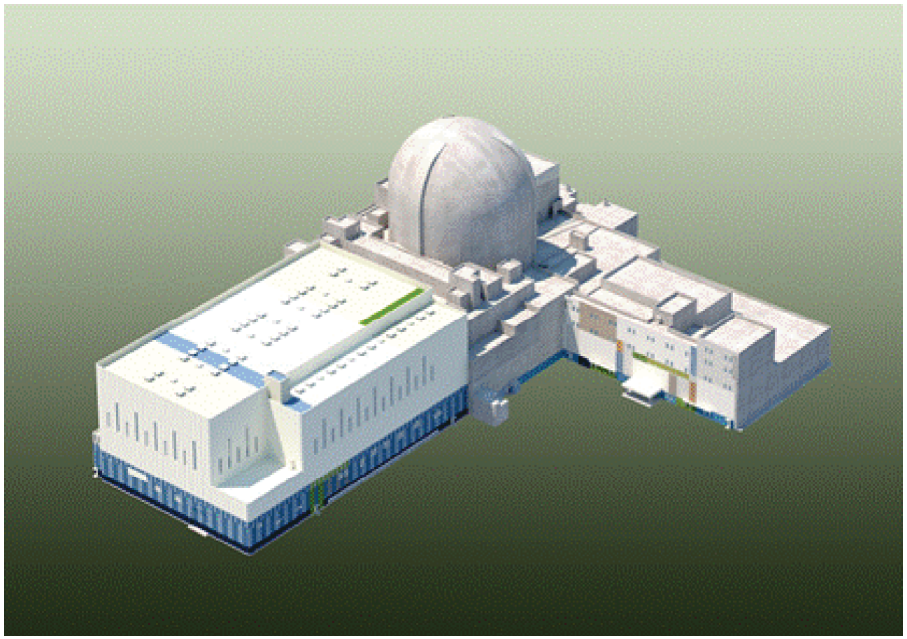
NON-PROPRIETARY

Instrumentation and Control Design (Instrumentation and Control System)



KEPCO/KHNP

April 20~21. 2016

ACRS Meeting (Apr.20-21. 2016)

Contents

- Overview
  - system design features
  - System 80+ vs APR1400
  - system architecture
- Simplified Diagrams
  - PPS and ESF-CCS
  - human-system interface (HSI)
- System Design Principles
  - redundancy
  - independence
  - deterministic performance
  - watchdog timer
  - control of access
  - diversity and defense-in-depth (D3)
- Conclusions

* For acronyms, see slide 5.

Overview (System Design Features)

- I&C systems are fully digitalized.
- I&C systems use diverse platforms;
  - safety system : Programmable Logic Controller (PLC)
  - non-safety system : Distributed Control System (DCS)
  - diverse actuation system : FPGA-based Logic Controller (FLC)
- Data communication systems maintain independence.
- Software common-cause failures (CCFs) are analyzed.
  - safety system
  - non-safety control system

Overview (System 80+ vs APR1400)

Design		System 80+	APR1400
Platform	Safety	PLC (Common Q*)	PLC (Common Q*)
	Control	DCS	DCS
	Diverse Protection	diverse from safety and control platforms	FLC
HSI		soft control	soft control
Reactor Trip Switchgear		one set not diverse (4 breakers)	two sets diverse (8 Breakers)
Procedure		paper	computerized

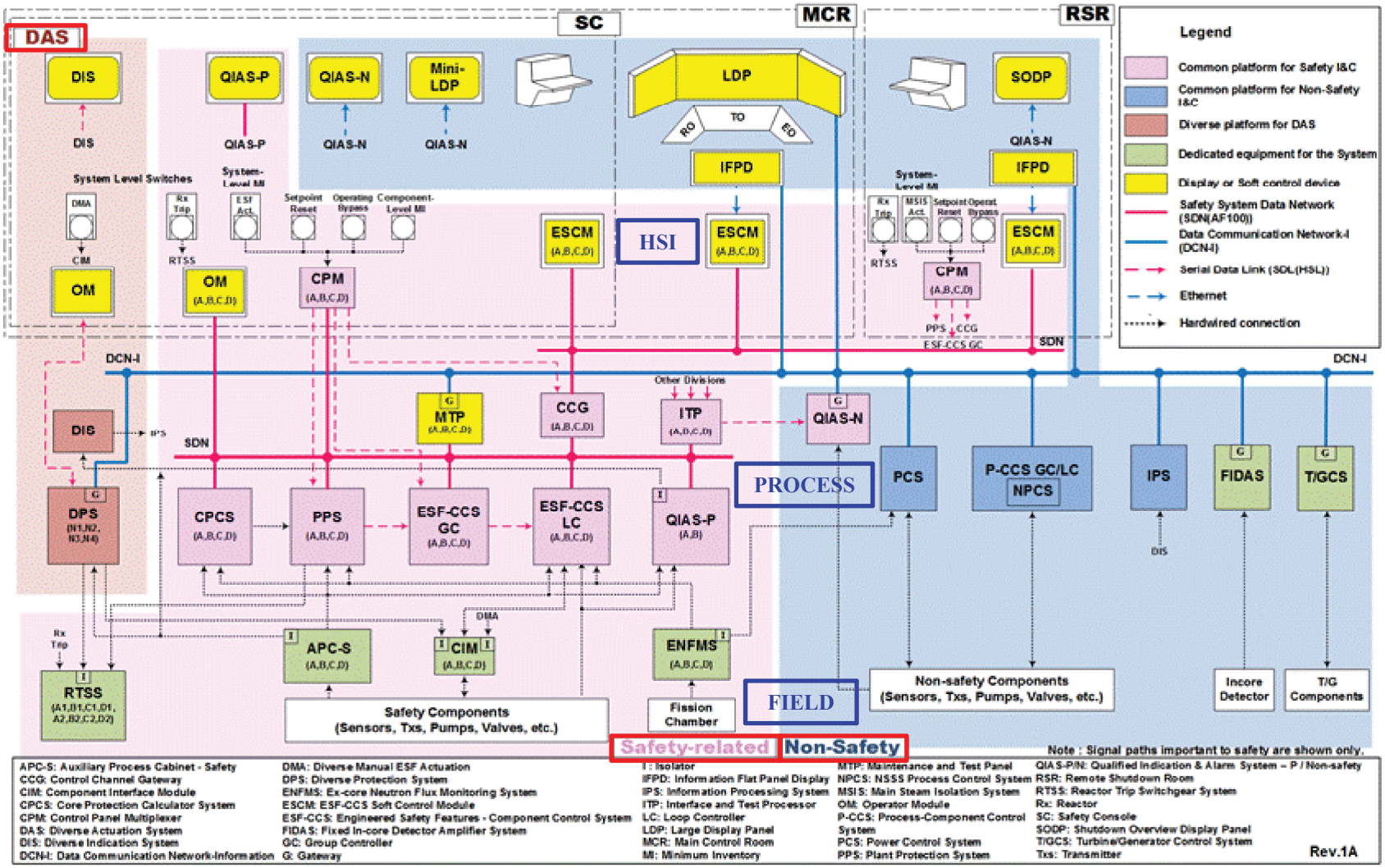
* Common Q : Westinghouse safety I&C platform certified by NRC

Overview (System Architecture) (1/2)

- Vertical Architecture
  - HSI (top*) : Main Control Room, Remote Shutdown Room
  - Process (middle*) : Safety, Control, and Diverse Actuation Systems
  - Field (bottom*) : sensors, actuators
- Horizontal Architecture
  - Safety System (center*) : PPS, ESF-CCS, CPCS, QIAS-P
  - Non-safety Control System (right*) : PCS, P-CCS, QIAS-N, IPS
  - Diverse Actuation System (left*) : DPS, DIS, DMA switch
- Data Communication System
  - Serial Data Link (SDL)
  - Safety System Data Network (SDN)
  - Non-safety Data Communication Network-Information (DCN-I)
  - Ethernet

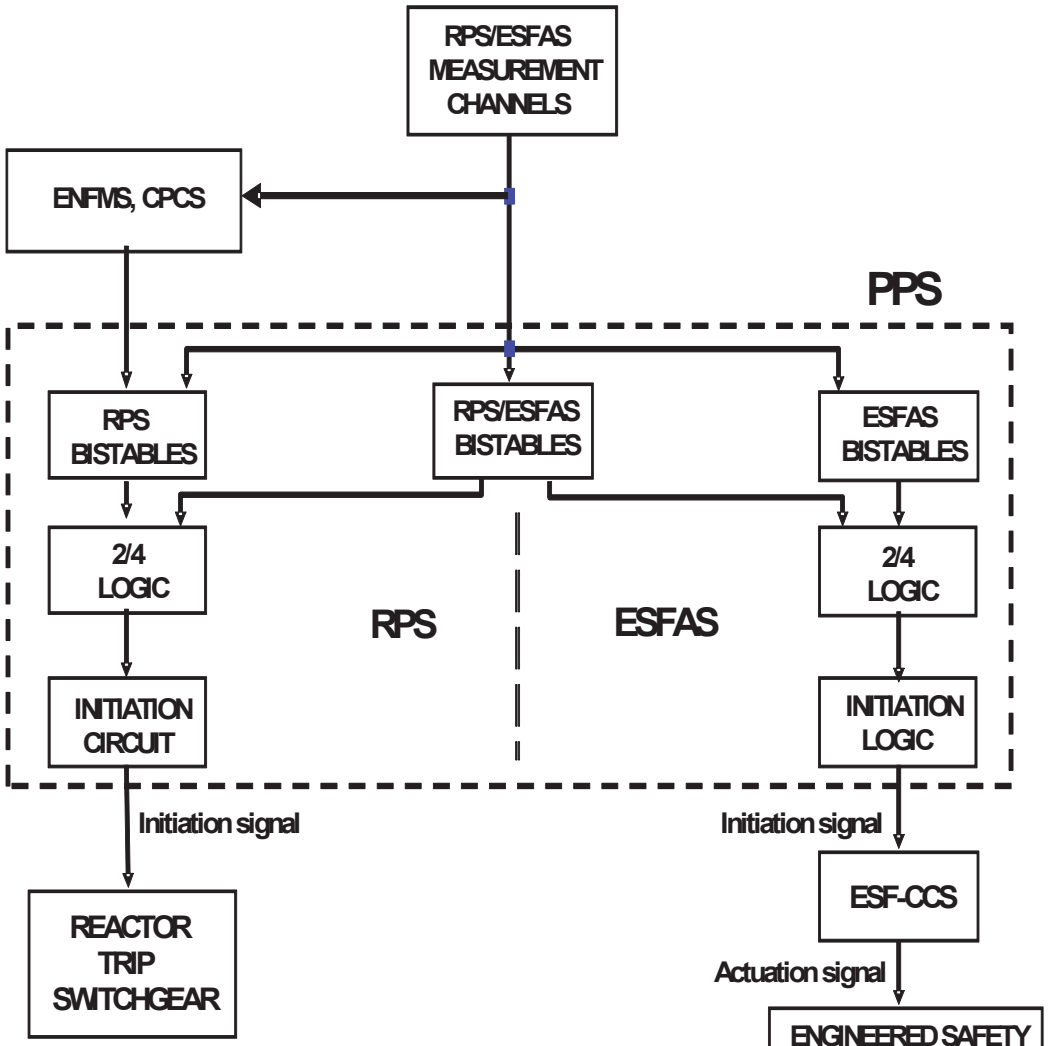
* See next page.

Overview (System Architecture) (2/2)



Simplified Diagram (PPS and ESF-CCS)

- Plant Protection System
  - initiates automatic/manual RPS and ESFAS
- ESF-CCS
  - receives automatic/manual ESFAS initiation signal
  - executes component control logic of ESF actuation devices

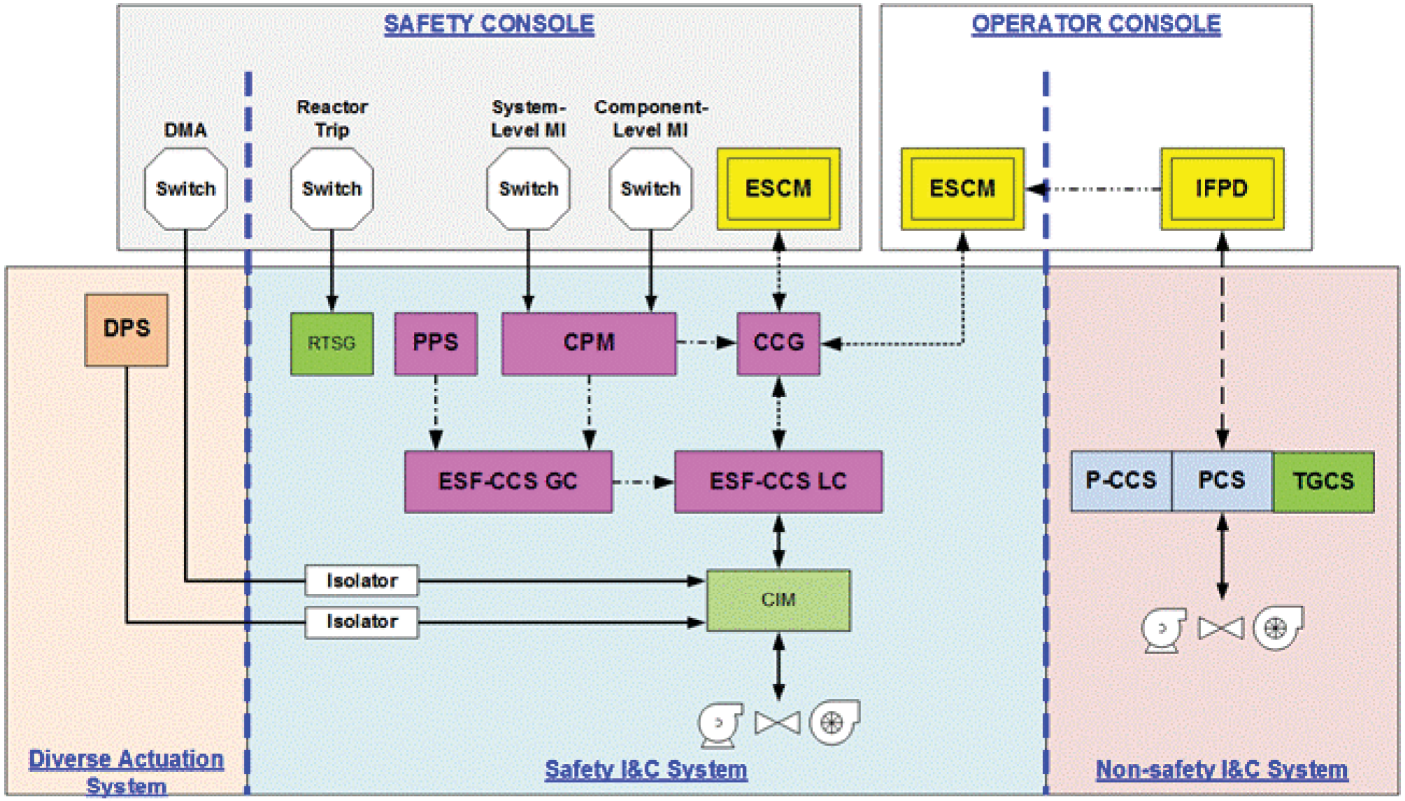


RPS : Reactor Protection System

ESFAS : Engineered Safety Features Actuation System

Simplified Diagram (HSI)

- Human-System Interface (HSI) for Component Control



ABBREVIATIONS AND LEGENDS

CCG: Control Channel Gateway
CIM: Component Interface Module
CPM: Control Panel Multiplexer
DMA: Diverse Manual ESF Actuation
DPS: Diverse Protection System
ESCM: ESF-CCS Soft Control Module
ESF-CCS: Engineered Safety Features-Component Control System
FLC : Field Programmable Gate Array (FPGA)-based Logic Controller
IFPD: Information Flat Panel Display
MI: Minimum Inventory
P-CCS: Process-Component Control System
PCS: Power Control System
PPS: Plant Protection System
RTSG: Reactor Trip Switchgear
TGCS: Turbine/Generator Control System

PLC Platform
Control and Display
DCS Platform
FLC Platform
Self-standing Platform

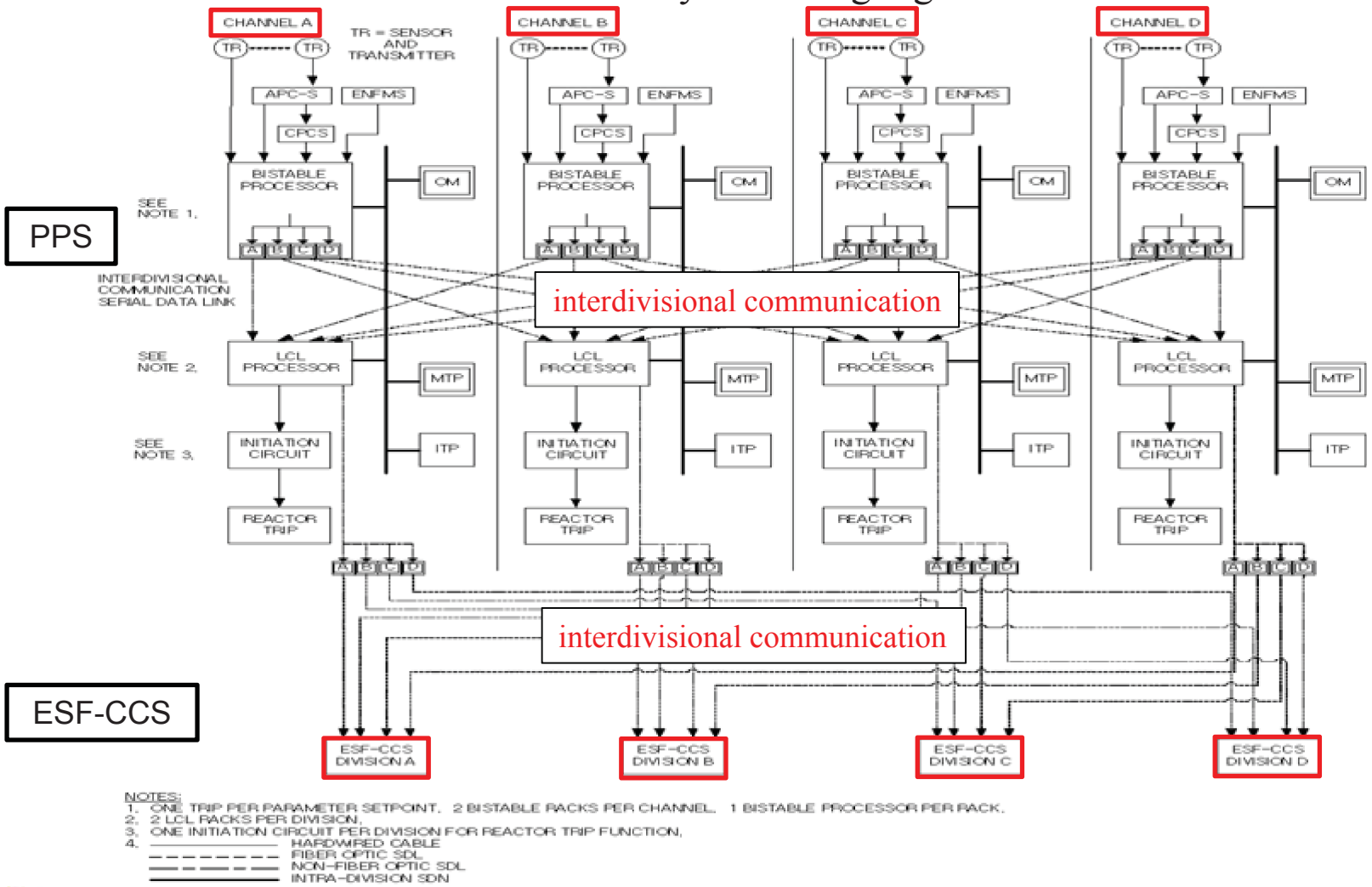
Hardwired
Safety System
Data Network (SDN)
Serial Data Link (SDL)
Data Communication Network - Information (DCN-I)
Ethernet

System Design Principles (Redundancy) (1/4)

- Four Channel/Division Redundancy for Single Failure Criteria
- Exceptional Two Channel/Division Redundancy
  - Reed Switch Position Transmitter (RSPT) for Control Element Assembly (CEA) positions
  - Qualified Indication and Alarm System - P (QIAS-P)

System Design Principles (Redundancy) (2/4)

- PPS and ESF-CCS
  - interdivisional communication only for voting logic



NOTES:
1. ONE TRIP PER PARAMETER SETPOINT. 2 BISTABLE RACKS PER CHANNEL. 1 BISTABLE PROCESSOR PER RACK.
2. 2 LCL RACKS PER DIVISION.
3. ONE INITIATION CIRCUIT PER DIVISION FOR REACTOR TRIP FUNCTION.
4. ——— HARDWIRED CABLE
   - - - - - - - - FIBER OPTIC SDL
   — — — — — NON-FIBER OPTIC SDL
   ——————— INTRA-DIVISION SDN

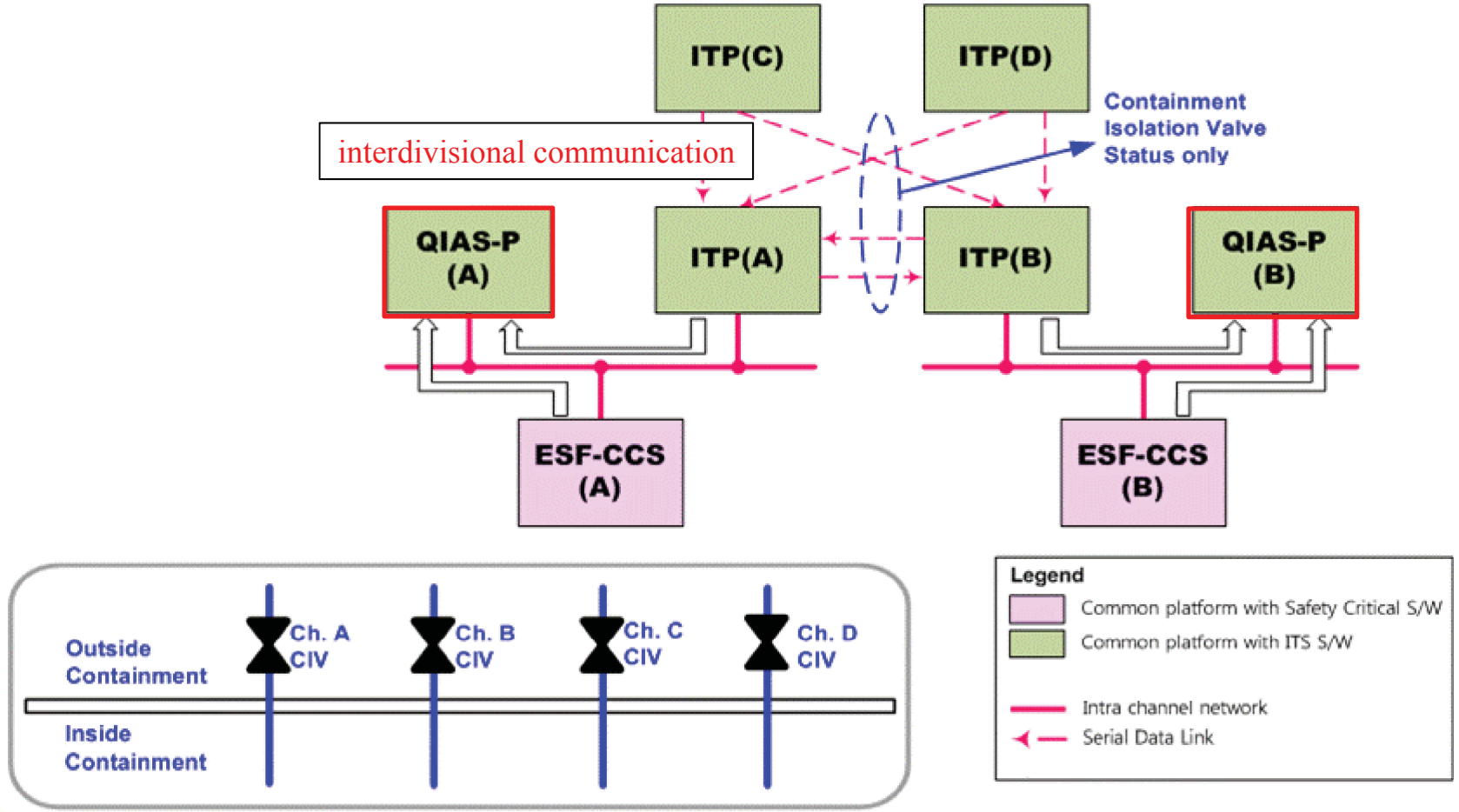
System Design Principles (Redundancy) (3/4)

- Core Protection Calculator System

TS

System Design Principles (Redundancy) (4/4)

- Qualified Indication and Alarm System – P (A/B)
  - interdivisional communication between ITPs for four channel valve status to display complete containment isolation



System Design Principles (Independence) (1/2)

- Interdivisional communication of CPCS (a*) * See next page.
  - by SDL for four channel CEA positions
- Interdivisional communication of PPS (b*, c*)
  - by SDL for voting logic (BP->LCL->GC)
- Interdivisional communication of ITP (d*)
  - by SDL for four channel containment isolation valves status
- Safety to non-safety communication
  - by SDL from the ITP to QIAS-N for safety information (e*)
  - by Ethernet from the MTP to DCS Gateway Server for safety information (f*)
- Non-safety to safety communication
  - by Ethernet from IFPD to ESCM for component identification information (g*)
- All communications are analyzed in Appendix C of Safety I&C System TeR as per ISG-04 for communication independence

System Design Principles (Independence) (2/2)

- Data Communication System

TS

System Design Principles(Deterministic Performance)

- Processor Module has Process Section and Communication Section
- Process Section
  - task scheduler schedules control module to execute a task
  - control module has its own cycle time, i.e., deterministic
- Communication Section
  - takes twice the cycle time of process section, i.e., deterministic
- Task Scheduler
  - monitors the cycle time
  - times out a watchdog timer (WDT), if cycle time is exceeded
- NRC Safety Evaluation Report (SER) of Common Q Topical Report (TR)
  - AC160* will operate deterministically to meet the recommendations in BTP-21.

* ABB PLC

System Design Principles (Watchdog Timer)

TS

System Design Principles (Control of Access)

- Physical Control of Access
  - administrative control of key locks
  - cabinet open alarms
- Electronic Control of Access
  - testing and setpoint modification are performed using Function Enable keyswitch
  - software loading is performed from workstation thru normally disconnected cable

System Design Principles (D3) (1/2)

- Diversity and Defense-in-Depth (D3) Assessment
  - addresses software CCF of digital safety I&C systems
- CCF Coping Analysis
  - analyzes each postulated CCF for each event evaluated in safety analysis using best-estimate method
- Diverse Actuation System (DAS)
  - DPS actuates automatic diverse reactor trip and ESFAS*
  - DMA switches actuate ESF components
  - DIS displays parameters to support safety functions

* Aux. Feedwater Actuation System (AFAS) and Safety Injection Actuation System (SIAS)

System Design Principles (D3) (2/2)

- Diversity between PPS and DPS

TS

Conclusions

- The APR1400 has fully digitalized I&C systems.
- System design principles comply with regulatory bases.
  - redundancy (IEEE 603-1991)
  - communication independence (ISG-04, Rev.1)
  - deterministic performance (BTP 7-21, Rev.5)
  - watchdog timer (BTP 7-17, Rev.5)
  - control of access (IEEE 603-1991)
  - diversity and defense-in-depth (BTP 7-19, Rev.6)