



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0116454
(43) 공개일자 2013년10월24일

(51) 국제특허분류(Int. Cl.)

G06F 21/30 (2013.01) G06F 21/10 (2013.01)

H04L 29/06 (2006.01)

(21) 출원번호 10-2012-0031328

(22) 출원일자 2012년03월27일

심사청구일자 2012년03월27일

(71) 출원인

계명대학교 산학협력단

대구광역시 달서구 달구벌대로 1095 (신당동)

(72) 발명자

주홍택

대구광역시 달서구 호산동 삼성한국형아파트 106동 304호

이준희

대구광역시 달서구 본동 월성주공5단지아파트 510동 811호

(74) 대리인

김건우

전체 청구항 수 : 총 19 항

(54) 발명의 명칭 뷰 기반의 아이이디 접근 제어 방법 및 시스템

(57) 요약

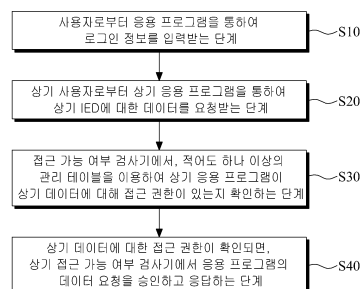
본 발명은 IED 접근 제어 방법 및 시스템에 관한 것으로서, 보다 구체적으로는, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 뷰 기반의 IED 접근 제어 방법은, 서버가, (1) 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계; (2) 상기 사용자로부터 상기 응용 프로그램을 통하여 상기 IED에 대한 데이터를 요청받는 단계; (3) 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 상기 응용 프로그램이 상기 데이터에 대해 접근 권한이 있는지 확인하는 단계; 및 (4) 상기 데이터에 대한 접근 권한이 확인되면, 상기 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 뷰 기반의 IED 접근 제어 방법 및 시스템에 따르면, 뷰 기반의 접근 제어 모델을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한함으로써, 모든 IED에 대하여 세밀하게 접근을 제어할 수 있다.

또한, 본 발명에 따르면, 각 응용 프로그램에 사용자가 로그인을 하면, 그 응용 프로그램을 통해서 IEC 61850 프로토콜로 동작하는 시스템 서버에 접근하도록 하고, 서버에 접근이 가능하면 각 응용 프로그램을 통해 제한된 데이터 객체 권한을 보여 주도록 함으로써, 사용자에게는 접근을 할 수 있는 객체만 보여주어 사용자들의 접근 권한을 가진 객체를 쉽게 알 수 있고, 접근권한을 벗어난 실수를 줄일 수 있으며, 뷰 기반의 접근 제어 모델로 응용 프로그램(HMI)에서 IED까지의 제어 및 모니터링이 보호될 수 있다.

뿐만 아니라, 본 발명에 따르면, IEC 61850 프로토콜에 기반을 둔 것으로서, IEC 61850 프로토콜의 데이터셋(Dataset)를 사용하여 응용 프로그램이 데이터에 접근 가능한지 여부를 확인하는 관리 테이블을 정의함으로써, 새로운 정보 모델을 만들 필요가 없다. 즉, IEC 61850 프로토콜은 명명 규칙을 통해서 각 데이터 객체에 대한 Dataset Class를 규정하고 있고, 명명 규칙에 의해서 각 객체별로 접근할 수 있는 서비스를 정의하고 있기 때문에 서비스 및 데이터 객체의 접근을 제어하기 위해서 Dataset를 활용할 수 있다.

대표도 - 도4



특허청구의 범위

청구항 1

IED(Intelligent Electronic Device) 접근 제어 방법으로서,

IEC 61850 프로토콜을 기반으로 하되,

뷰 기반의 접근 제어 모델(view based access control model)을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 2

제1항에 있어서, 상기 IED 접근 제어 방법은,

DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 3

제1항에 있어서, 상기 IED 접근 제어 방법은,

변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 4

IED 접근 제어 방법으로서, 서버가,

- (1) 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계;
- (2) 상기 사용자로부터 상기 응용 프로그램을 통하여 상기 IED에 대한 데이터를 요청받는 단계;
- (3) 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 상기 응용 프로그램이 상기 데이터에 대해 접근 권한이 있는지 확인하는 단계; 및
- (4) 상기 데이터에 대한 접근 권한이 확인되면, 상기 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계를 포함하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 5

제4항에 있어서, 상기 접근 가능 여부 검사기는,

VACM(View-based Access Control Model) 검사기인 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 6

제4항에 있어서, 상기 접근 제어 방법은,

IEC 61850 프로토콜에 기반을 둔 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 7

제6항에 있어서,

상기 응용 프로그램이 상기 데이터에 접근 가능한지 여부를 확인하는 데에 이용되는 상기 관리 테이블은, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 8

제4항에 있어서, 상기 관리 테이블은,

컨텍스트 테이블과 애플리케이션 테이블의 두 개로 구성되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 9

제8항 있어서, 상기 컨텍스트 테이블에는,

각각의 데이터에 대한 색인을 할당하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 10

제8항에 있어서, 상기 애플리케이션 테이블에는,

각각의 응용 프로그램이 접근할 수 있는 색인을 할당하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 11

제4항에 있어서, 상기 IED 접근 제어 방법은,

변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 12

제6항에 있어서, 상기 IED 접근 제어 방법은,

DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 13

IED 접근 제어 방법으로서, 서버가,

- (a) 각각의 데이터 객체에 대하여 색인을 할당하여 제1 관리 테이블(Context Table)을 정의하는 단계;
- (b) 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 제2 관리 테이블(Application Table)을 정의하는 단계;
- (c) 상기 응용 프로그램을 사용하여 서버에 로그인한 사용자로부터 데이터를 요청받는 단계;
- (d) VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기에서, 상기 제2 관리 테이블에,

상기 응용 프로그램이 상기 요청된 데이터 객체에 대해 접근 권한이 있는지 물어보는 쿼리를 보내는 단계;
 (e) 상기 제2 관리 테이블에 쿼리가 들어오면, 상기 응용 프로그램의 색인을 확인하는 단계;
 (f) 상기 제1 관리 테이블에서 상기 확인된 색인에 할당된 데이터 객체를 확인하는 단계; 및
 (g) 상기 제1 관리 테이블에서 상기 데이터 객체에 대한 접근 권한 유무를 확인하는 단계를 포함하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 14

제13항에 있어서,

(h) 상기 접근 가능 여부 검사기에서 상기 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계를 더 포함하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 15

제13항에 있어서,

상기 접근 제어 방법은, IEC 61850 프로토콜에 기반을 둔 것으로서,

상기 제1 관리 테이블 및 제2 관리 테이블은, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 16

제13항에 있어서, 상기 접근 제어 방법은,

변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 17

제15항에 있어서, 상기 IED 접근 제어 방법은,

DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 방법.

청구항 18

IED 접근 제어 시스템으로서,

응용 프로그램이 설치된 사용자 단말기; 및

상기 사용자 단말기로부터 정보를 입력받는 입력부, VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기, 데이터 저장부, 및 상기 사용자 단말기로 정보를 출력하는 출력부를 포함하는 서버를 포함하는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 시스템.

청구항 19

제18항에 있어서,

상기 IED 접근 제어 시스템은, IEC 61850 프로토콜을 기반으로 하고,

상기 VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기는, 각각의 데이터 객체에 대하여 색인을 할당하여 정의된 제1 관리 테이블(Context Table) 및 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 정의된 제2 관리 테이블(Application Table)이 저장되어 있으며, 상기 제1 관리 테이블 및 제2 관리 테이블을 이용하여 접근 가능 여부를 판단하도록 구현되는 것을 특징으로 하는, 뷰 기반의 IED 접근 제어 시스템.

명세서

기술분야

[0001] 본 발명은 IED 접근 제어 방법 및 시스템에 관한 것으로서, 보다 구체적으로는 뷰 기반의 IED 접근 제어 방법 및 시스템에 관한 것이다.

배경기술

[0002] 기존의 변전소와 IED(Intelligent Electronic Device) 간의 통신에서 중요한 점은 최적화 비용이었다. 통신에서 대역폭의 제한으로 변전소와 IED 또는 IED 간의 통신에서 얼마나 많은 양의 데이터를 최대한 빠르게 보내는가 하는 것이 최적화의 가장 큰 문제였다. 하지만 디지털 시대로 이동 후에는 더 이상 대역폭은 제한 요소가 되지 않았다. 대역폭의 제한이 사라지면서 통신에 대한 제한 요소가 사라져 변전소 자동화 및 상호운용성이 중요한 점이 되었다. 그리고 변전소의 자동화가 이루어지면서 변전소의 종합적인 정보를 실시간으로 쉽게 얻을 수 있게 되었다. 초기의 변전소 자동화에서 쓰이는 통신 프로토콜은 DNP(Distributed Network Protocol), MODBUS 등이었다. DNP와 MODBUS는 변전소의 SCADA(Supervisory Control and Data Acquisition) 시스템에서 사용되는 통신 프로토콜로서, RTU(Remote Terminal Unit)와 IED 간의 통신 또는 IED와 센서 및 계측 장치 사이의 통신을 지원한다. 이와 같은 프로토콜들은 초기 RS232 또는 RS-485 등과 같은 시리얼 방식으로 연결되었으며 현재는 이더넷을 통해 통신이 가능하도록 구현하지만, 주로 변전소 내부의 통신을 목적으로 만들어졌다. 이와 같은 기존의 여러 프로토콜을 하나의 표준 프로토콜로 통합하도록 만든 것이 IEC 61850 프로토콜이다.

[0003] IEC 61850 프로토콜은, 이더넷 환경에 맞게 다양한 기능을 제공하며, 기존의 변전소 및 변전소 장치들의 호환성을 높여준다. 그리고 변전소 내부뿐만 아니라 외부에서의 원격 통신에 대해서도 지원한다. 원격 통신으로 외부에서 변전소 내부 및 RTU, IED 등과 같은 장치들을 제어하는 것은 운용 관점에서 큰 이익을 가져온다. 높은 가용성, 낮은 유지보수 비용 등이 그러한 것이다. 하지만 외부에서 변전소 내부의 시스템 및 장치들에 접근 및 제어가 가능하기 때문에 보안에 대한 중요성이 더욱 커졌다. 만약 악의적인 목적으로 외부에서 변전소 내부의 시스템 및 변전소 장치들에 접근이 이루어진다면, 변전소 또는 변전소 장치만의 문제가 아니라 국가 전력망의 위험을 초래할 수 있다. 따라서 변전소 시스템 및 장치들에 대한 접근 제어가 중요한 보안 개념 중 하나라 할 수 있다.

[0004] 한편, 접근 권한에 있어서, 컴퓨터의 경우 사용자는 컴퓨터에 로그인을 하고서 컴퓨터 내부의 파일 및 프로그램의 실행 권한을 얻는다. 이것은 일반적인 컴퓨터 환경에서 사용되는 잘 알려진 접근 제어 방법이다. 그러나 변전소 시스템 및 장치들의 접근 제어는 컴퓨터보다 더 복잡하고 어려운 문제이다. 변전소 시스템 및 장치들의 운용에는 많은 다수 사업자의 장치, 다양한 기능, 다양한 기술 및 많은 기술자가 관련되어 있기 때문이다. 이와 같은 점들이 특정 IED의 운용 또는 접근에 대한 권한을 누가 가지는지 결정하는 것을 어렵게 한다.

[0005] 전통적인 변전소 시스템 및 장치들의 접근 제어에는, 로그인 기반 방식이 사용되었다. 로그인 기반 방식은, 사용자가 로그인만 하면 그 시스템 또는 프로그램의 권한을 획득하는 것으로서, 사용자 ID에 권한을 주기 때문에 정확한 권한을 알지 못하거나, 자신의 권한을 넘어선 관리자 권한까지도 가질 수 있어, 보안에 상당히 취약하다. 즉, 사용자 또는 사용자 그룹에 광범위한 접근 권한 또는 관리자 권한이 주어지므로, 사용자는 필요한 접근 및 제어 범위를 벗어나서 불필요한 시스템 또는 프로그램에 접근 및 제어를 할 수 있다. 따라서 로그인 기반 접근 제어 방법보다 향상된 접근 제어 방법이 필요하다.

발명의 내용

해결하려는 과제

- [0006] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 뷰 기반의 접근 제어 모델을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한함으로써, 모든 IED에 대하여 세밀하게 접근을 제어할 수 있는, 뷰 기반의 IED 접근 제어 방법 및 시스템을 제공하는 것을 그 목적으로 한다.
- [0007] 또한, 본 발명은, 각 응용 프로그램에 사용자가 로그인을 하면, 그 응용 프로그램을 통해서 IEC 61850 프로토콜로 동작하는 시스템 서버에 접근하도록 하고, 서버에 접근이 가능하면 각 응용 프로그램을 통해 제한된 데이터 객체 권한을 보여 주도록 함으로써, 사용자에게는 접근을 할 수 있는 객체만 보여주어 사용자들의 접근 권한을 가진 객체를 쉽게 알 수 있고, 접근권한을 벗어난 실수를 줄일 수 있으며, 뷰 기반의 접근 제어 모델로 응용 프로그램(HMI)에서 IED까지의 제어 및 모니터링이 보호될 수 있는, 뷰 기반의 IED 접근 제어 방법 및 시스템을 제공하는 것을 다른 목적으로 한다.
- [0008] 뿐만 아니라, 본 발명은, IEC 61850 프로토콜에 기반을 둔 것으로서, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 응용 프로그램이 데이터에 접근 가능한지 여부를 확인하는 관리 테이블을 정의함으로써, 새로운 정보 모델을 만들 필요가 없는, 뷰 기반의 IED 접근 제어 방법 및 시스템을 제공하는 것을 또 다른 목적으로 한다.

과제의 해결 수단

- [0009] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 뷰 기반의 IED 접근 제어 방법은,
- [0010] IEC 61850 프로토콜을 기반으로 하되,
- [0011] 뷰 기반의 접근 제어 모델(view based access control model)을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 그 구성상의 특징으로 한다.
- [0012] 바람직하게는, 상기 IED 접근 제어 방법은,
- [0013] DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환될 수 있다.
- [0014] 바람직하게는, 상기 IED 접근 제어 방법은,
- [0015] 변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용될 수 있다.
- [0016] 또한, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 뷰 기반의 IED 접근 제어 방법은, 서버가,
- [0017] (1) 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계;
- [0018] (2) 상기 사용자로부터 상기 응용 프로그램을 통하여 상기 IED에 대한 데이터를 요청받는 단계;
- [0019] (3) 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 상기 응용 프로그램이 상기 데이터에 대해 접근 권한이 있는지 확인하는 단계; 및
- [0020] (4) 상기 데이터에 대한 접근 권한이 확인되면, 상기 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.
- [0021] 바람직하게는, 상기 접근 가능 여부 검사기는,
- [0022] VACM(View-based Access Control Model) 검사기일 수 있다.

- [0023] 바람직하게는, 상기 접근 제어 방법은,
- [0024] IEC 61850 프로토콜에 기반을 둔 것일 수 있다.
- [0025] 더욱 바람직하게는,
- [0026] 상기 응용 프로그램이 상기 데이터에 접근 가능한지 여부를 확인하는 데에 이용되는 상기 관리 테이블은,
- [0027] IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의되는 것일 수 있다.
- [0028] 바람직하게는, 상기 관리 테이블은,
- [0029] 컨텍스트 테이블과 애플리케이션 테이블의 두 개로 구성될 수 있다.
- [0030] 더욱 바람직하게는, 상기 컨텍스트 테이블에는,
- [0031] 각각의 데이터에 대한 색인을 할당할 수 있다.
- [0032] 더욱 바람직하게는, 상기 애플리케이션 테이블에는,
- [0033] 각각의 응용 프로그램이 접근할 수 있는 색인을 할당할 수 있다.
- [0034] 바람직하게는, 상기 IED 접근 제어 방법은,
- [0035] 변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용될 수 있다.
- [0036] 더욱 바람직하게는, 상기 IED 접근 제어 방법은,
- [0037] DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환될 수 있다.
- [0038] 뿐만 아니라, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 뷰 기반의 IED 접근 제어 방법은, 서버가,
- [0039] (a) 각각의 데이터 객체에 대하여 색인을 할당하여 제1 관리 테이블(Context Table)을 정의하는 단계;
- [0040] (b) 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 제2 관리 테이블(Application Table)을 정의하는 단계;
- [0041] (c) 상기 응용 프로그램을 사용하여 서버에 로그인한 사용자로부터 데이터를 요청받는 단계;
- [0042] (d) VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기에서, 상기 제2 관리 테이블에, 상기 응용 프로그램이 상기 요청된 데이터 객체에 대해 접근 권한이 있는지 물어보는 쿼리를 보내는 단계;
- [0043] (e) 상기 제2 관리 테이블에 쿼리가 들어오면, 상기 응용 프로그램의 색인을 확인하는 단계;
- [0044] (f) 상기 제1 관리 테이블에서 상기 확인된 색인에 할당된 데이터 객체를 확인하는 단계; 및
- [0045] (g) 상기 제1 관리 테이블에서 상기 데이터 객체에 대한 접근 권한 유무를 확인하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.
- [0046] 바람직하게는,
- [0047] (h) 상기 접근 가능 여부 검사기에서 상기 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계를 더 포함할 수 있다.

- [0048] 바람직하게는,
- [0049] 상기 접근 제어 방법은, IEC 61850 프로토콜에 기반을 둔 것으로서,
- [0050] 상기 제1 관리 테이블 및 제2 관리 테이블은, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의될 수 있다.
- [0051] 바람직하게는, 상기 접근 제어 방법은,
- [0052] 변전소와 IED(Intelligent Electronic Device) 간의 통신, 또는 IED와 다른 IED 간의 통신에 사용될 수 있다.
- [0053] 더욱 바람직하게는, 상기 IED 접근 제어 방법은,
- [0054] DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환될 수 있다.
- [0055] 한편, 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 뷰 기반의 IED 접근 제어 시스템은,
- [0056] 응용 프로그램이 설치된 사용자 단말기; 및
- [0057] 상기 사용자 단말기로부터 정보를 입력받는 입력부, VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기, 데이터 저장부, 및 상기 사용자 단말기로 정보를 출력하는 출력부를 포함하는 서버를 포함하는 것을 그 구성상의 특징으로 한다.
- [0058] 바람직하게는,
- [0059] 상기 IED 접근 제어 시스템은, IEC 61850 프로토콜을 기반으로 하고,
- [0060] 상기 VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기는, 각각의 데이터 객체에 대하여 색인을 할당하여 정의된 제1 관리 테이블(Context Table) 및 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 정의된 제2 관리 테이블(Application Table)이 저장되어 있으며, 상기 제1 관리 테이블 및 제2 관리 테이블을 이용하여 접근 가능 여부를 판단하도록 구현될 수 있다.

발명의 효과

- [0061] 본 발명에서 제안하고 있는 뷰 기반의 IED 접근 제어 방법 및 시스템에 따르면, 뷰 기반의 접근 제어 모델을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한함으로써, 모든 IED에 대하여 세밀하게 접근을 제어할 수 있다.
- [0062] 또한, 본 발명에 따르면, 각 응용 프로그램에 사용자가 로그인을 하면, 그 응용 프로그램을 통해서 IEC 61850 프로토콜로 동작하는 시스템 서버에 접근하도록 하고, 서버에 접근이 가능하면 각 응용 프로그램을 통해 제한된 데이터 객체 권한을 보여 주도록 함으로써, 사용자에게는 접근을 할 수 있는 객체만 보여주어 사용자들의 접근 권한을 가진 객체를 쉽게 알 수 있고, 접근권한을 벗어난 실수를 줄일 수 있으며, 뷰 기반의 접근 제어 모델을 응용 프로그램(HMI)에서 IED까지의 제어 및 모니터링이 보호될 수 있다.
- [0063] 뿐만 아니라, 본 발명에 따르면, IEC 61850 프로토콜에 기반을 둔 것으로서, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 응용 프로그램이 데이터에 접근 가능한지 여부를 확인하는 관리 테이블을 정의함으로써, 새로운 정보 모델을 만들 필요가 없다. 즉, IEC 61850 프로토콜은 명명 규칙을 통해서 각 데이터 객체에 대한 Dataset Class를 규정하고 있고, 명명 규칙에 의해서 각 객체별로 접근할 수 있는 서비스를 정의하고 있기 때문에 서비스 및 데이터 객체의 접근을 제어하기 위해서 Dataset를 활용할 수 있다.

도면의 간단한 설명

- [0064] 도 1은 일반적인 변전소와 IED 간의 운용 모델을 도식화한 도면.
- 도 2는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 도시한 도면.
- 도 3은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, IEC 61850 응용 프로그램을 통해서 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 도시한 도면.
- 도 4는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법의 흐름을 도시한 도면.
- 도 5는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, 관리 테이블을 도시한 도면.
- 도 6은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법의 흐름을 도시한 도면.
- 도 7은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법을 도식화한 도면.
- 도 8은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 시스템을 도시한 도면.

발명을 실시하기 위한 구체적인 내용

- [0065] 이하에서는 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있도록 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시예를 상세하게 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다. 또한, 유사한 기능 및 작용을 하는 부분에 대해서는 도면 전체에 걸쳐 동일 또는 유사한 부호를 사용한다.
- [0066] 덧붙여, 명세서 전체에서, 어떤 부분이 다른 부분과 ‘연결’되어 있다고 할 때, 이는 ‘직접적으로 연결’되어 있는 경우뿐만 아니라, 그 중간에 다른 소자를 사이에 두고 ‘간접적으로 연결’되어 있는 경우도 포함한다. 또한, 어떤 구성요소를 ‘포함’ 한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다.
- [0067] 본 발명의 일 측면은, IEC 61850 프로토콜을 기반으로 하되, 뷰 기반의 접근 제어 모델(view based access control model)을 적용하여 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는, 뷰 기반의 IED(Intelligent Electronic Device) 접근 제어 방법을 제공한다.
- [0068] 기존의 변전소와 IED 간의 통신 프로토콜은 DNP, MODBUS 등이었다. DNP와 MODBUS는 자동화 시스템(감시제어시스템)의 통신 프로토콜로 변전소 내부의 통신만을 위해 사용되어 라우팅이 필요 없고, 점 대 점 방식의 통신이 일방적으로 쓰였다. 그리고 일반적으로 OSI 7 계층 중 물리, 데이터 링크, 응용 계층을 사용한다. 하지만 시간이 지나면서 IED를 지원하는 여러 프로토콜이 만들어졌고 멀티 벤더에 의해 만들어진 IED 때문에 상호 운용성이 낮아졌을 뿐만 아니라, 통신 프로토콜에 대하여 IED 간의 고속 통신, 높은 가용성, 멀티 벤더 상호 운용성, 파일 변환에 대한 지원, 환경 설정에 대한 지원 등의 다양한 요구사항이 나타났다.
- [0069] IEC 61850 프로토콜은, 이와 같은 요구로 인하여 개발된 것으로서, 멀티 벤더 간의 상호 운용성을 지원하고, IED의 역할(기능)의 정의나 설정 등을 운용자가 편리하게 설정할 수 있게 지원한다. 표준화된 IEC 61850 프로토콜은 변전소 및 IED의 지원에 사용될 수 있는데, 원격으로 변전소 내부에 접근할 수 있다는 장점이 있다. 원격으로 변전소 외부에서 내부로 접근이 가능해져 변전소 내부의 상황을 실시간으로 감시할 수 있고, 종합적인 데이터를 획득할 수 있으며, 유지 보수의 비용이 낮아진다. 그러나 외부에서의 접근이 가능해져, 보안의 위험은 더욱 커지게 된다.

- [0070] 도 1은 일반적인 변전소와 IED 간의 운용 모델을 도식화한 도면이다. 도 1에 도시된 바와 같이, 현재 변전소, IED 간의 통신은 server-client 통신과 같다. 변전소에서 IED에 정보를 요청하면 IED는 정보를 전송하고, 변전소에서 IED에 동작을 요구하면 IED는 그 동작을 실행한다. 구체적으로, 사용자가 시스템 서버에 접근을 해서 로그인을 하고, 로그인이 성공하면 HMI(Human Machine Interface) 프로그램을 실행하여 접근하고자 하는 IED에 접근을 하며, IED에 필요한 정보를 요청하거나 동작을 실행한다. 그러나 이러한 구조는 IED의 접근에서 전부 아니면 전무의 접근 권한을 사용자에게 제공한다. 결국 인증 받은 사용자는, IEC 61850 객체, 즉, IED에 대한 모든 접근 권한을 가지게 되는데, 사용자에게 모든 접근 권한을 주는 것은, 보안상 매우 위험하다는 문제가 있다.
- [0071] 따라서 본 발명자들은, 뷰 기반의 접근 제어 모델(view based access control model)을 적용하여, 접근 권한을 제한하는 방법을 개발하였다.
- [0072] 뷰 기반의 접근 제어 방법은, SNMPv3에 주로 쓰이는 방법이다. SNMPv3의 목적 중 하나는 SNMP를 이용한 통신망의 보안 기능을 높이는 것으로서 보완된 데이터 출처 인증, 데이터의 암호화, 데이터 스트림 변경 방지, MIB에 대한 접근 제한 등의 기능이 추가되었으며, 이 중에서 MIB에 대한 접근 제한 기능이 뷰 기반 접근 제어 모델에 의해 제공될 수 있다. 뷰 기반 접근 제어 모델은 사용자 이름과 보안 모델로 구성되는 그룹, 컨텍스트 이름, 보안 모델, 보안 수준, 뷰 모드(view, write, notify)의 입력으로, 사용자가 접근하려고 하는 데이터에 대한 접근을 제어하는 기능을 수행한다. 앞에서 입력들을 구분하기 위해서 각각의 관리 테이블을 두고 이를 이용하여 각 입력에 대해 세밀하게 접근 제어 기능을 수행할 수 있다.
- [0073] 도 2는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 도시한 도면이다. 도 2에 도시된 바와 같이, 사용자 m과 n은 각각 접근할 수 있는 객체들이 제한되어 있다. 사용자 m은 객체 a, b, c, x, y, z에 접근할 수 있고, 사용자 n은 s, t, u, x, y, z에 접근할 수 있다. 사용자들에게는 각각 접근할 수 있는 객체만 보여줌으로써, 사용자들이 접근 권한을 가진 객체를 쉽게 알 수 있고, 접근 권한을 벗어나 접근하는 실수를 줄일 수 있다.
- [0074] 도 3은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, IEC 61850 응용 프로그램을 통해서 사용자별로 접근할 수 있는 데이터 접근 범위를 각각 제한하는 것을 도시한 도면이다. 즉, 도 3은 도 2를 IEC 61850 프로토콜에 적용한 것이다. 도 3에 도시된 바와 같이, IEC 61850 응용 프로그램을 통해서 각 데이터 객체의 접근 범위를 제한할 수 있다. 구체적으로, 각 응용 프로그램에 사용자가 로그인을 하면 그 응용 프로그램을 통해서 IEC 61850 프로토콜로 동작하는 시스템 서버에 접근을 할 수 있고, 서버에 접근이 가능하면 각 응용 프로그램은 제한된 데이터 객체 권한을 볼 수 있다. 도 3에서, 응용 프로그램 X는 논리적인 장치에 접근이 가능함을 보여주고, 응용 프로그램 Y는 논리적인 노드 XCBR에 속한 각각의 데이터 객체에 접근이 가능함을 보여준다.
- [0075] 한편, 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, IEC 61850 프로토콜을 기반으로 하는데, DNP(Distribute Network Protocol) 및 MODBUS 프로토콜을 포함하는 통신 프로토콜과 호환될 수 있어, 기존의 변전소 및 변전소 장치들의 호환성을 높일 수 있다. 또한, 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, 변전소와 IED 간의 통신이나, IED와 다른 IED 간의 통신에 사용될 수 있다. 변전소는 특히 보안이 중요한 것으로서, 보안 미비로 인해 심각한 정전 사고, 사건 등이 발생할 수 있고, 이는 국가적인 위험을 초래할 수도 있는바, 본 발명을 이용하여, 세밀한 접근 제어 및 보안을 기대할 수 있다.
- [0076] 도 4는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법의 흐름을 도시한 도면이다. 도 4에 도시된 바와 같이, 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, 서버가, 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계(S10), 사용자로부터 응용 프로그램을 통하여 IED에 대한 데이터를 요청받는 단계(S20), 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 응용 프로그램이 데이터에 대해 접근 권한이 있는지 확인하는 단계(S30), 데이터에 대한 접근 권한이 확인되면, 접근 가능 여부 검

사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계(S40)를 포함할 수 있다.

- [0077] 단계 S10은, 서버가 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계로서, 서버가 데이터 등을 요청하는 사용자를 식별하기 위한 단계이다. 또한, 단계 S20은, 서버가 사용자로부터 응용 프로그램을 통하여 IED에 대한 데이터를 요청받는 단계로서, 이후 단계에 의해 데이터 접근 권한이 확인되면, 사용자는 요청한 데이터에 접근할 수 있다.
- [0078] 단계 S30은, 서버가 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 응용 프로그램이 데이터에 대해 접근 권한이 있는지 확인하는 단계이다. 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, IEC 61850 프로토콜에 기반을 둔 것일 수 있고, 접근 가능 여부 검사기는 VACM(View-based Access Control Model) 검사기일 수 있다.
- [0079] 또한, 실시예에 따라서는, 응용 프로그램이 데이터에 접근 가능한지 여부를 확인하는 데에 이용되는 관리 테이블은, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의될 수 있다. 즉, IEC 61850 프로토콜에서는 명명 규칙을 통해서 각 데이터 객체에 대해서 Dataset Class를 규정하고 있기 때문에 새로운 정보 모델을 만들 필요 없이, 이 Dataset Class를 사용하여 관리 테이블을 정의할 수 있다. IEC 61850 프로토콜에서 Dataset Class는 데이터, 데이터 속성 등이 있는 Class 모델인데, 명명 규칙에 의해서 각 객체별로 접근할 수 있는 서비스를 정의하고 있다. 따라서 서비스 및 데이터 객체의 접근을 제어하기 위해서 IEC 61850 프로토콜의 Dataset을 사용할 수 있다. 다만, 이 Dataset에 어떤 정보가 들어있는지에 대한 인스턴스화할 수 있는 테이블의 정의가 필요하다.
- [0080] 도 5는 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, 관리 테이블을 도시한 도면이다. 도 5에 도시된 바와 같이, 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법에서, 관리 테이블은, 컨텍스트 테이블(Context Table, CTXTBL)과 애플리케이션 테이블(Application Table, APPTBL)의 두 개로 구성될 수 있다. 컨텍스트 테이블에는, 각각의 데이터에 대한 색인을 할당될 수 있으며, 애플리케이션 테이블에는, 각각의 응용 프로그램이 접근할 수 있는 색인이 할당될 수 있다. 예를 들어, 응용 프로그램 X가 IEC 61850 서버에 접근을 해서 IED에 대한 정보를 요청할 때, IED에서 응용 프로그램 X에 할당된 색인을 확인해서 그 색인에 맞는 데이터만 접근이 가능하도록 구현할 수 있다. 이렇게 Dataset Class를 활용하면 기존의 IEC 61850 시스템을 변경할 필요 없이 두 개의 테이블만 추가하여 각 데이터에 대한 접근 제한을 구현할 수 있다.
- [0081] 단계 S40은, 서버가 데이터에 대한 접근 권한이 확인되면, 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계로서, 사용자가 접근 권한을 확인받고, 데이터에 접근할 수 있게 된다.
- [0082] 도 6은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법의 흐름을 도시한 도면이다. 도 6에 도시된 바와 같이, 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, 서버가, 각각의 데이터 객체에 대하여 색인을 할당하여 제1 관리 테이블(Context Table)을 정의하는 단계(S100), 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 제2 관리 테이블(Application Table)을 정의하는 단계(S200), 응용 프로그램을 사용하여 서버에 로그인한 사용자로부터 데이터를 요청받는 단계(S300), VACM(View-based Access Control Mode 1)을 이용한 접근 가능 여부 검사기에서, 제2 관리 테이블에, 응용 프로그램이 요청된 데이터 객체에 대해 접근 권한이 있는지 물어보는 쿼리를 보내는 단계(S400), 제2 관리 테이블에 쿼리가 들어오면, 응용 프로그램의 색인을 확인하는 단계(S500), 제1 관리 테이블에서 확인된 색인에 할당된 데이터 객체를 확인하는 단계(S600), 제1 관리 테이블에서 데이터 객체에 대한 접근 권한 유무를 확인하는 단계(S700)를 포함할 수 있다. 또한, 실시예에 따라서는, 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계(S800)를 더 포함할 수 있다.

- [0083] 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법은, IEC 61850 프로토콜에 기반을 둔 것으로서, 제1 관리 테이블 및 제2 관리 테이블은, IEC 61850 프로토콜의 데이터세트(Dataset)를 사용하여 정의될 수 있다.
- [0084] 단계 S100은, 서버가, 각각의 데이터 객체에 대하여 색인을 할당하여 제1 관리 테이블(Context Table)을 정의하는 단계이고, 단계 S200은, 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 제2 관리 테이블(Application Table)을 정의하는 단계이다. 컨텍스트 테이블과 애플리케이션 테이블에 대해서는 도 5와 관련하여 설명하였으므로 상세한 설명은 생략하기로 한다.
- [0085] 단계 S300 내지 단계 S700에 대하여 살펴보면, 서버가, 응용 프로그램을 사용하여 서버에 로그인한 사용자로부터 데이터를 요청받으면(S300), VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기에서 제2 관리 테이블에 응용 프로그램이 요청된 데이터 객체에 대해 접근 권한이 있는지 물어보는 쿼리를 보낼 수 있고(S400), 제2 관리 테이블에 쿼리가 들어오면, 응용 프로그램의 색인을 확인할 수 있으며(S500), 제1 관리 테이블에서 확인된 색인에 할당된 데이터 객체를 확인(S600)한 후에, 제1 관리 테이블에서 데이터 객체에 대한 접근 권한 유무를 확인(S700)할 수 있다. 즉, 접근 제어 시스템의 운용상 접근이 일어날 때마다, 접근이 올바른지 검사하기 위하여, VACM 검사기를 사용할 수 있다. 즉, 각 접근에 대해서 APPTBL에 쿼리를 보내서 접근이 합당한지 검사한 후에 각 데이터에 대해서 접근을 허락할 수 있다. 접근이 허락되면 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답(S800)할 수 있다.
- [0086] 도 7은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 방법을 도식화한 도면이다. 도 7에 도시된 바와 같이, 사용자가 응용 프로그램 X를 사용해서 서버에 로그인을 한 후, D01 이라는 데이터를 요청하면, 데이터 요청을 받은 서버가 VACM 검사기에서 APPTBL에 응용 프로그램 X가 D01에 대해 접근 권한이 있는지 물어보는 쿼리를 보내고, APPTBL에 쿼리가 들어오면 응용 프로그램 X의 색인을 확인한 후에 CTXTBL에서 그 색인에 할당된 데이터를 확인할 수 있다. CTXTBL에서 데이터에 대한 접근 권한이 확인되면, VACM 검사기에서 응용 프로그램 X의 데이터 D01 요청을 승인하고 응답할 수 있다.
- [0087] 본 발명의 다른 측면은, 뷰 기반의 IED 접근 제어 시스템을 제공한다. 도 8은 본 발명의 일실시예에 따른 뷰 기반의 IED 접근 제어 시스템을 도시한 도면이다. 도 8에 도시된 바와 같이, 본 발명의 일실시예에 따른 뷰 기반 IED 접근 제어 시스템은, 응용 프로그램이 설치된 사용자 단말기(100) 및 사용자 단말기(100)로부터 정보를 입력받는 입력부(210), VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기(220), 데이터 저장부(230), 및 사용자 단말기(100)로 정보를 출력하는 출력부(240)를 포함하는 서버(200)를 포함할 수 있다. 사용자 단말기(100)는 응용 프로그램이 설치되고, 로그인 정보 등을 입력하는 수단일 수 있고, 서버는, 본 발명의 일련의 접근 제어 및 데이터 관리 기능을 수행할 수 있다. 구체적으로, 서버(200)는, 입력부(210)를 통해 사용자 단말기(100)로부터 정보를 입력받을 수 있고, 접근 가능 여부 검사기(220)에서는, VACM(View-based Access Control Model)을 이용하여, 사용자의 접근 권한을 확인할 수 있다. 접근 권한이 확인되면, 데이터 저장부(230)에 저장된 정보 등을 출력부(240)를 통해서 사용자 단말기(100)로 출력할 수 있다. 바람직하게는, IED 접근 제어 시스템은, IEC 61850 프로토콜을 기반으로 하고, VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기는, 각각의 데이터 객체에 대하여 색인을 할당하여 정의된 제1 관리 테이블(Context Table) 및 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 정의된 제2 관리 테이블(Application Table)이 저장되어 있으며, 제1 관리 테이블 및 제2 관리 테이블을 이용하여 접근 가능 여부를 판단하도록 구현될 수 있다.
- [0088] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

부호의 설명

- [0089] 100: 사용자 단말기 200: 서버

210: 입력부

220: 접근 가능 여부 검사기

230: 데이터 저장부

240: 출력부

S10: 사용자로부터 응용 프로그램을 통하여 로그인 정보를 입력받는 단계

S20: 상기 사용자로부터 상기 응용 프로그램을 통하여 상기 IED에 대한 데이터를 요청받는 단계

S30: 접근 가능 여부 검사기에서, 적어도 하나 이상의 관리 테이블을 이용하여 상기 응용 프로그램이 상기 데이터에 대해 접근 권한이 있는지 확인하는 단계

S40: 상기 데이터에 대한 접근 권한이 확인되면, 상기 접근 가능 여부 검사기에서 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계

S100: 각각의 데이터 객체에 대하여 색인을 할당하여 제1 관리 테이블(Context Table)을 정의하는 단계

S200: 각각의 응용 프로그램에 대하여 접근할 수 있는 색인을 할당하여 제2 관리 테이블(Application Table)을 정의하는 단계

S300: 상기 응용 프로그램을 사용하여 서버에 로그인한 사용자로부터 데이터를 요청받는 단계

S400: VACM(View-based Access Control Model)을 이용한 접근 가능 여부 검사기에서, 상기 제2 관리 테이블에, 상기 응용 프로그램이 상기 요청된 데이터 객체에 대해 접근 권한이 있는지 물어보는 쿼리를 보내는 단계

S500: 상기 제2 관리 테이블에 쿼리가 들어오면, 상기 응용 프로그램의 색인을 확인하는 단계

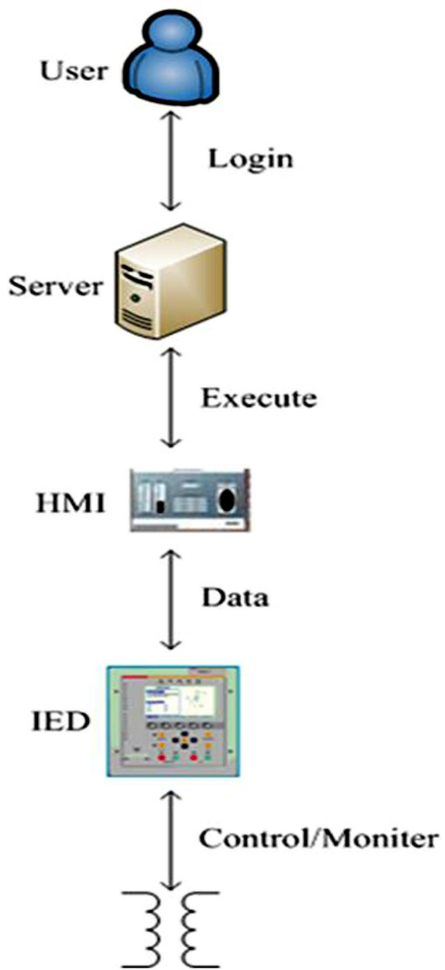
S600: 상기 제1 관리 테이블에서 상기 확인된 색인에 할당된 데이터 객체를 확인하는 단계; 및

S700: 상기 제1 관리 테이블에서 상기 데이터 객체에 대한 접근 권한 유무를 확인하는 단계

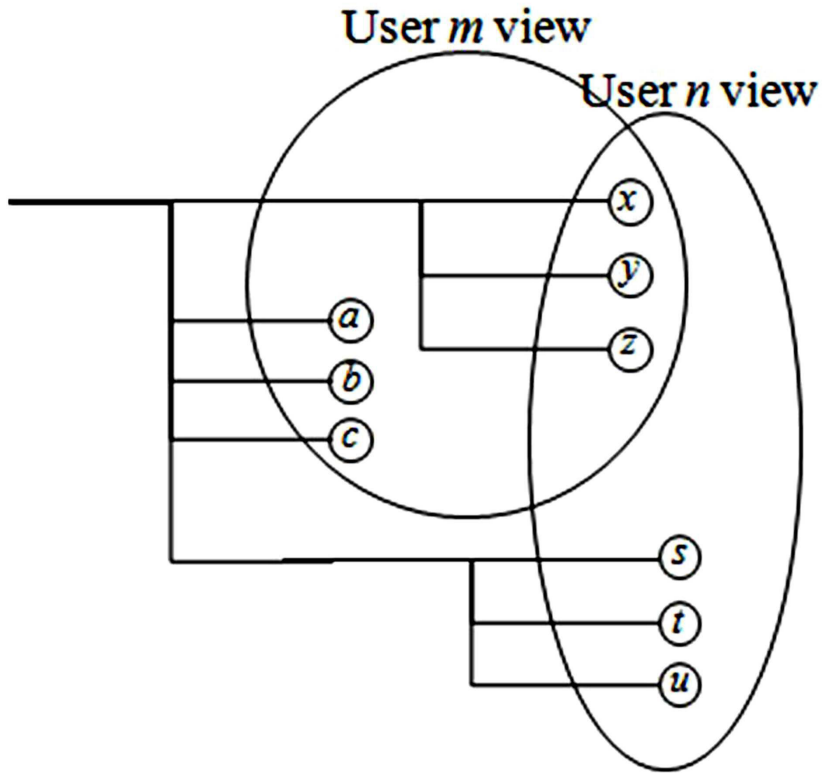
S800: 상기 접근 가능 여부 검사기에서 상기 응용 프로그램의 데이터 요청을 승인하고 응답하는 단계

도면

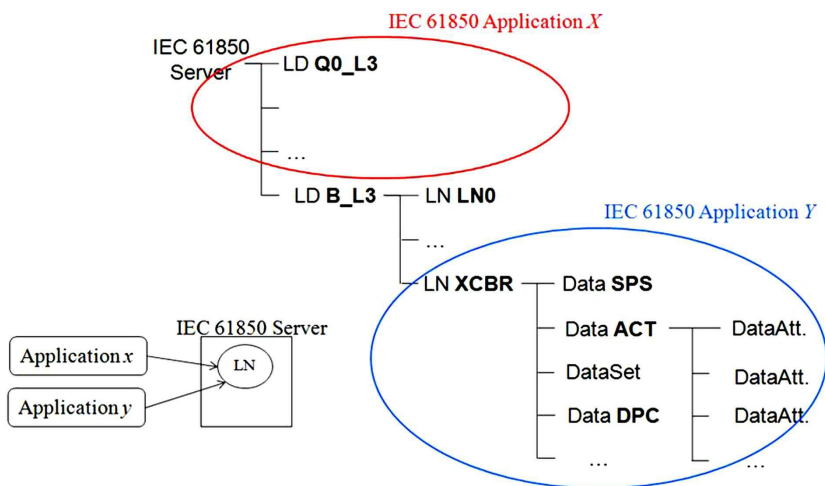
도면1



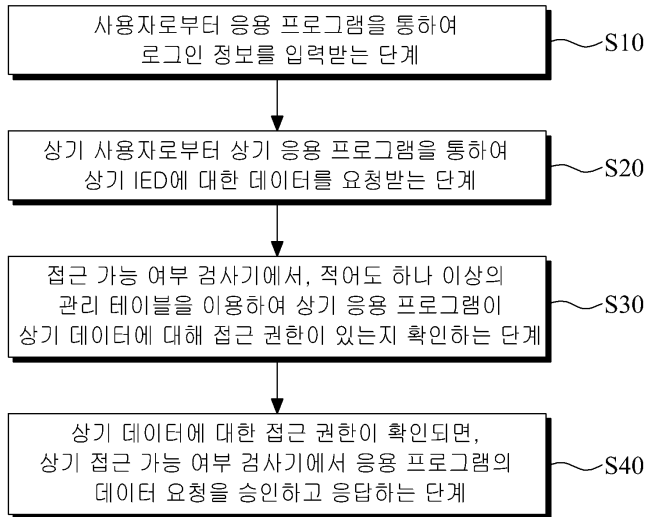
도면2



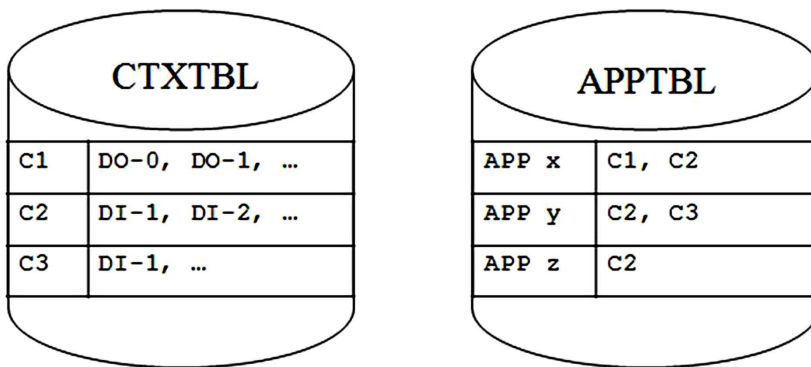
도면3



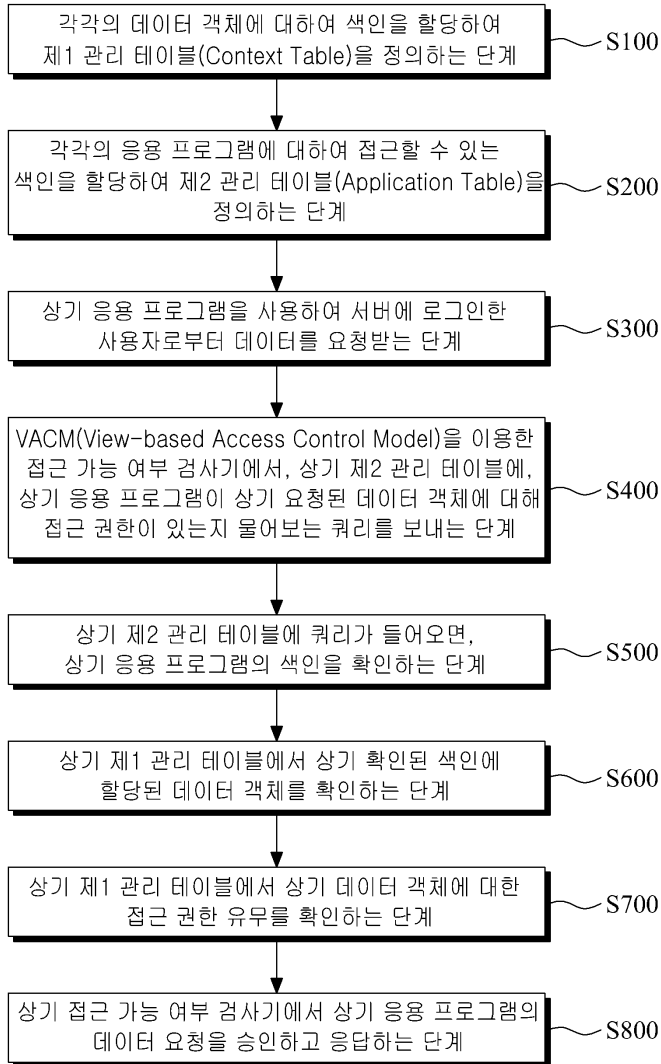
도면4



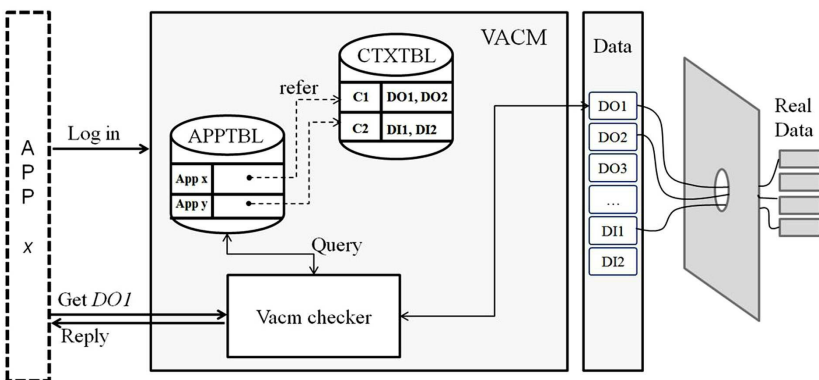
도면5



도면6



도면7



도면8

