86
논문번호 09-02-12

신・재생에너지 발전설비의 원격 데이터 수집을 위한 통합 보안 관리시스템에 관한 연구

A Study on Unified Security Management System for remote data acquisition of New and Renewable Energy Facilities

김 형 주*, 임 중 열*★
Hyoung-ju Kim*, Jung-Yol Lim*★

ABSTRACT

Development and diffusion of a new and renewable energy are acutely required at domestic energy actualities to be inferior as industrialization is accelerated, and use of information electric appliance is increased rapidly.
For the diessemination and practical use of new and renewable energy, this paper presents an unified security management system that is efficiently able to acquire operational status date and control distributed generation facilities. Also, the unified security management system is suggested to protect gathered operational status date from unpredictable problems such as computer virus, spy ware, and any other network problems.

요 약

산업화가 가속되고 정보 가전기기의 사용이 급증함에 따라 열악한 국내 에너지 현실에서 신・재생 에너지의 개발과 보급은 절실히 요구되고 있다. 따라서 본 논문에서는 신・재생에너지의 적극적인 보급과 활용을 위하여, 분산 배치된 신・재생에너지 발전설비의 발전 데이터를 효율적으로 관리할 수 있는 통합 관리 운영시스템을 제안하였다. 또한 컴퓨터 바이러스. 스파이웨어와 다른 네트워크 문제로 인해 수집된 데이터의 유실을 방지하기 위해 통합 보완 관리 시스템을 적용하여 발전 데이터를 보호하도록 구성하였다.

Key Words : New & Renewable Energy, Unified Security Management System, Remote Monitoring

Ⅰ. 서론

산업화가 가속되고 정보 가전기기의 사용이 기하급수적으로 늘어남에 따라 에너지 사용량도 비례하여 증가하고 있다. 국제 유가 폭등으로 인해 세계 각국의 에너지 확보전이 치열해지고 BRICs' 국가의 소비 급증에 따른 에너지안보의 중요성이 대두되고 있다. 우리나라의 경우 세계 10대 에너지 소비국, 세계 5위 석유 수입국, 세계 2위 천연가스 수입국,96[%]에 이르는 높은 에너지 해외 의존도를 보이고 있으며 에너지 다 소비형 산업구조와 소비구조로 인해 향후 에너지 대란이 예측되고 있다. 이러한 열악한 국내 에너지 현실에서 태양광·풍력·수소연료전지로 대표되는 신·재생에너지원의 개발과 보급은 필수적이고 매우 중요한 사안이라 할 수 있으며, 발전설비의 부지선정 및 설계 자료로서의 신뢰할 수 있는 기초자료가 절실히 요구되고 있다. 하지만 효율적인 정보제공체계가 마련되지 않아 데이터의 확보가 어렵고, 데이터의 축적 기반이 열악하여 기존 데이터의 유실빈도가 상당히 높은 편이어서 지속가능한 신·재생에너지 이용가능성 평가 및 신뢰성 확보를 위한 체계적인 시스템은 현재 마련되어 있지 않다[1].

이러한 배경으로 본 논문에서는 지역적으로 분산 배치된 신・재생에너지 발전설비들을 효율적으로 관

* 남부대학교 디지털경영정보학과
(Department of Digital Management Information Graduate school of Nambu University)
★ 교신저자 (Corresponding author)
接受日:2009年 5月 12日, 修正完了日: 2009年 6月 16日

리하기위해 각각의 발전현황을 한 곳에서 통합적으로 모니터링 할 수 있는 네트워크 기반의 원격 데이터 수집/관리 시스템을 제안하였고, 추가적으로 축적된 데이터 유실 방지를 위해 다수의 보안시스템을 한 번에 통합 관리하고 모니터링 할 수 있는 새로운 형태의 통합 보안 관리 시스템을 개발하고자 한다.

II. 원격 데이터 수집/관리 시스템

가. 시스템 개요

본 시스템은 원격지에 떨어진 각각의 발전시스템들을 한곳에서 통합하여 운전데이터를 모니터링 방식으로 그림 1에 원격 데이터 수집/관리 시스템의 개체도를 나타내었으며, 분산 배치된 신·재생 에너지 발전설비들은 A 발전소의 3kW 태양광 발전시스템과 B 발전소의 3kW급 풍력/태양광 복합발전시스템, C 발전소의 30kW 태양광 발전시스템, 1kW 가정용 연료전지, 태양열 온수 시스템 등이 있다. 추가적으로 C 발전소에서 간헐적으로 운전되고 있는 수전해장치, 천연가스 이용 수소 발생 개질시스템 등과 같은 신·재생에너지 관련 설비들도 본 원격 데이터 수집/관리 시스템에 적용되어 구축하였다.

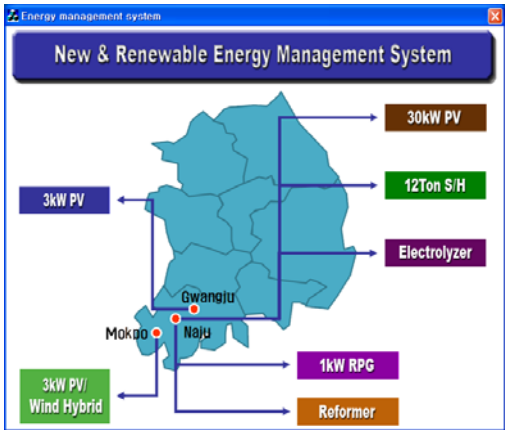

Fig. 1. The component of remote data acquisition and Management System

그림 1. 원격 데이터 수집/관리 시스템 개체도

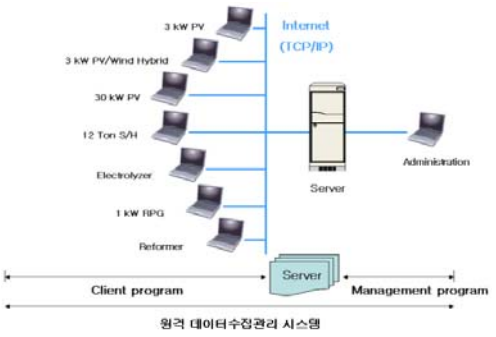

Fig. 2. The structure of remote data acquisition and Management System

그림 2. 원격 데이터 수집/관리 시스템 구성도

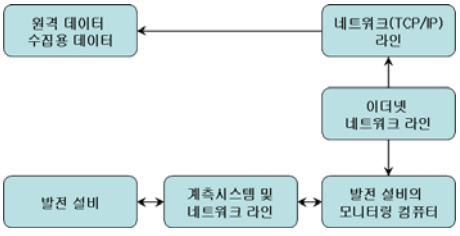

Fig. 3. The flow chart of remote data acquisition and Management System

그림 3. 원격 데이터 수집/관리 시스템의 데이터 흐름도

원격 데이터 수집/관리 시스템은 직접 통신과 간접 통신 방식을 혼합하여 원격지에 떨어진 각각의 시스템을 한곳에서 통합 모니터링을 할 수 있도록 구축하였다. TCP/IP 프로토콜을 기반으로 visual C++를 이용하여 서버와 각 지역의 컴퓨터를 1:1로 연결할 수 있는 client 프로그램을 구성하였고, 이렇게 연결된 각각의 네트워크의 정보를 한곳에서 모두 연결할 수 있도록 management 프로그램을 그림 2와 같이 구성하였다. client 프로그램은 컴퓨터의 IP 주소와 이름을 서버에 전달하고 management 프로그램은 이 정보를 서버로부터 전달 받아 단일 네트워크를 형성하게 된다. client-management 프로그램은 단일 네트워크로 구성된 모든 컴퓨터에 동시 접속이 가능하기 때문에 단일 네트워크로 구성된 컴퓨터들을 하나의 표시 창에서 쉽게 관리할 수 있도록 원격 데이터 수집/관리 시스템을 구성하여 모니터링이 가능하도록 하였다.

그림 3은 원격 데이터 수집/관리 시스템의 데이터 흐름도이다.

각 발전설비의 모니터링 컴퓨터로부터 저장된 발전

데이터를 호스트 컴퓨터에서 통합 관리 시스템을 이용하여 데이터를 취득한다. 이는 호스트 컴퓨터와 각 클라이언트 컴퓨터를 연계하여, 분산 배치된 각 모니터링 컴퓨터에 실시간으로 저장되는 발전 데이터를 호스트 컴퓨터에서 취득함에 있어 용이하도록 하였다.

다음 그림 4는 원격 데이터 수집/관리 시스템의 측정 파라미터를 나타낸 것이다.

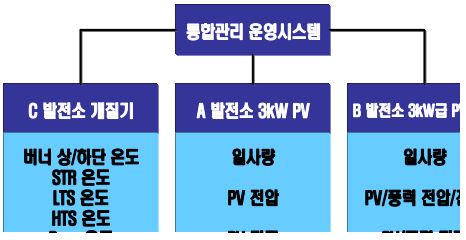

Fig. 4. The Measurement Parameter
그림 4. 측정 파라미터

나. 통합 보안 관리 시스템 설계

본 연구에 의해 구축된 원격 데이터 수집/관리 시스템은 개방 네트워크를 통한 데이터의 공유 및 전송 등의 이용 비율이 증가하고 침입의 유형이 매우 다양화 되면서 데이터의 무결성과 보안에 대한 위험성이 더욱 증가하게 되었다. 예를 들어 네트워크를 통하여 침입하거나 사용자의 부주의로 인해 악성 프로그램이 설치되어 통합 모니터링 관련 소프트웨어가 피해를 입게 된다면 장기간에 걸쳐 축적된 데이터가 한순간에 유실될 수도 있으며, 이를 복구하는 데에도 많은 시간과 노력을 허비하게 된다[2,3]. 이 때문에 네트워크 환경에서 허가받지 않은 사용자로부터 데이터를 내·외부의 공격으로부터 안전하게 보호할 수 있도록 보안을 적용한 효율적인 통합 보안 관리 시스템 모델을 제안하였다.

네트워크 보안이란 일차적인 보안으로 컴퓨터나 통신매체 그 자체를 포함하여 하드웨어가 포함하고 있는 정보를 돌발적인 사고나 악의적인 해킹으로부터 보호함과 동시에 시스템의 안전성과 신뢰성을 확보하려고 하는 것을 말한다. 네트워크 간에 철저하게 분리해 지원하고 분리된 네트워크 간에 연동하는 트래픽에 대한 안전도 검사가 주요기능이다. 네트워크 보안 시스템으로는 침입 차단 시스템(Firewall), 침입 탐지 시스템(IDS: Intrusion Detection System), 침입 방지 시스템(IPS: Intrusion Prevention System), 가상사설망(VPN: Virtual Private Network) 등이 있다[5].

본 연구에서 제안하고자 하는 통합 보안 관리 시스템이란 다양한 독립된 네트워크 보안 시스템들을 하나로 통합해 관리해 줄 수 있는 시스템이다.

통합 관리란 한마디로 말하여 지속적이고 상시적인 위험관리(Risk Management)활동이며 업무(비지니스)의 연속성을 위한 네트워크, 시스템 등의 주요 인프라에 대한 위협요인을 사전에 예방하고 위협요인 발생 시 적절히 대응하기 위한 일련의 제반 활동이다.

통합 보안 관리 시스템은 전사적인 보안 시스템에 대한 일관성 있는 보안 관리를 추구하고 보안 사고를 원인으로 하는 정보 시스템의 침해 사고 예방 및 신속한 식별 조치가 가능하다. 또한 최소화된 보안관리 인력으로 체계적인 유지 및 관리를 추구하고, 보안 관리를 위해 투입되는 인력, 비용, 시간 등이 절감되는 장점을 가지고 있다.

그림 5는 본 연구에서 제시한 통합 보안 관리 시스템 구조를 보여준다. 통합 보완 관리 시스템을 내부 네트워크와 외부 네트워크 사이의 통로에 설치하여 데이터 수집/관리 시스템과 분산 배치된 각각의 발전 시스템과의 데이터 통신 시 암호화 통신을 통해 데이터의 노출 및 위변조를 방지하고 (네트워크와 시스템 측면에서의 보안 위협 요소인) 시스템 권한 습득 및 정보 습득에 목적을 둔 공격과 Buffer overflow를 이용한 DDoS(Distribute Denial of Service attack: 분산 서비스 거부), 웜의 무작위 공격, 유해 트래픽에 의한 외부의 불법적인 접근으로부터 내부 네트워크를 방어하도록 하였다.

이 시스템의 구성은 두 네트워크 간의 트래픽을 제어하기 위한 침입 차단 시스템(방화벽: Firewall)과 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하고 차단조치 할 수 있는 능동적인 보안 개념인 침입 방지 시스템(IPS: Intrusion Prevention System), 둘 이상의 네트워크를 안전하게 연결하여 암호화된 데이터를 전송할 수 있는 가상사설망(VPN : Virtual Private Network), 코드 및 파일에 대한 실시간 바이러스 및 스파이웨어, 백 도어 및 악성코드로부터 시스템의 자원을 보호하는 바이러스 월(Viruswall)시스템 4가지의 기능을 하나로 통합하여 개발한 통합 보안 관리 시스템 모델이다.

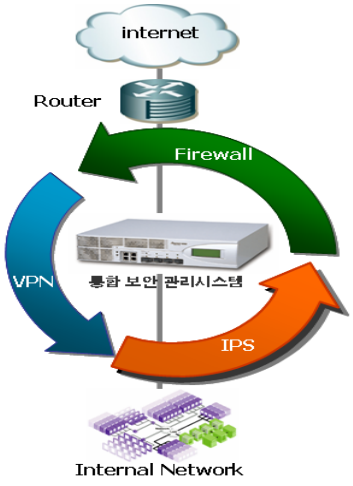

Fig. 5. The structure of unified security management system
그림 5. 통합 보안 관리 시스템의 구조

Ⅲ. 시스템 구축

가. 통합 보안 관리 시스템 구축

본 시스템은 앞에서 언급한 네트워크 보안시스템인 침입 차단 시스템(방화벽: Firewall)과 바이러스 월 시스템을 하나의 통합 보안 관리 시스템으로 개발하여 한 번에 여러 개의 보안제품을 동시에 손쉽게 관리할 수 있도록 구축하였다.

각각의 분산 배치된 지역발전설비에 통합 보안 관리 시스템을 설치하고 중앙발전설비에는 통합 보안 관리 시스템과 분산된 통합 관리 시스템들을 관리할 수 있는 통합 집중 관리 시스템을 설치하여 중앙발전설비와 지역발전설비간의 원격 LAN을 통해 연결하였다.

이로 인해 공개된 인터넷 망으로부터 내부 망을 보호하고자 중앙발전설비와 각각의 지역발전설비를 가상사설망 시스템을 설치하여 데이터의 무결성을 유지하고 외부로부터의 불순한 침입을 원천적으로 차단하고 있다.

본 시스템에서 사용한 통합 집중관리 시스템은 다수의 게이트 군과 클라이언트 군을 통합 관리하는 시스템으로 중앙관리, 통합 로그 관리, 전체 장비의 실시간 상태 모니터링 등을 통합적이고 집중적으로 관리하는 기능을 제공하고 있다. 그리하여 각각의 분산되어 있는 지역발전설비 시스템의 통합 보안 관리 시스템을 실시간 모니터링 보안 장비들의 상태, 로그 관리, 감사 기록 및 추적하고 장비 및 사용자 인증 및 암호화 알고리즘을 설정하고 있다. 또한 IP, 사용자, 사용자 보안 정책 설정 및 분배하는 보안 정책 관리 기능을 가지고 있으며 로그 관리 및 보관의 한계를 극복하고 다양한 모니터링 기능을 제공하기 위한 대용량, 고 가용성, 고성능 DBMS(DataBase Management System) 기반의 로그 관리 시스템 제공으로 관리의 편의성을 제공하고 있다.

이러한 통합 집중 관리 시스템을 중앙발전설비 메인시스템에 설치하고 각각의 지역발전설비의 통합 보안 관리시스템을 원격 네트워크를 이용하여 그림 6과 같이 구성하였다.

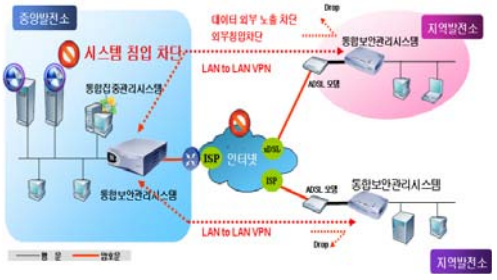

Fig. 6. The structure of unified security management system
그림 6. 통합 보안 관리시스템 구성도

본 시스템은 보다 전문적이고 다양한 보안 시스템들을 실시간 모니터링을 통해 손쉽게 관리하고 VPN을 이용하여 손쉬운 대역폭 증설 및 내부 트래픽을 조절하여 트래픽 문제를 해결하고 향후 추가된 전용선 백업 및 대체 등 다양한 형태로 구축할 수 있도록 하였다.

나. 네트워크기반에 제안된 통합 보안 관리 시스템 적용 및 평가

본 시스템을 적용해보면 서비스의 사용여부, 출발지 네트워크, 목적지 네트워크, 서비스, 정책 및 시간을 선택할 수 있고 간단하게 보안정책을 추가하여 트래픽을 제어할 수 있는 보안 정책화면과 추가된 보안정책을 실시간으로 확인 및 적용이 가능한 보안 정책 목록 화면으로 구성되어있다.

그림 7과 그림 8은 보안 시스템 중 IPS 보안정책을 적용한 화면과 IPS 로그 viewer 화면과 보안 정책 목록 및 적용된 화면으로서, 보안정책에서 탐지 및 차단 정책 적용을 통해 유해 트래픽 탐지만 할 것인지, 차단을 할 것인지, 보안정책을 적용할 것인지를 결정할 수 있다.

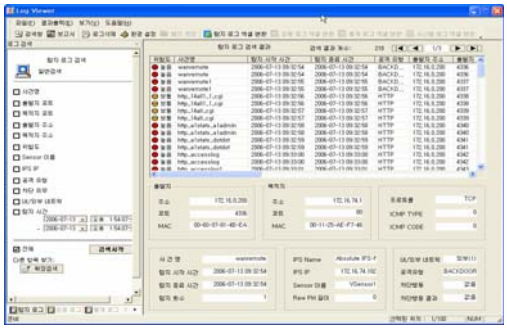

Fig. 7. IPS log viewer
그림 7. IPS 로그 Viewer

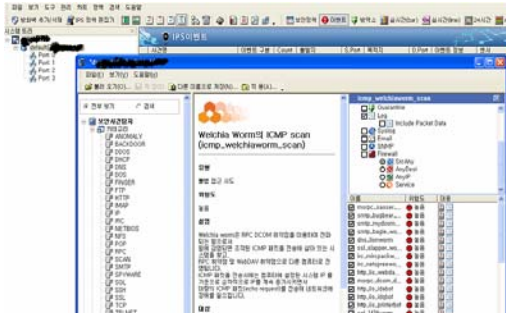

Fig. 8. The list of IPS security policy
그림 8. IPS 보안 정책 목록

그림 9는 시스템 자원 모니터링 화면으로 보안 시스템 사용 현황을 모니터링 한 결과화면으로 그림 9-(a)는 IPS 시스템의 CPU와 메모리의 사용현황을 나타내주고, 그림 9-(b)는 시스템에서 탐지하고 있는 모듈들을 보여주고 있다. 그림 9-(c)는 Top 포트 분석그래프로 이상 트래픽 분석 및 신종 바이러스들의 식별과 네트워크 전체 현황을 나타내주고 있다.

그림 10은 네트워크 트래픽을 한눈에 볼 수 있게 해주는 BPS/PPS 분석 그래프 화면으로 네트워크 자원 모니터링 화면으로 실시간 사용 트래픽 사용현황 모니터링을 통해 유해 트래픽 유입 여부를 모니터링 한 결과이다.

그림 11은 보안 로그 모니터링 화면으로 IPS 기능에 따라 차단된 이벤트 확인을 통해 외부 불법 침입 시도를 모니터링 한다. 즉 실시간으로 내부 사용자들의 네트워크에 비정상 트래픽이 검출되는지를 확인하고 해당IP로부터 비정상 트래픽이 검출되면 특정시간 이후에 네트워크로부터 분리 차단되는지를 확인하고 탐지된 비정상 트래픽에 대한 메시지와 해당IP, 모듈, 조치사항들을 모니터링 화면이다.

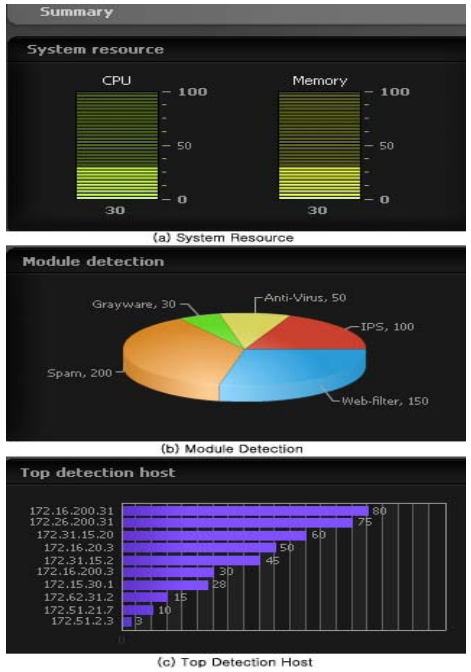

Fig. 9. IPS monitoring-system resource monitoring
그림 9. IPS 모니터링 - 시스템 자원 모니터링

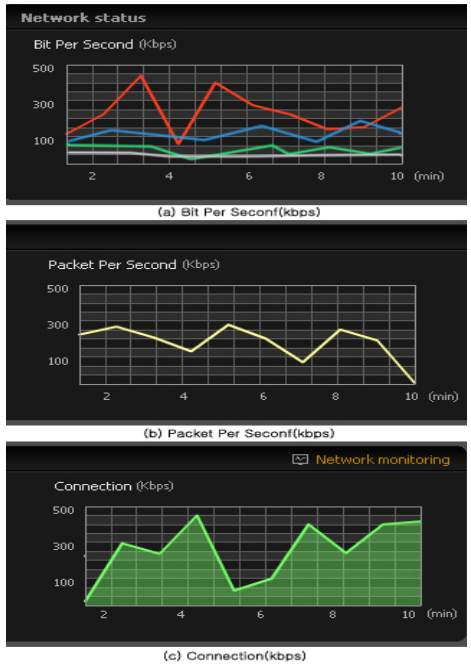

Fig. 10. IPS monitoring-network resource monitoring
그림 10. IPS 모니터링 - 네트워크 자원 모니터링

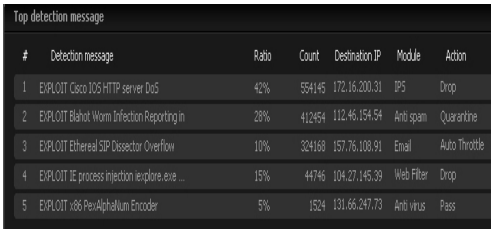

Fig. 11. IPS monitoring - Security Log monitoring
그림 11. IPS 모니터링 - 보안 로그 모니터링

제안된 통합 보안 관리 시스템 중 방화벽 시스템을 적용시키면 그림 12와 같이 방화벽 로그 서버 관리 화면이 나오며 보안정책에 의해 허용된 트래픽과 보안정책에 의해 거부된 트래픽의 모니터링을 확인할 수 있으며 보안정책에 따른 비정상 트래픽은 차단되었음을 확인할 수 있다.

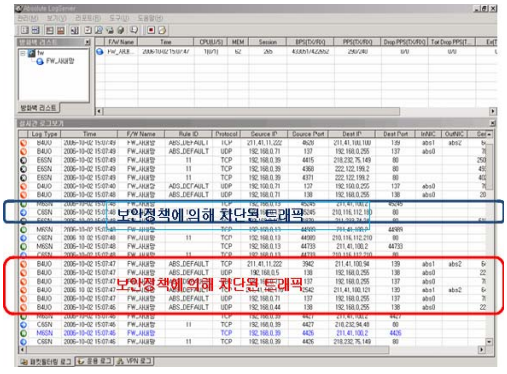

Fig. 12. The firewall log server screen
그림 12. 방화벽 로그서버화면

그림 13과 그림 14는 TCP/UDP/ICMP 등 각 프로토콜별, 그리고 각 포트 번호별 단위 시간당 최대 전송 가능한 패킷의 수 또는 세션의 수에 대한 트래픽 사용 현황과 모니터링 과다 트래픽을 확인할 수 있는 모니터링 화면이다. 그림 13은 네트워크 사용량에 관한 모니터링 화면이고, 그림 14는 네트워크 사용현황으로 각 프로토콜 및 서비스별 사용량과 비율을 모니터링 화면으로 네트워크 사용량 상세 모니터링을 통해 Protocol 별 사용량 확인 및 서비스 사용량 확인을 통해 위협요소 사전 확인과 이상 트래픽 발생여부를 확인한다.

이와 같이 통합 집중 관리 시스템을 통해 중앙 발전설비와 지역발전설비의 데이터 통신간의 데이터 노출 및 위변조를 방지하고 접근 제어 보안정책을 통한 인가되지 않은 사용자의 접근을 차단하며 방화벽시스템과 IPS, 바이러스 월을 통해 보다 안정적으로 수집된 데이터를 보호하도록 시스템을 구축하였다.

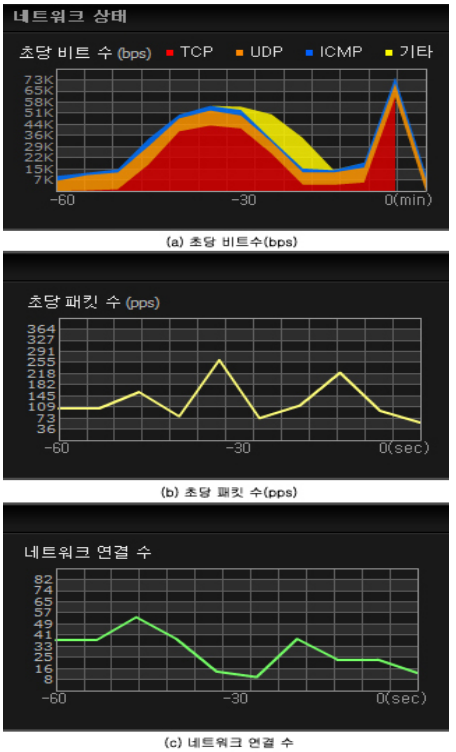

Fig. 13. The monitoring of Network Status
그림 13. 네트워크 사용량에 관한 모니터링

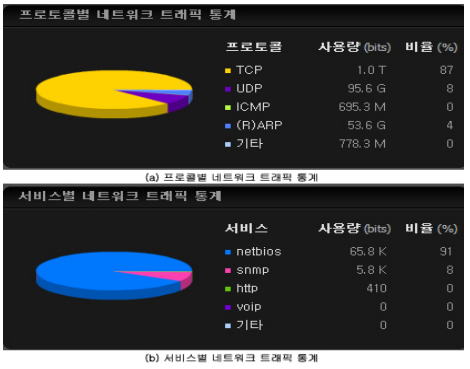

Fig. 14. The Network Traffic Statistic of Protocol and Service
그림 14. 프로토콜 및 서비스별 네트워크 트래픽 통계

그림 15는 각 에너지원으로 선별된 3개 발전소를 모니터링 데이터이다. 모니터링 에너지원은 태양광, 풍력, 연료전지로써 신·재생에너지를 대표하는 에너지원을 선정하였다. 태양광발전시스템은 태양의 일사량에 따라 좌우되어 낮 동안에 발전이 이루어지고, 풍력발전시스템은 바람의 세기에 따라 발전량이 변동되는데 국내 기후 여건상 낮보다는 밤 동안에 큰 발전량을 확보할 수 있으며, 연료전지시스템은 가스를 개질시켜 발생된 수소를 이용하여 발전되는 시스템으로 밤과 낮에 상관없이 수소의 순도에 의하여 안정적인 발전량을 확보할 수 있다. 그림 15-(a)는 A 발전소의 2008년 태양광발전현황을 월단위로 나타낸 것이고, 그림 15-(b)는 B 발전소의 태양광/풍력발전량을 일일단위로 나타냈으며, 그림 15-(c)는 C 발전소의 구동시간에 따른 부분별 온도 특성과 가스 챔버, 개질기 입구, 스팀 입구의 압력에 따른 데이터 출력 현황을 나타낸 것이다. 그림 15-(a) 중 최대값을 산출해 보면, 일사량 120.95kWh/㎡, 태양광어레이 전압 206Vdc, 전류 5.43A, 3151.9kWh, 인버터 출력전력 3078.1kWh을 나타내고 있으며 변환효율은 약 97%로 산출된다. 그림 15-(b)는 태양광발전시스템과 풍력발전시스템을 복합한 하이브리드 시스템으로 태양광발전시스템과 풍력발전시스템의 발전량을 Battery에 저장하여 DC부하를 구동시키도록 구성되어 있다. 최대 발전량을 분석하였을 때, 태양광발전시스템 825Wp, 풍력발전시스템은 816Wp가 산출되어 하이브리드로 발전량을 저장하고 있음을 알 수 있다. 그림 15-(c)는 연료전지 시스템의 개질 부분을 모니터링 데이터로서 초기 기동을 시작하여 버너 상단이 최대 900℃까지 상승한 이후 점차적으로 안정화 되고, 온도가 최대가 된 시점에서 챔버의 압력 또한 최대가 됨을 알 수 있다.

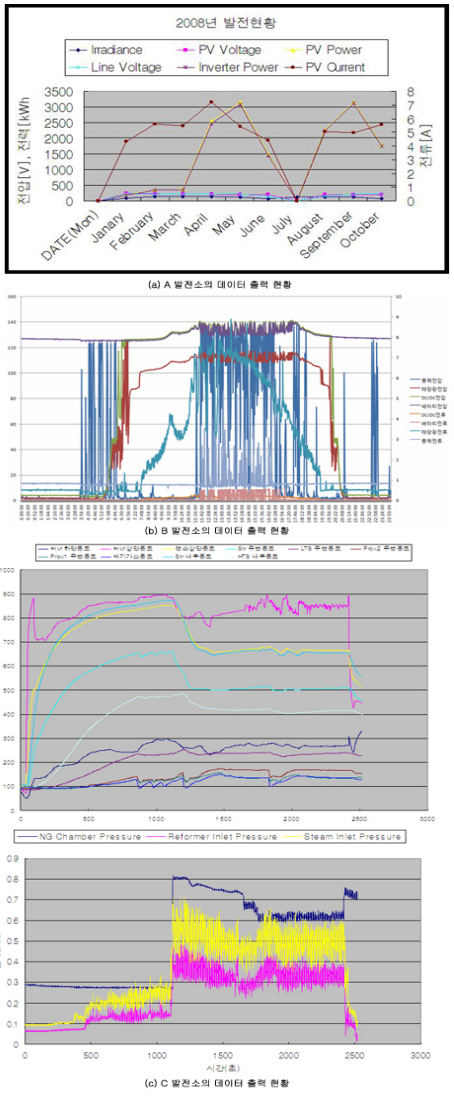

Fig. 15. Data Output File

그림 15. 데이터 출력 현황

III 결론

본 연구에서는 분산 배치된 A발전소 태양에너지 발전시스템, B 발전소 풍력/태양광 복합 발전시스템, C 연료전지 등의 신・재생에너지 발전설비들을 원격으로 계측하여 DB화 할 수 있도록 개발된 원격 데이터수집/관리 시스템에, 공개된 네트워크로부터 수집된 데이터의 공개, 변조, 파괴, 재난 등의 위협으로부터 보호하기 위해 보안시스템을 적용하였다. 또한 다양한 네트워크 보안 시스템을 하나로 통합하여 데이터의 기밀성, 무결성, 가용성을 확보하도록 통합 보안 시스템을 개발하고 이를 통합 집중 관리 시스템을 통해 실시간 모니터링이 가능하도록 구축하였다. 이로 인해 지역별로 분산된 신・재생에너지 발전설비를 중앙에서 그 발전현황을 모니터링하고 제어기능을 부여하여 중앙에서 동시에 효율적으로 관리 할 수 있도록 하였다.

아울러 여러 가지 파라미터를 이용하여 특정 기간이나 시간대 별로 축적된 데이터를 불러내어 필요한 정보를 활용할 수 있는 백업시스템을 개발하는 연구가 필요하겠으며, 본 시스템에서 취득된 각 발전설비별 운전현황 데이터는 지역별 자연환경에 적합한 신・재생에너지발전 형태를 도출하는데 이바지 할 것이라고 사료된다.

참고문헌

[1] 강용혁 외, “신・재생에너지 자원조사・종합관리시스템 구축사업”, 한국에너지기술연구소, 산업자원부연구보고서, 2004-N-NC02-P-01

[2] 윤동식, 구기준, 전은희 편저, “정보 보호 입문을 위한 인터넷 정보 보안”

[3] Backup/Recovery Tutorial, Stroage Netwoking Industry Association, 2001

[4] M. Mesiner, G.R. Ganger, and E. Riedel, "Object-Based Storage," IEEE Communications Magazine, Aug. 2003, pp.84-90.

[5] 정국용, "네트워크 시스템의 통합 보안 방안에 대한 연구," 서울산업대학교 산업대학원, 2005

저 자 소 개

김 형 주 (정회원)

1999년 : 조선대학교 전산통계학과 졸업 (이학사)
2002년 : 원광대학교 대학원 컴퓨터 공학과 (공학석사)
2006년~현재 : 남부대학교 대학원 디지털경영정보과 (박사과정)

<주관심분야>
신·재생 에너지, 정보 보안, 백업, 멀티미디어 통신

임 중 열 (정회원)

2002년 : 동신대학교 전기전자공학과 박사 졸업
2003년 3월~현재 : 남부대학교 컴퓨터전기정보학과 조교수
<주관심분야> 전력변환, 신·재생 에너지, 멀티미디어 통신