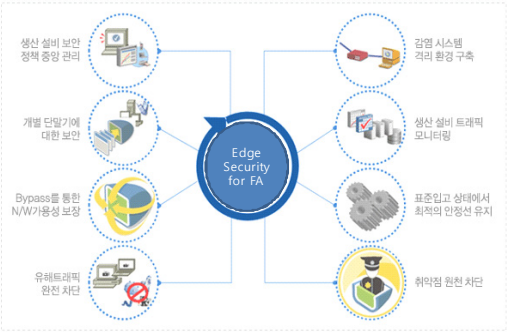

그림 5. 연구결과의 기술적 기대효과
Fig. 5. Expected Technical Results.

III. 결 론

네트워크 환경의 변화에 따라 내/외부의 위협에 모두 대처할 수 있는 보안솔루션으로서 자동화 기기에 대한 보안 밀착성과 사용 및 관리의 편리성을 갖춘 시스템구조를 제안하였다. 개발 시스템은 신뢰성 있는 패킷제어를 통하여 공장자동화 생산설비의 보안위협을 원천적으로 차단하며, 능동적인 패킷 분석으로 손쉬운 보안 정책 구현을 실현할 수 있도록 한다. 본 시스템에서는 각 생산설비별로 임베디드 시스템에 기반한 종단보안시스템을 설치하여 공장자동화 설비의 내부보안위협을 차단하고, 종단(Edge) 시스템을 관리하는 중앙관리 서버(Server)를 설치하여 원활한 관리를 지원하도록 한다.

참 고 문 헌

[1] I. Chung, I. Kim, J. Oh, J. Chang, "Intelligent Network Security Technology for Zero-day attacks," Journal of Korea Information and Communications Society, Vol. 24, No. 11, pp. 14-24, Nov. 2007

[2] Ro chul-woo, Kee-Won Kim, Lee ji-woong, Jeon jae-hyun, "Computer Network Security Platform with NAC," Proceedings of Spring Conference of Korea Contents Association, Vol. 7, No. 1, pp. 8-11, May 2009.

[3] KyoungGyu Lee, Youngwoo Lee, "The NAC Application for Wireless Sensor Networks," Proceedings of KCC 2007, Vol. 34, No. 1(D), pp. 257-260, Jun. 2007

[4] Jong-Hyun Sun, Myung-Mook Han, "Group Decision through Behavior Information in the pre-connect of NAC," Proceedings of Fall Conference of Korean Society for Internet Information, pp. 55-58, Oct. 2009

[5] Won-Jin Lee, Kee-Won Kim, Ki-Dong Bu, Jongjung Woo, "A Study on the Adoption of NAC for Guaranteeing Reliability of u-Campus Network," Journal of Korea Institute of Information Technology, pp. 252-258, Aug. 2009

[6] Min-Gyun Kang, Seok-Soo Kim, "Design and Implementation of Security Solution Structure to Enhance Inside Security in Enterprise Security Management System," Journal of Korea Contents Association, Vol. 5, No. 6, pp. 360-367, Dec. 2005

[7] H. Ju, "A Study on the Integrated Security Solution for Future Network," Communications of Korean Society for Internet Information, Vol. 10, No. 4, pp. 68-76, Dec. 2009

※ 본 연구는 한성대학교 교내연구비 지원으로 수행되었음.

저자 소개

황 호 영 (정회원)

- 1993 서울대학교 컴퓨터공학 학사
- 1995 서울대학교 컴퓨터공학 석사
- 2003 서울대학교 전기컴퓨터공학 박사
- 2003 ~ 2007 안양대학교 디지털미디어학부 조교수
- 2007 ~ 현재 한성대학교 멀티미디어 공학과 부교수

<주관심분야 : 정보통신, 유무선 네트워크, 센서네트워크, 멀티미디어>

노 광 현 (정회원)

- 1995 고려대학교 산업공학 학사
- 1997 고려대학교 산업공학 석사
- 2001 고려대학교 산업공학 박사
- 2001 ~ 2002 Ecole des Mines de Paris(Post-Doc)
- 2003 ~ 2006 한국전자통신연구원 연구원
- 2006 ~ 2007 한국항공우주연구원 선임연구원
- 2007 ~ 현재 한성대학교 산업경영공학과 부교수

<주관심분야 : 차세대이동통신, ITS, RFID/USN>

김 승 천 (정회원)

- 1994 연세대학교 전자공학과 학사
- 1996 연세대학교 전자공학과 석사
- 1999 연세대학교 전기컴퓨터공학과 박사
- 2000 Univ. of Sydney Post Doc.
- 2001 ~ 2003 LG전자 DTV연구소 선임연구원
- 2003 ~ 현재 한성대학교 정보시스템공학과 부교수

<주관심분야 : 위성통신망, 고속통신망, 무선통신, 유비쿼터스 센서 네트워크>