KOREA UNIVERSITY

LIBERTAS
JUSTITIA
VERITAS

스마트 그리드 & 신뢰성

황 대 연
고려대학교 정형기법 연구실
2010. 1. 8

KOREA UNIVERSITY

LIBERTAS
JUSTITIA
VERITAS

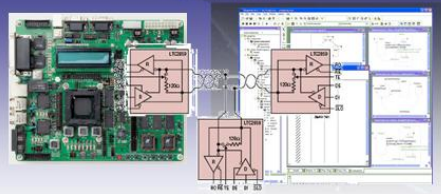
목차

- 서론
- 스마트 그리드
- 정형기법
- 연구 방향

LIBERTAS
JUSTITIA
VERITAS

Software Everywhere!!

SOC



Highly-Integrated Circuit

Security

Security Protocols / Smart Card

Robotics

Planning / Ontology / Hybrid Control System

Railway

Railway Control System

Safety Critical

Mission Critical

Security Critical

Aerospace

Space Shuttle / Aircraft Guidance / Navigation / Control System

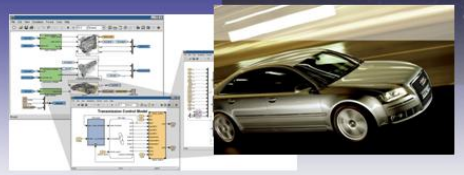
Nuclear Power Plant

Nuclear Power Plant Control System

Medical

Safety-Critical System In Medical Areas

Automotive



ECU (Electronic Control Unit) / Cruise Control System

KOREA UNIVERSITY

LIBERTAS
JUSTITIA
VERITAS

소프트웨어 오류로 인한 사고들

- 1985년 캐나다 Therac-25 방사선치료기 오류
- 1991년 이라크전 - 패트리어트 미사일 유도 실패
- 1994년 인텔 펜티엄 CPU 오류
- 1995년 미 덴버 공항 수하물 시스템 오류 -개항지연
- 1996년 Ariane5 로켓 발사실패
- 2003년 뉴욕 정전 사태
- 2005년 미 FBI VCF 프로젝트 실패

스마트 그리드 (Smart Grid)

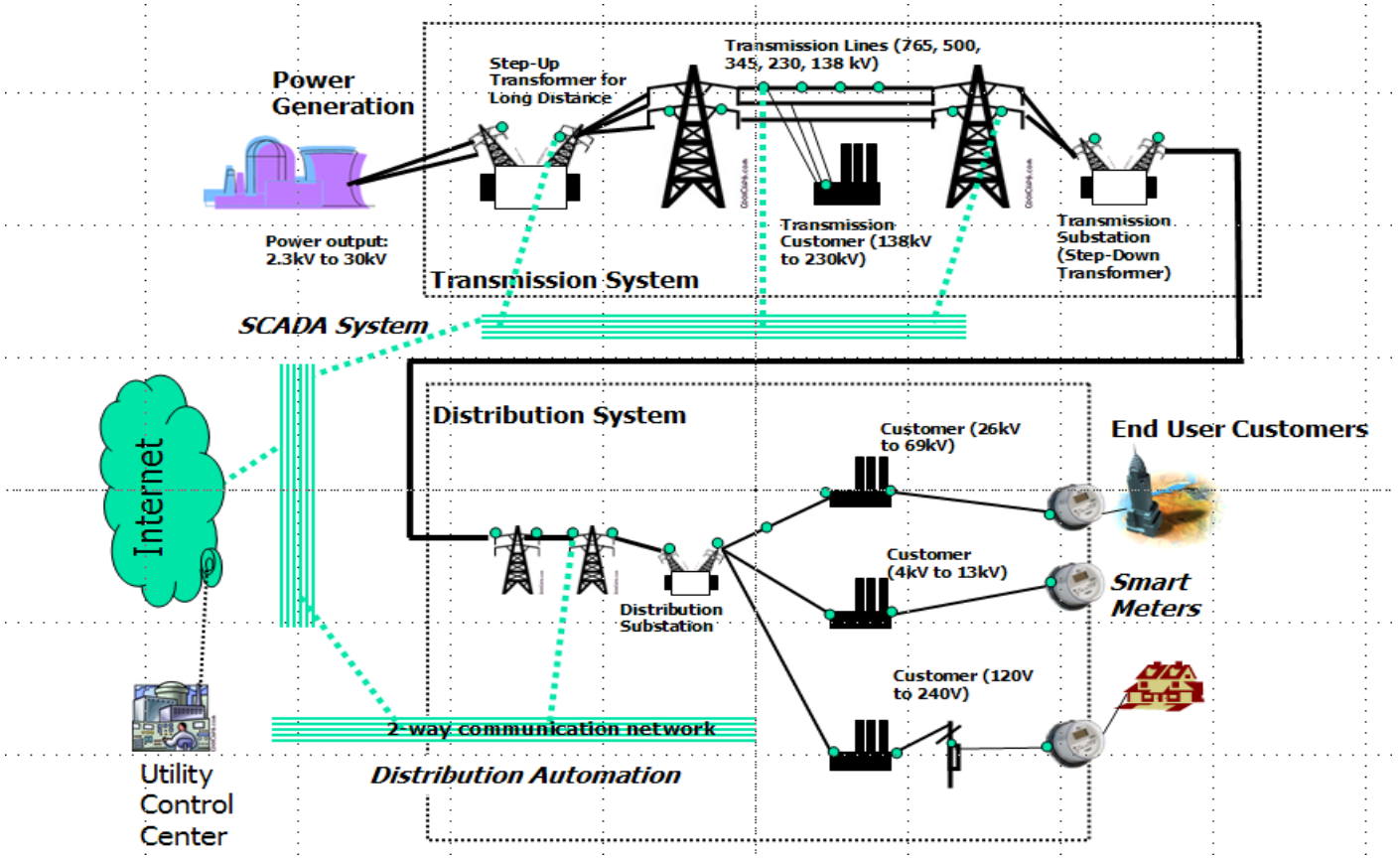
- **기존 전력망에 IT 기술을 접목한 스마트그리드**
  - 차세대 전력망, 지능형 전력망
  - 체계적이고 효율적인 관리

- **에너지 효율**
  - 전력공급자와 소비자가 양방향으로 실시간 정보 교환 (Smart Meter)
  - 최적의 요금 시간대를 찾아 전기를 사용
  - 에너지효율을 최적
  - 온실가스 배출 감소

- **녹색성장을 위한 스마트그리드 과제**
  - 기존 전력IT사업단에서 확대 및 개편된 사업단

스마트 그리드

- 두 망의 결합 (Electrical + Information)



The Smart Grid: Underlying Component Technologies and Architecture
(Copyright 2009, Dr. Lloyd Nirenberg)

LIBERTAS
JUSTITIA
VERITAS

전력 산업의 사건들

Power outages force evacuation of Woodstock hospital 7/30/08
Chicago, IL

Woman in iron lung dies during a power outage
Los Angeles, CA 5/29/08

Storm knocks out Euro 2008 TV feed worldwide
Vienna, Austria 6/25/08

Lights out in Vancouver after underground fire
Thousands in left without power
Vancouver, Canada 6/14/08

Power outages widespread in Texas after Dolly
Harlingen, Texas 7/25/08

Trip on Mexico's transmission line causes national power outage 5/26/08
Mexico City, Mexico

South Africa's power outages create national emergency
Johannesburg, South Africa 2/13/08

Power outage disrupts Hynix DRAM production
South Korea, Korea 5/22/08

Hours-long power outages anger, frustrate Pakistanis; government pushes daylight savings 6/1/08
Islamabad, Pakistan

USEA
United States Energy Association

USEA In Cooperation with General Electric

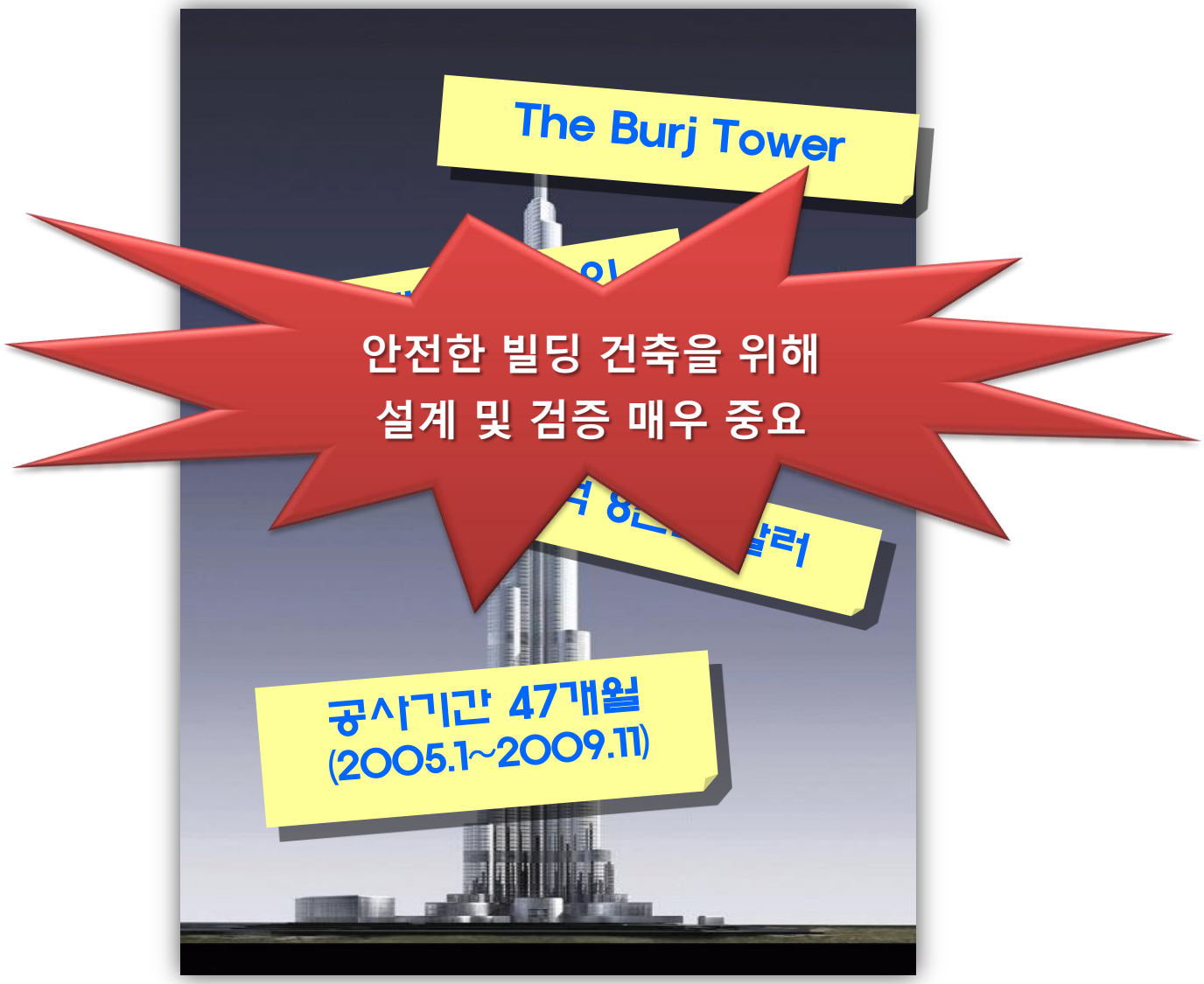
SMART GRID LUNCH AND LEARN SESSIONS

imagination at work

KOREA UNIVERSITY

LIBERTAS
JUSTITIA
VERITAS

고품질의 소프트웨어 개발 필요

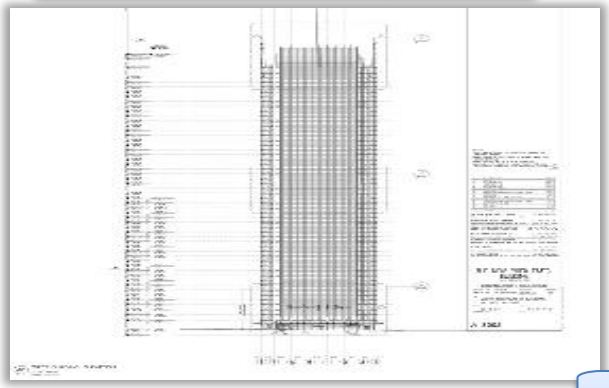


LIBERTAS
JUSTITIA
VERITAS

정형 기법 소개

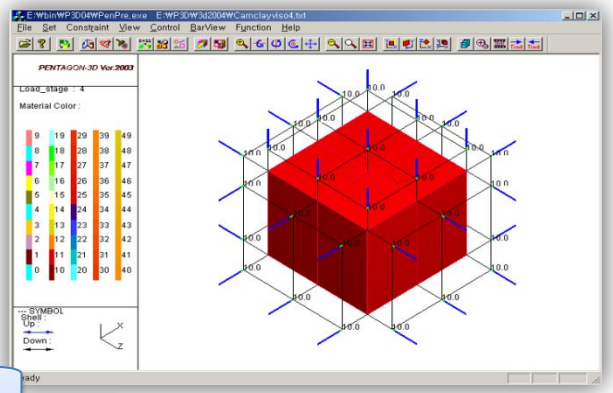
안전한 건축물

건축 설계



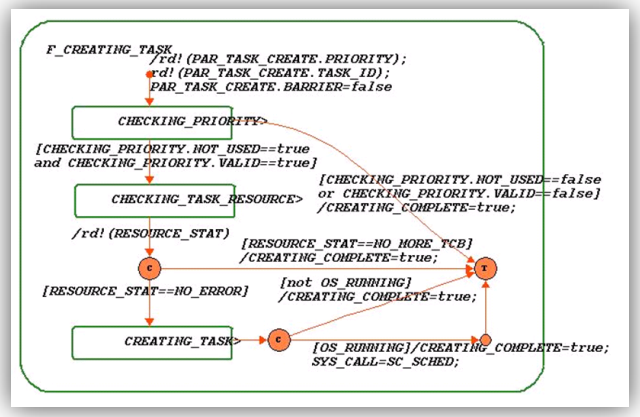
- 지진시의 내진성
- 하중에 관한 안전율
- 고온에서의 내열성

구조 해석



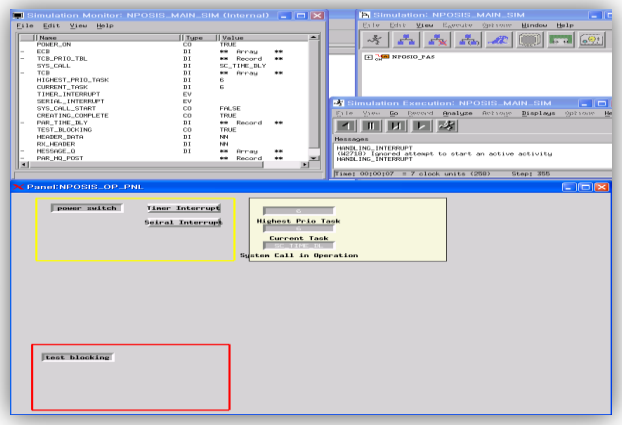
안전한 시스템

정형 명세



- 위험 요소에 대한 안전성
- 외부 공격에 대한 보안성
- 요구 조건에 대한 부합성

정형 검증



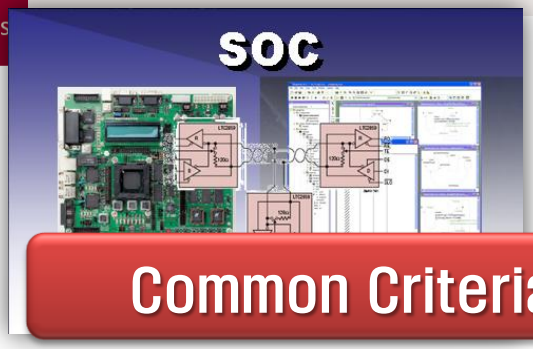
정형 기법

- **정형 기법**
  - 수학이나 논리 기반의 명세와 설계의 기술을 사용하여 컴퓨터 시스템이나 소프트웨어를 개발하는 기법

  - **정형 명세 (Formal Specification)**
    - 수리논리 등을 이용하여 시스템의 동작 환경, 시스템 요구사항, 시스템의 설계 등을 기술하는 것.
    - 요구 명세, 설계 명세
    - 논리 기반, 상태 기계 기반, algebra 기반

  - **정형 검증 (Formal Verification)**
    - 수학적, 논리적 증명방법을 통해 시스템의 설계와 시스템 요구사항의 만족 여부를 증명
    - 정리 증명, 모델 검사

국제적 규약



Common Criteria

ecurity Protocols / Smart Card

Planning / Ontology / Hybrid Control System

요구 사항	EAL 5	EAL 6	EAL 7
보안 정책 모델	정형적 보안 정책 모델	정형적 보안 정책 모델	정형적 보안 정책 모델
기능 명세	준정형적 기능 명세	준정형적 기능 명세	정형적 기능 명세
구조 설계	준정형적 구조 설계	준정형적 구조 설계	정형적 구조 설계
상세 설계	기술적 상세 설계	준정형적 상세 설계	준정형적 상세 설계
상호 관계	준정형적 상호 관계	준정형적 상호 관계	정형적 상호 관계

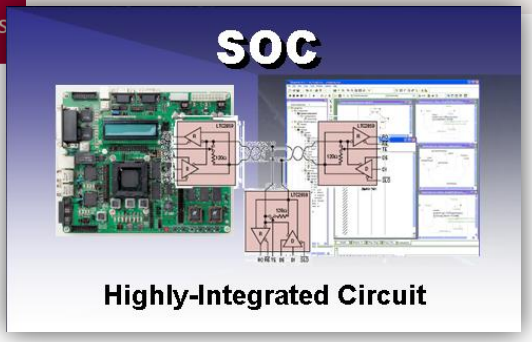
Nuclear Power Plant Control System

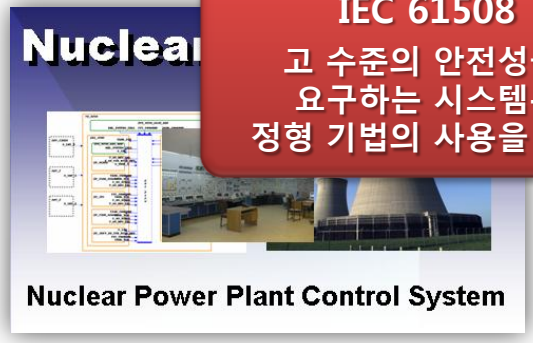
Safety-Critical System In Medical Areas

ECU (Electronic Control Unit) / Cruise Control System

LIBERTAS
JUSTITIA
VERITAS

국제적 규약





IEC 61508
고 수준의 안전성을
요구하는 시스템은
정형 기법의 사용을 권장

Table A.1 – Software safety requirements specification (see 7.2)

	Technique/Measure*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Computer-aided specification tools	B.2.4	R	R	HR	HR
2a	Semi-formal methods	Table B.7	R	R	HR	HR
	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR

NOTE 1 – The software safety requirements specification will always require a description of the problem in natural language and any necessary mathematical notation that reflects the application.

NOTE 2 – The table reflects additional requirements for specifying the software safety requirements clearly and precisely.

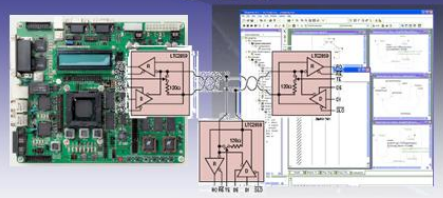
* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

Table B.1 – Recommendations to avoid mistakes during specification of E/E/PES requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Separation of E/E/PE safety-related systems from non-safety-related systems	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
	Inspection of the specification	B.2.6	– low	HR low	HR medium	HR high
	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	R low	R low	R medium	R high
	Computer aided specification tools	B.2.4	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

국제적 규약 (자동차, 항공 등)

SOC



Highly-Integrated Circuit

Security

Security Protocols / Smart Card

Robotics

Planning / Ontology / Hybrid Control System

Railway

Railway Control System

Safety Critical

Mission Critical

Security Critical

DO-178B

Aerospace

Space Shuttle / Aircraft Guidance / Navigation / Control System

Nuclear Power Plant

Nuclear Power Plant Control System

MISRA C Rule

Safety-Critical System In Medical Areas

Automotive

ECU (Electronic Control Unit) / Cruise Control System

정형 기법을 이용한 해외 개발 사례

- **파리 Metro 14호선 (1998)**
  - 적용 기술
    - B Method
    - 안전 필수 부분 개발 (전체 프로그램의 1/3 정도)
  - 적용 성과
    - 프랑스 철도국 인허가 획득.
    - Metro 전체 구간 레일 추가 비용 절감
    - 완전 자동화된 시스템 구축

- **파리 Roissy 공항 24시간 무인 셔틀 (2007)**
  - 적용 기술
    - B Method
    - 코드 생성 툴 사용
  - 적용 성과
    - 모델 작성에 많은 시간 단축
    - 뉴욕, 바르셀로나, 프라하, 파리 지하철 등에 기술 적용

정형 기법을 이용한 해외 개발 사례

- **Eurocopter (우주 항공)**
  - 적용 기술
    - 정형 기법 도구인 SCADE 적용
    - 유로콥터 자동 항법장치 S/W 개발
  - 적용 성과
    - 디버깅 시간 단축
    - 48시간 내 신규 버전 수정 및 통합 가능

- **SAAB, GM, Siemens (자동차)**
  - 적용 기술
    - 정형기법 기반 설계도구인 I-Logix사의 Statemate MAGNUM 사용
    - 차체 전자 제어 어플리케이션 설계 검증 및 코드 생성
  - 적용 성과
    - 설계 및 자동 코드 생성을 통한 디버깅 시간 단축
  - GM은 OEM에게 정형기법 기반의 도구 사용을 공식적으로 요구

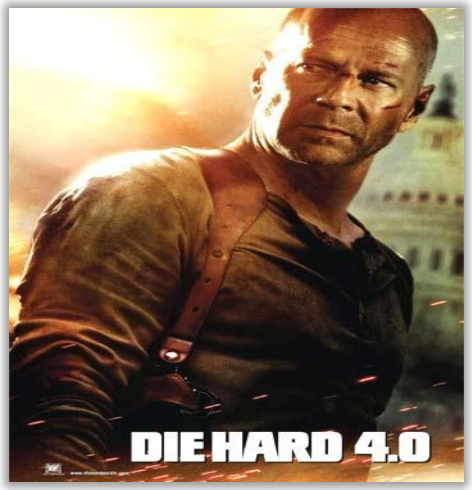
SCADA

- **SCADA (Supervisory Control And Data Acquisition) system**
  - 집중 원격감시 제어시스템 또는 감시제어 데이터 수집시스템
  - 통신 경로상의 아날로그 또는 디지털 신호를 사용하여 원격장치의 상태정보 데이터를 원격장치(remote terminal unit)로 수집, 수신, 기록, 표시하여 중앙제어 시스템이 원격장치를 감시 제어하는 시스템을 말한다.
  - SCADA 시스템은 발전, 송배전시설, 석유화학플랜트, 제철공정시설, 공장 자동화 시설 등 여러 종류의 원격지 시설장치를 중앙집중식으로 감시 제어하는 시스템이다.
  - SCADA 시스템의 주요 기능으로는 ANSI/IEEE Stdc37.1-1987의 권고안에 명시된
    - 1. 원격장치의 경보상태에 따라 미리 규정된 동작을 하는 감시시스템의 기능인 경보기능
    - 2. 원격 외부장치를 선택적으로 수동, 자동 또는 수.자동복합으로 동작하는 감시제어기능
    - 3. 원격장치의 상태정보를 수신, 표시, 기록하는 감시시스템의 지시(표시) 기능
    - 4. 디지털 펄스정보를 수신, 합산하여 표시, 기록에 사용할 수 있도록 하는 누산 기능
    - 5. 미리 규정된 사상을 인식, 발생사상의 데이터를 제공하는 감시시스템 기능

    등이 있다.

SCADA

- **SCADA의 보안**
  - 경영환경의 변화로 비즈니스 시스템과 통합되고 개방형 시스템으로 표준화되고 있으며 인터넷에 연결
  - 국가주요기반시설이 인터넷을 통해 어디서나 공격 당할 수 있게 되어 국가안보를 위협받는 결과
  - "전기 및 소프트웨어에 대한 약간의 지식과 500달러짜리 장비만 있으면 스마트 그리드 시스템에 침입할 수 있다. 게다가 한 개의 장비를 해킹하면 다른 스마트 그리드 시스템 전체를 조종할 수 있는 것으로 나타났다. " - 미국의 보안 컨설팅 업체인 IO 액티브



FIRE SALE이 등장한 다이하드 4

2009.2 미국 인디아나폴리스 표지판 해킹

Formal Methods in SCADA

- **정형기법 적용 연구**
  - Security Considerations in SCADA Communication Protocols
    - Intelligent Systems Research Laboratory, Sep 2004
    - Casper with FDR etc.
  - Using Model-based Intrusion Detection for SCADA Networks
    - Proceedings of the SCADA Security Scientific Symposium, Jan 2007
    - Modbus TCP : simple request-response protocol
    - Model Based Detection, PVS language

LIBERTAS
JUSTITIA
VERITAS

AMI와 Smart Meter

- **AMI(Advanced Metering Infrastructure)**
  - Smart Grid를 가능하게 하는 기본적인 기술
  - 전기요금 절감에 관하여, 소비자에게 진보된 계측, 통신, 정보기술을 통합하여 제공하는 것을 의미
  - 계측(metering)을 통한 쌍방향 의사소통 및 Home Area Network, 계측기 **(Smart Meter)**를 이용한 전력 수요의 통제, 실시간 확인 가능한 각 시간 별 및 날짜 별 전력 사용량, MDM(Meter Data Management) 시스템을 포함

- **Smart Meter**
  - 소비자에게 전력 요금을 실시간으로 보여주며 동시에 전기 사용에 대한 정보를 모아 중앙 센터로 보내는 역할을 한다.
  - 현재 4000만개의 스마트 미터가 전세계적으로 사용되고 있음
  - 대략 5-15%정도의 전기료 감소
  - 전력 정보에 대한 쉬운 접근 제공
  - Google PowerMeter

KOREA UNIVERSITY

LIBERTAS
JUSTITIA
VERITAS

감사합니다