채널 액세스 게이트웨이를 적용한 분산 네트워크 통신에서의 데이터 보안에 관한 연구

안은미, 송영기, 조용섭
한국원자력연구원 양성자기반공학기술개발사업단
e-mail:aem@kaeri.re.kr

A Study on Data Security in the Distributed Network Communication using Channel Access Gateway

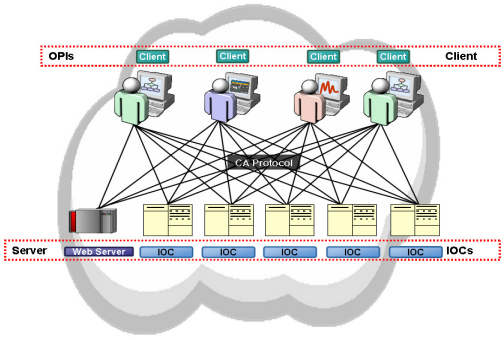
Eun-Mi An, Young-Gi Song, Yong-Sub Cho
Proton Engineering Frontier Project, Korea Atomic Energy Research Institute

요 약

양성자 기반 공학 기술 개발 사업단은 20MeV 양성자 가속기를 운전 중이며, 진공, 빔 계측, 전원 등의 장치에 대한 제어 시스템을 개발 운영 중이다. 대형 입자 가속기를 위한 제어 시스템의 전체 네트워크는 사용자 인터페이스와 제어계가 단일 네트워크를 공유하고 있으며 EPICS(Experimental Physics and Industrial Control System) CA(Channel Access)통신을 이용하여 데이터를 상호 교환한다. 그러나 단일 네트워크를 사용함으로서 관리자만이 제어해야 할 데이터는 많은 클라이언트에게 노출되는 문제점이 있다. 그러므로 클라이언트의 접근을 제어하여 제어계로부터 전달되는 신호들의 안정성과 보안성을 유지할 수 있는 방법이 요구된다. 본 논문에서는 제어시스템에 보안성과 안정성을 유지하기 위하여 클라이언트를 Control Network, 제어계를 Machine Network로 분산시키고 통신 중계기 역할을 하는 CA Gateway를 적용하여 클라이언트에게 접근 권한을 주는 기법을 제시하고 구현 및 그 결과를 보고한다.

1. 서론

한국 원자력 연구원 양성자 기반 공학 기술 개발 사업단(PEFP, Proton Engineering Frontier Project)에서는 2002년 7월부터 100MeV, 20mA 선형 양성자 가속장치 개발 프로젝트[1]를 수행중이며, 현재 20MeV 양성자 가속장치를 개발하여 진공, 빔 계측, 전원 등의 장치에 대한 제어시스템을 개발 운영 중이다.



(그림 1) 단일 네트워크상의 제어시스템 네트워크 구조

그림 1은 PEFP 제어 시스템의 네트워크 구조로서 클라이언트와 서버 측 제어계는 단일 네트워크상에서 CA (Channel Access)[2] 프로토콜을 통하여 데이터를 전송한다. 그러나 같은 네트워크망을 사용함으로서 관리자만이 제어해야 할 데이터들에 대한 보안성과 안정성을 보장할 수 없다. 가속기 제어 시스템에서 보안 및 안정성은 필수적으로 요구되며 앞으로 확장될 제어 시스템에 필수 요구사항이다. 이러한 요구를 만족시키기 위하여 첫째로 사용목적에 따라 네트워크를 분리시키고, 그 다음으로 CA Gateway[3]를 적용하여 보안의 요구사항과 지원 가능한 보안의 정도를 명시하는 방법을 제공하고자 한다.

이 논문의 구성은 다음과 같다. 2장에서는 가속기 제어 시스템 관련 연구를 살펴보고 3장에서는 CA Gateway를 적용한 전체 네트워크에 대한 설계를 논하고 4장에서는 구현 방법에 대해 설명하며 5장에서는 결론을 제시한다.

2. 관련연구

제어시스템 개발자들은 유지보수가 간편하며, 확장성/이식성이 뛰어난 이유로 주로 EPICS를 사용한다.

독일의 ISL-Berlin (Ion-Beam-Labor atory Berlin)[4]는 Linux 기반으로 Labview와 PVWave(Visual Numerics Inc.)를 이용하여 OPI 시스템을 개발사용 중이다.

SNS(Spallation Neutron Source)[5]는 FE(Front-End) 가속기를 제어시스템을 EPICS 의 Knob Manager, StripTool, Channel Archiver, Backup Restore Tool, Probe를 사용하여 상위 제어 시스템을 제공하고 있다.

3. 요구사항 및 설계

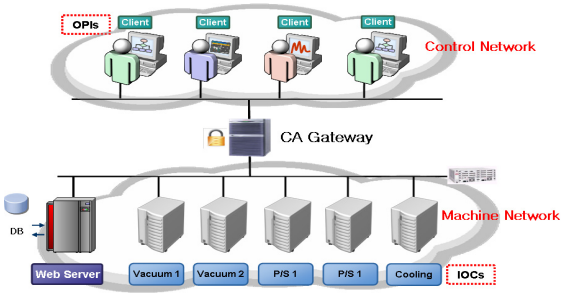
네트워크를 분산시키고 데이터 보안을 유지하기 위한 CA Gateway 서버는 저장 장치나 메모리의 요구사항은 낮은 반면 CPU의 계산 능력과 네트워크 처리 능력이 중요시 된다. 또한 데이터를 실시간으로 교환하는 Channel Access 관련 트래픽을 처리하고 다수의 이더넷 포트를 이용하여 트래픽을 분산하여 처리할 수 있어야 한다. 운영체제는 Linux를 기반으로 하며 EPICS의 CA gateway 프로세스를 실행할 소프트웨어의 요구사항은 다음과 같다.

- EPICS Base 3.14.9 ▸ GNU Regex 0.13
- Gateway 2.0.3.0 ▸ MEDM 3.1.3 ▸ StripTool 12.5.12

먼저 사용목적에 따라 네트워크를 분산한다. 제어계를 구성하는 IOC(Input Output Controller)들은 Machine Network로 구성하고 사용자 인터페이스를 위한 OPI (Operator Interface)는 Control Network로 분산 시킨다. 분산된 네트워크는 CA Gateway를 통해 통신이 이뤄지도록 한다. CA Gateway에서는 통신을 시도하는 클라이언트들의 권한을 설정하여 인증된 클라이언트만 Control Network에 접속할 수 있도록 한다.

4. CA Gateway 적용한 데이터 보안 구현

그림 2는 사용 목적에 따라 분산된 네트워크를 보여주고 있다. 제어계를 구성하는 Machine Network와 사용자 인터페이스를 위한 Control Network는 서로 분리된 이더넷이다. CA Gateway는 분리된 이더넷 사이에 CA 통신을 중계해 주는 역할을 수행한다.



(그림 2) 사용 목적에 따라 분산된 네트워크

또한 CA Gateway는 Control Network에서 Machine Network로 접근을 시도하는 사용자에 대한 권한을 설정한다. CA Gateway의 access파일의 설정을 통하여 제어계의 데이터에 대한 접근 제어를 수행한다. 즉, 인증된 사용자만이 통신을 허가하고 데이터를 접근할 수 있도록 한다. 그림 3은 CA Gateway에서 접근허가에 대한 권한설정의 일부이다.

```
EVALUATION ORDER ALLOW, DENY
#RFQ Gauge
HVME01:DEV1:CH1:.*  ALLOW
HVME01:DEV1:CH2:.*  ALLOW

#DTL Gauge 1
HVME02:DEV6:CH1:.*  ALLOW
HVME02:DEV6:CH2:.*  ALLOW
HVME02:DEV6:CH3:.*  ALLOW
HVME02:DEV6:CH4:.*  ALLOW

##special Security :DTL ION pump Controller##
HVME03:DEV4:CH1:.*  ALLOW Admin 1
HVME03:DEV4:CH2:.*  ALLOW Admin 1
HVME03:DEV4:CH3:.*   ALLOW PowerSupply 1
HVME03:DEV4:CH4:.*  ALLOW Gateway Admin 1

#block everything
!x12SA-1MPGW.*        DENY FROM 147.43.48.***
```

(그림 3) CA Gateway의 접근 및 데이터 권한 설정

Control Network에 권한이 가진 클라이언트가 Machine Network로 접근을 시도하면 CA Gateway를 통하여 접근하여 CA통신에서의 데이터의 보안을 유지한다.

5. 결과 및 향후 과제

본 논문에서는 사용 목적에 따라 네트워크를 분산시킨 후 서로 다른 네트워크간의 CA통신을 위해 CA Gateway를 적용시켰다. CA Gateway의 사용자 접근권한 및 데이터 접근권한으로 CA 통신상의 데이터 보안 요구사항을 만족시켰다. CA 통신에서의 데이터 보안은 교환되는 데이터에 접근 권한과 사용자 인증 기능을 제공함으로써 교환하는 데이터와 사용하는 서비스 모두에게 안전한 제어환경을 구축할 수 있었다.

본 논문에서는 CA Gateway를 적용하여 네트워크를 분산시키고 데이터의 보안성을 제공하였지만, 향후에는 CA Gateway를 원격에서도 제어할 수 있는 연구가 진행되어야 할 것이다.

사사(Acknowledgement)

본 연구는 교육과학부 지원을 받은 연구임

참고문헌

[1] B. H. Choi, "Proton Linear Accelerator Development and its Utilization Program in PEFP," APAC'04, pp. 231-233, Gyeongju, Korea, 2004

[2] J. O. Hill, "Channel Access: A Software Bus for the LAACS," ICALEPCS'89, pp. 352-355, Vancouver, British Columbia, 1989.

[3] CA Gateway http://www.aps.anl.gov/epics/extensions/gateway/index.html

[4] W. Busse, C. Rethfeldt, "A Seamless Control System Upgrade for a Continuously Running Accelerator Facility," PCaPAC'02, Frascati, 2002.

[5] S.A.Lewis, C. A. Lionberger, "Status of the Control System for the Front-End of the Spallation Neutron Source," ICALEPCS'01, pp. 119-121, San Jose, 2001