中广核 CGN

Nuclear Power China Techenergy Co.,Ltd.

Simplicity and Application simplicity in FitRel R&D

Zhang Chunlei, CTEC
September 13th, 2015

Natural Energy Powering Nature

8th Workshop,
"Simplicity and Application simplicity in FitRel R&D "

7th Workshop,
"Customer's Viewpoint of FPGA-based I&C Platform"

6th Workshop,
"FPGA-based DAS system used in Yangjiang Unit 5/6"

5th Workshop,
"FitRel Platform by FPGA Technology"

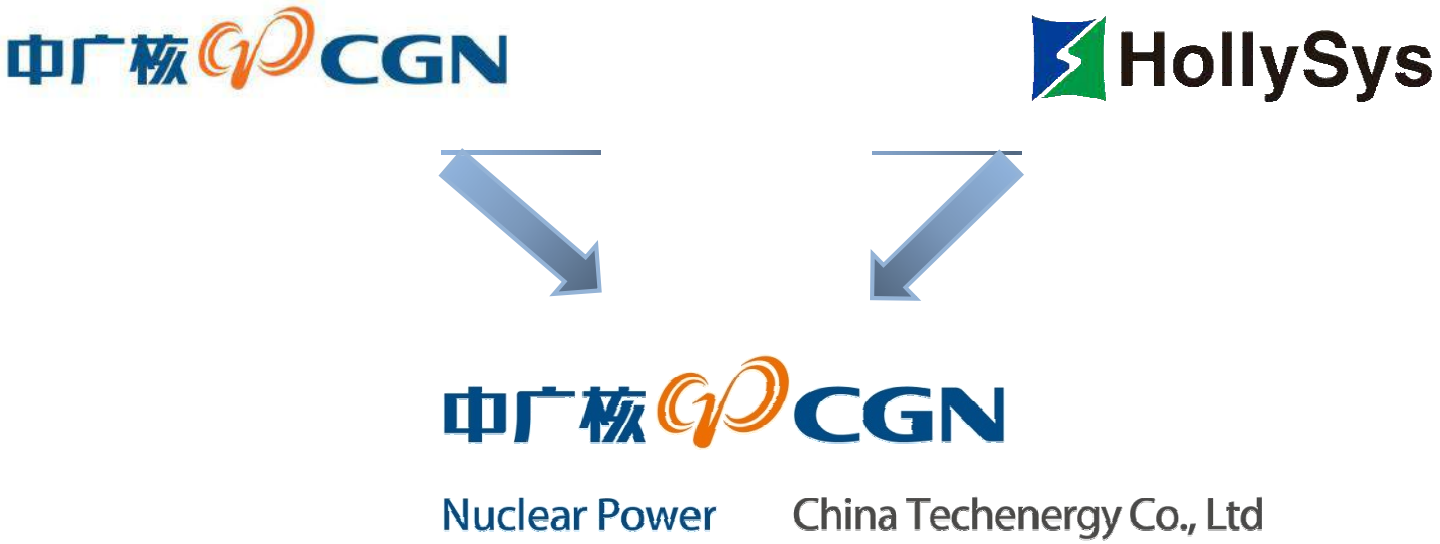
中广核 CGN

Nuclear Power China Techenergy Co.,Ltd.

01. About CTEC

Natural Energy Powering Nature

1.0 Basic Info. of CTEC



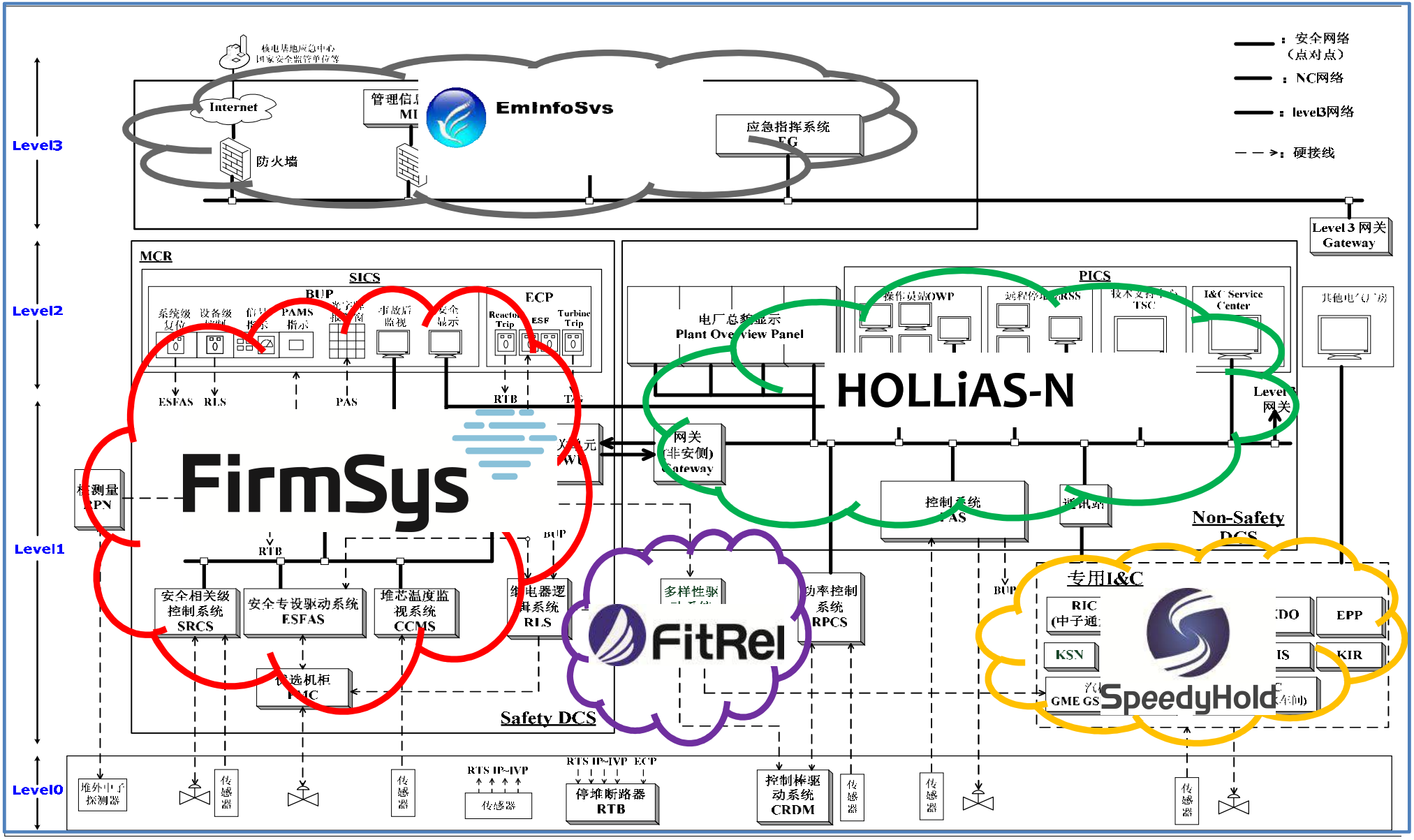
- Established in December 2005
- Share: CNPEC (60%) & Hollysys(40%)
- Staff Number: 859 (until March 2015)

1.1 Qualifications

2014	TUV ISTec Certificate	TÜV ISTec
2013	1E DCS Panel & Screen Design/Manufacture License	
	NRC Certification Preliminary Evaluation	
	Safety Integrity Level 3 Certificate	SIL3
	V&V Assessment Certificate by ISTec	ISTec
2011	V&V Evaluation by TÜV	TÜV
	Capability Maturity Model Integration Level 4	CMMI L4
	EDF Supplier Qualification License on Power and I&C Industry	
2010	Civil Nuclear Safety Electrical Equipment Design/Manufacture License	
	ISO14001 Certificate	ISO14001
	OHSAS18001 Certificate	OHSAS18001
2009	Corporate Standard	Q/GLHJ
2008	Capability Maturity Model Integration Level 3	CMMI L3
2006	ISO9001 Certificate	ISO9001

1.2 Solution and Platform

Overall Solution of I&C NPP



1.3 FirmSys application

Upgraded CCMS for Daya Bay NPP put into operation on Nov 19th, 2013

"大亚湾 RIC 控制柜升级改造项目" 工程样机鉴定
专家评审会评审意见

2013 年 8 月 8 日，北京广利核系统工程有限公司（以下简称"广利核"）邀请专家（名单附后）在北京举行了"大亚湾 RIC 控制柜升级改造项目"工程样机鉴定专家评审会。

与会专家在听取了广利核公司对该项目中的核电站数字化堆芯冷却监测系统（CCMS）的工程样机 V&V、系统测试和设备鉴定的工作汇报基础上，经过充分讨论，形成如下意见：

1. 该项目所提供的工程样机 V&V、系统测试和设备鉴定资料齐全可信，方法完整，符合鉴定要求；
2. 工程样机 V&V 过程符合标准要求，结果真实、可信；
3. 工程样机测试过程符合要求，验证了 CCMS 工程样机已实现合同与技术说明书中的功能、性能及接口要求；
4. 工程样机设备鉴定试验（环境试验、EMC 试验、抗震试验）的试验项目的内容及结果满足法规、标准和合同要求。

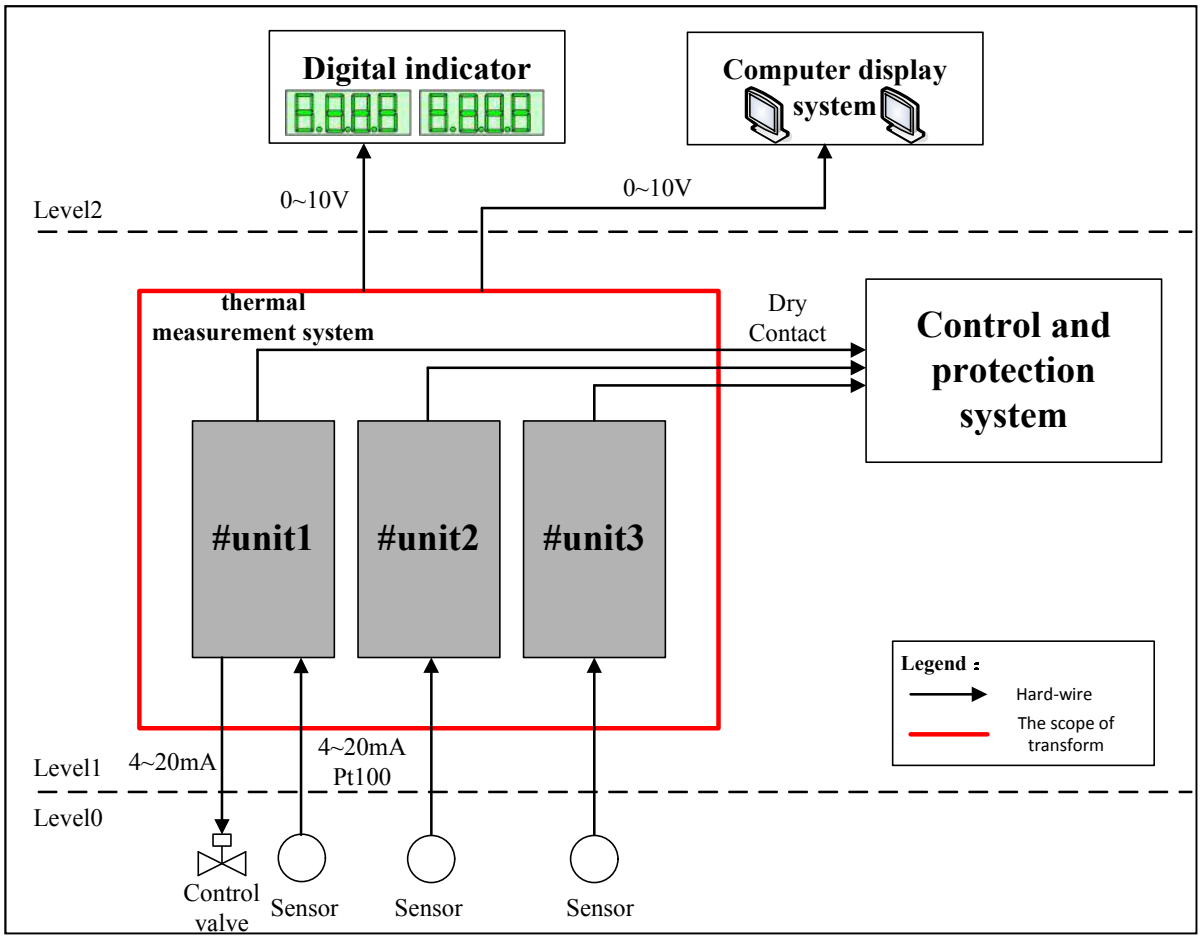
同时，与会专家建议，供货设备应与被鉴定的工程样机保持一致，如有差别要进行必要的分析或验证。

专家组组长：
日期 2013.8.8.

7

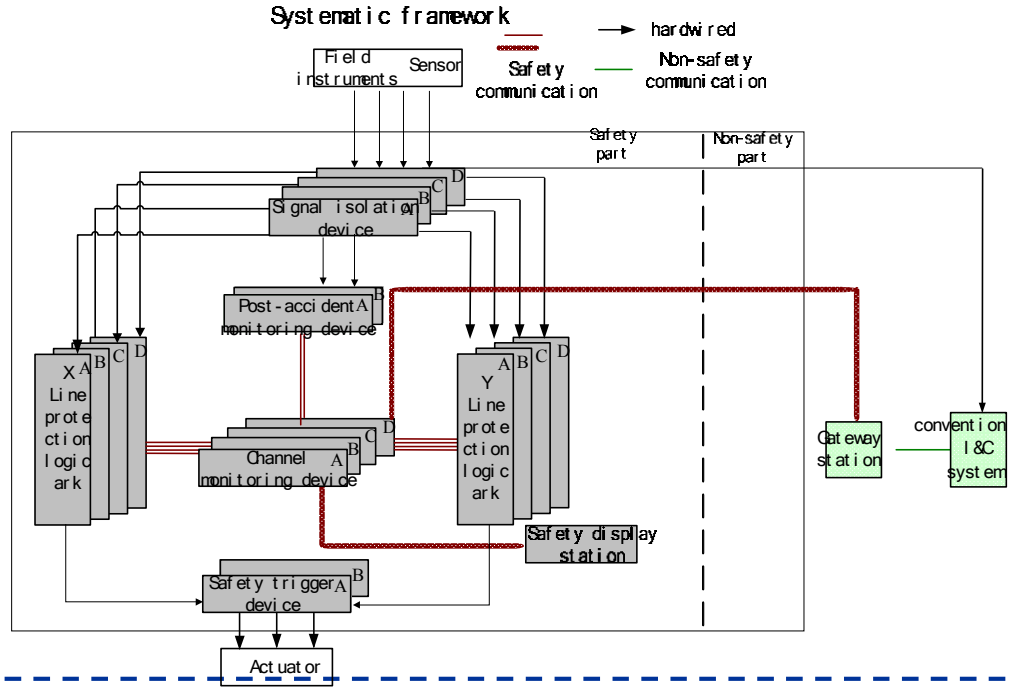
1.4 FirmSys application

Process Monitoring Control System put into operation on Aug 30th, 2013

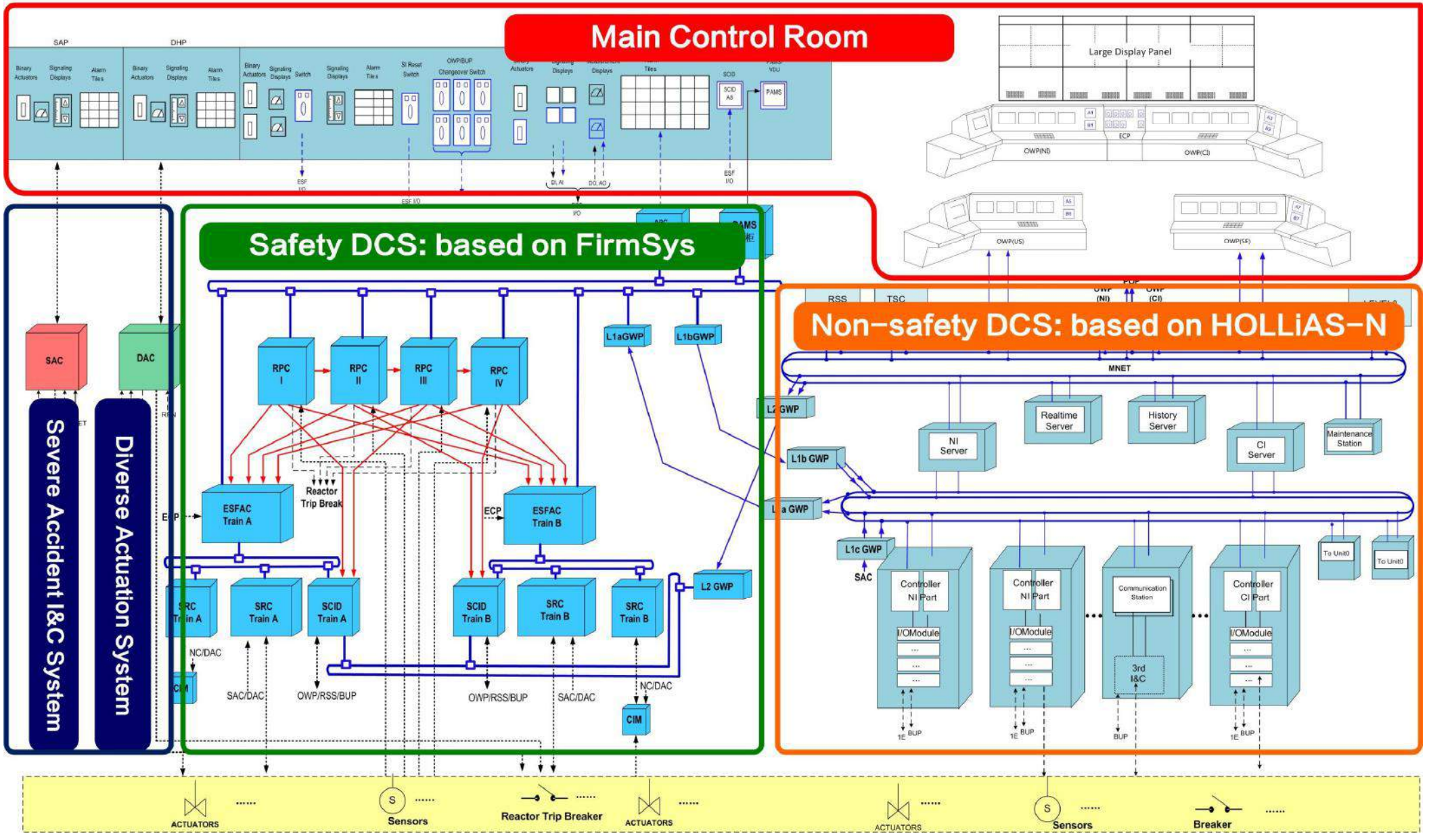


1.5 FirmSys application

HTR-PM RPS Prototype developed since 2009



1.6 YJ unit 5


Main Control Room
SAP
DHP
Large Display Panel
OWP(NI)
OWP(CI)
OWP(US)
OWP(SS)
ECP
Safety DCS: based on FirmSys
SAC
DAC
Severe Accident I&C System
Diverse Actuation System
RPC I
RPC II
RPC III
RPC IV
L1aGWP
L1bGWP
L2 GWP
Reactor Trip Break
ESFAC Train A
ESFAC Train B
SRC Train A
SCID Train A
SCID Train B
SRC Train B
NC/DAC
SAC/DAC
OWP/RSS/BUP
CIM
Non-safety DCS: based on HOLLiAS-N
RSS
TSC
MNET
L2 GWP
L1b GWP
L1c GWP
NI Server
Realtime Server
History Server
CI Server
Maintenance Station
Controller NI Part
Controller CI Part
I/OModule
Communication Station
3rd I&C
To Unit0
BUP
ACTUATORS
Sensors
Reactor Trip Breaker
Breaker

02. FitRel Platform

2.0 FitRel platform overview

FitRel

FitRel ：Fit and Reliability.

based on FPGA technique

- **Processing in parallel**
- **Fast response time**

Simplicity	Reliability	Platform
No OS	Seismic ability	Algorithm independence
No Processor	Thermal design	Easy maintenance
Function independence	EMC design	Configurable and modularity
Easy to verify	Reliability prediction	
	FMEA analizy	
	High diagnosis coverage	

2.1 FitRel Platform market position

1. DAS
   FPGA have sufficient diversity to Processor-based Platform.

2. RPS(large scale reactor)
   Processor + FPGA.
   e.g. RTS with FPGA and ESFAC with Processor.
   e.g. 2 channels with FPGA and 2 channels with Processor.
   e.g. station-A with FPGA and station-B with Processor
   for a parallel redundant station.

3. RPS(small scale reactor)

2.2 Component

FitRel Platform

Hardware

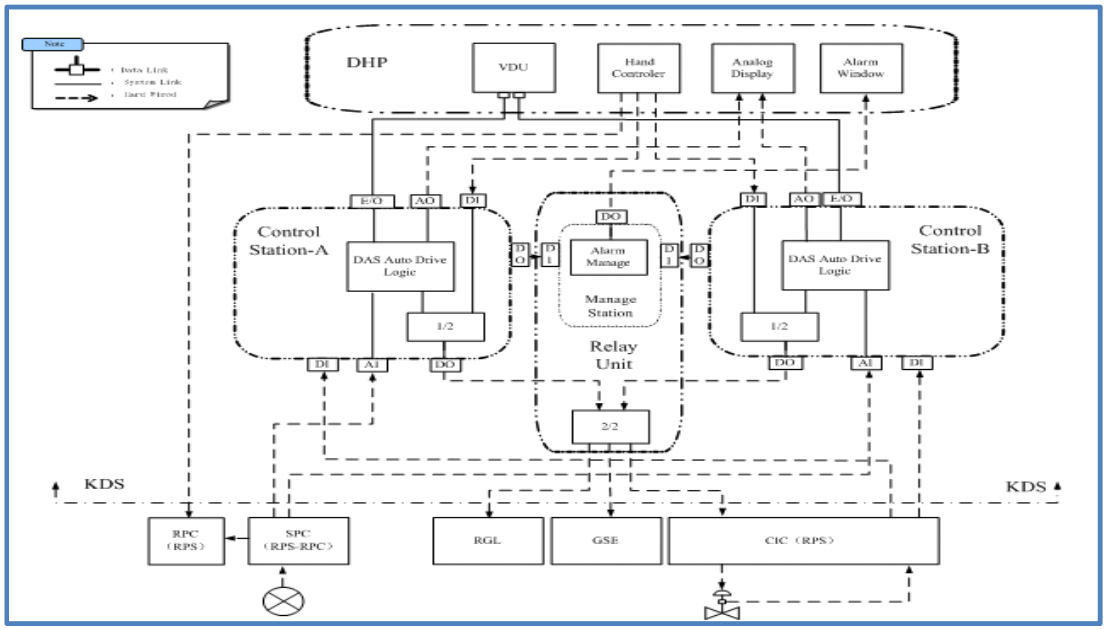
Cabinet and Rack

Software tools

2.3 Application case

YJ5/6 DAS

-- 2 of 2 architecture to have enough ability of anti-malfunction.
-- Unit 5 in FT stage.
-- 5 cabinets fulfill the function of DAC.



03. Simplicity in FitRel Platform R&D

3.0 Why simplicity?

Simplicity

- intrinsic property of FPGA
- Architecture design
- Hardware design
- Algorithm block design

Decrease the complexity of platform
Decrease the workload of R&D and qualifation
Decrease the workload of V&V

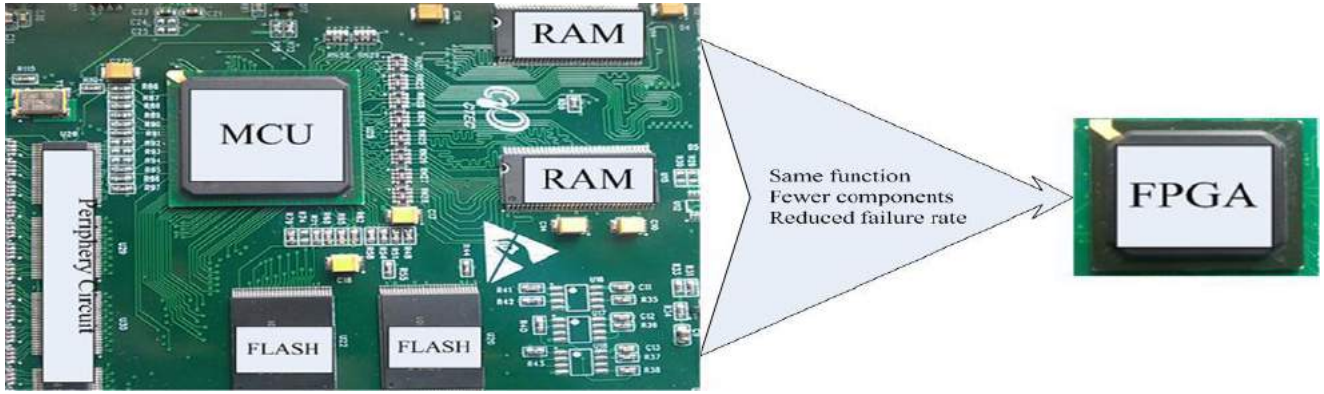
Safety

3.1 Simplicity in hardware design

1. Reduce the failure rate

The truth is that hardware design is more complicated to gain the high level DC. It is unnecessary to reserve to much hardware resource.

e.g.



Simplicity hardware design can also:

- reduce the power consumption,
- reduce the spare of PCB,
- and easier replacement in case of obsolescence.

3.2 Simplicity in hardware and driver design

1. Reduce the complexity of driver

e.g. Ethernet physical layer and data link layer design.
To fulfill the physical layer and data link layer function of Ethernet, you can use FPGA + MAC + PHY, and you also can use PFGA + PHY.

MAC+PHY

PHY

MAC chip afford whole function of data link layer, and you must configure all the register bit by bit, like the mode and the FIFO.

But the application function is just the customized data transceiver, the second design can simplify the scale of HLD code and decrease the complexity of V&V.

3.3 Simplicity in Algorithm block design

1. Not use IP core

IP core is black box. It is difficult to verify the safety by V&V team, and the IP core also take too much resource of FPGA.

e.g. the float_adder block, the customized algorithm takes 770 cells, and the IP takes 1557 cells.

Report for cell m_adc.netlist
Instance path: ai_chl_ctl.ai_data_inf.m_adc

Cell usage:

cell	count	area	count*area
AO1	2	1.0	2.0
DFN1C0	54	1.0	54.0
DFN1E1	2	1.0	2.0
DFN1E1C0	33	1.0	33.0
GND	1	0.0	0.0
MX2	23	1.0	23.0
MX2A	1	1.0	1.0
MX2B	28	1.0	28.0
NOR2A	3	1.0	3.0
NOR2B	25	1.0	25.0
NOR3C	4	1.0	4.0
OA1B	1	1.0	1.0
OR2	2	1.0	2.0
OR2A	4	1.0	4.0
OR3	1	1.0	1.0
VCC	1	0.0	0.0
com_agb_26s	1	154.0	154.0
com_agb_6s	1	33.0	33.0
com_alb_26s	1	145.0	145.0
com_alb_6s	1	14.0	14.0
com_alb_8s	1	19.0	19.0
fix_2_float	1	657.0	657.0
float_2_fix	1	735.0	735.0
float_adder	1	1391.0	1391.0
float_multiplier	1	1557.0	1557.0
signed_multiplier_24s_13s_37s_36s_74s_6	1	769.0	7
TOTAL	195		5657.0

04. Application Simplicity

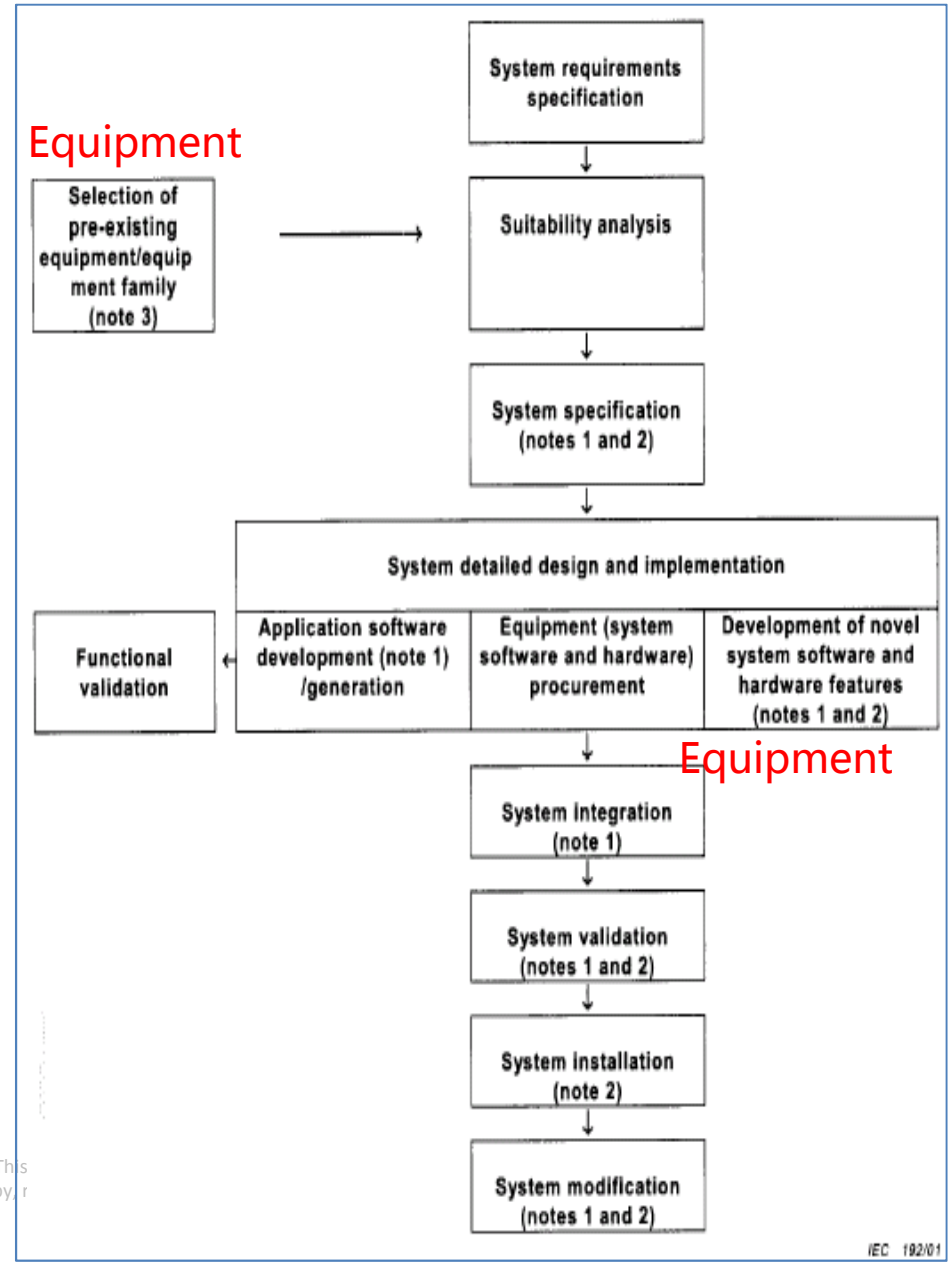
4.0 Application simplicity

1. What is application simplicity ?

As an equipment supplier, we said that FPGA-based I&C platform have some advantages, we also need to analyse the requirements from our users, who integrate the system with platform(I&C engineer) and final users in the safety system life cycle.

-- they need a configurable platform.
-- they need powerful tools in different life cycle.

These requirements are defined as **application simplicity** (which can also be called **easy-to-use**).

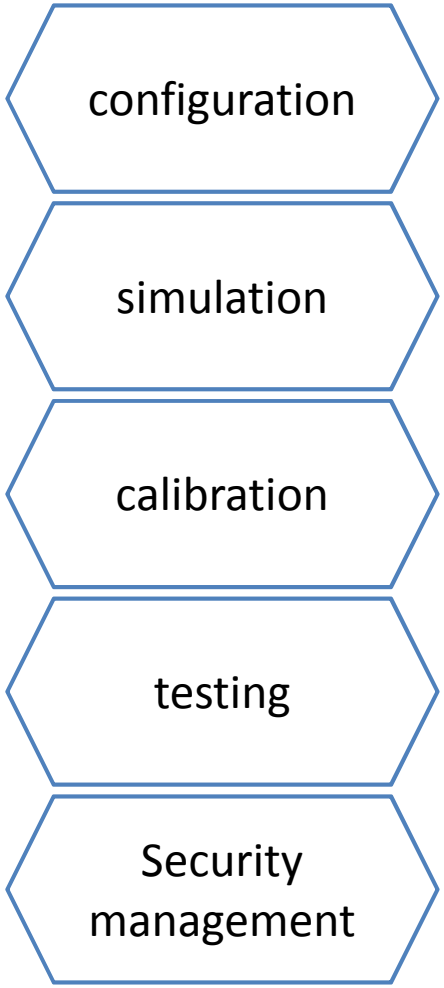


4.1 ancillary functions and tools

1. ancillary functions and tools

I&C platform needs to provide a number of so-called ancillary functions such as run-time monitoring and diagnostics (including the monitoring of sensors), which can increase the DC coverage and reduce the part of periodic testing, the time-to-repair, the risk of human errors that maybe injected in performing periodic tests.

Tools include security management, simulation, calibration,monitoring, testing etc.
The operator or maintenance technician need to change the parameters such as setpoints, monitor the diagnose information, and run periodic testing in the defined interval.



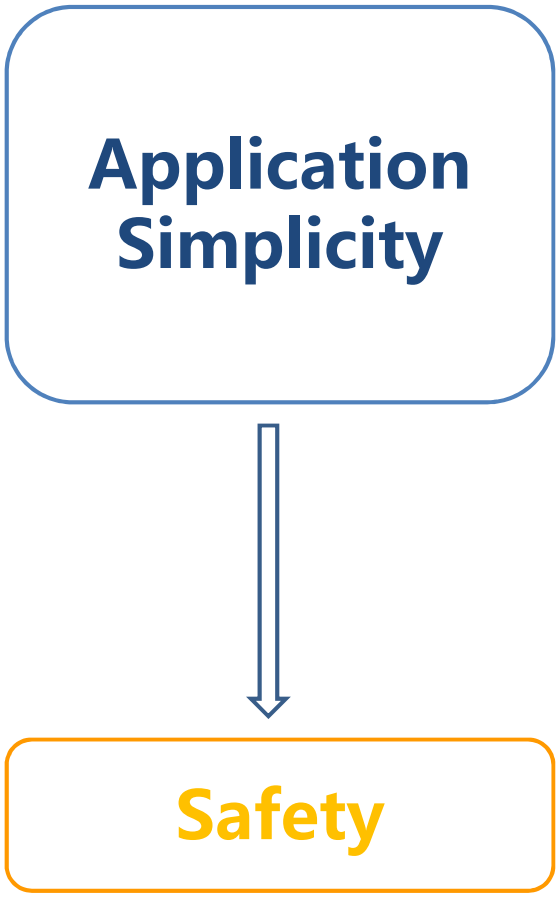
4.2 Safety and application simplicity

1. Safety and application simplicity

Why should we pay more attention to the application simplicity ?

The complexity is decreased in the different stages of system safety life cycle.

The more function that tools fulfill, the less job saved by people, then the total complexity will be decreased, and the probability of malfunction injected by people is decreased.

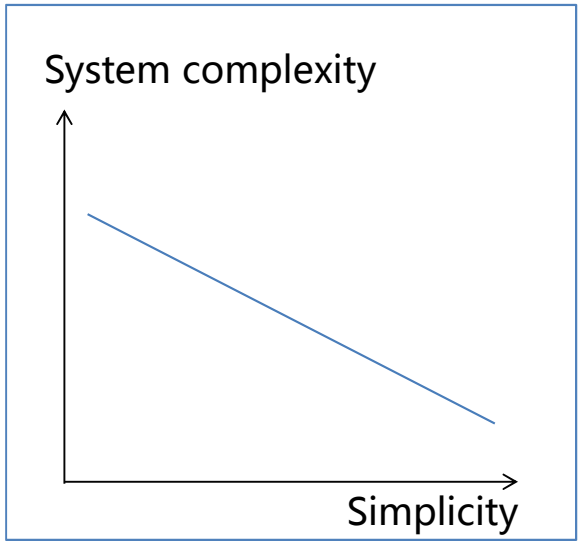


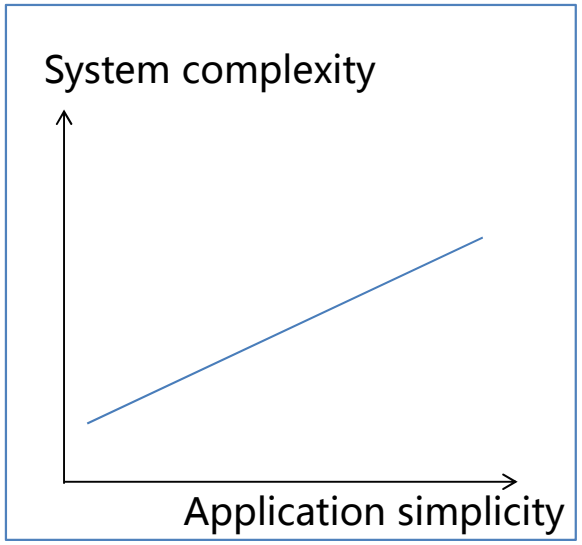
05. Simpliciy and Application Simplicity

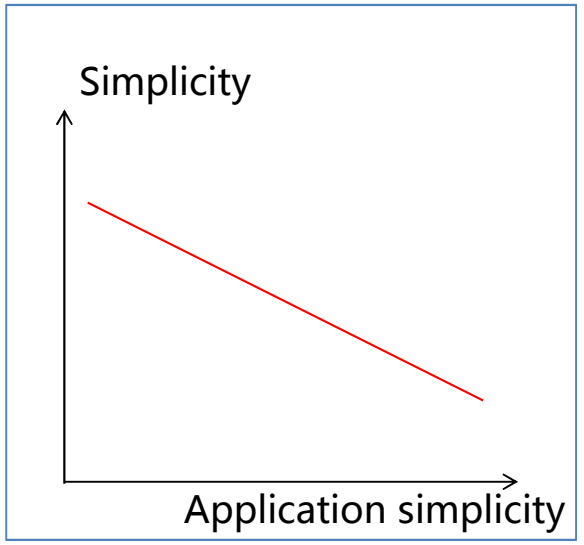
5.0 System complexity

1. System complexity

Both the simplicity and the application simplicity contribute to safety.







It is contradictory between simplicity and application simplicity.
You can't have your cake and eat it too ?

5.1 Measures to practice

1. Function segregation

-- Draw lessons from the architecture of DCS and PLC (not explain below).

-- Segregate the safety function and ancillary function. An intrinsic difference between microprocessor-based and FPGA-based solutions is the parallel structure to segregate functions that are logically independent.

One of the advantages of FPGA technology is the ability to design system architectures of which ancillary functions (e.g., run-time monitoring of sensors and I&C functions)are segregated such that failures or anomalies in the processing of those functions will not impact the ability of the circuit to perform its safety I&C functions.

5.1 Measures to practice

2. Independence and constraint

-- independence between safety functions and ancillary functions.

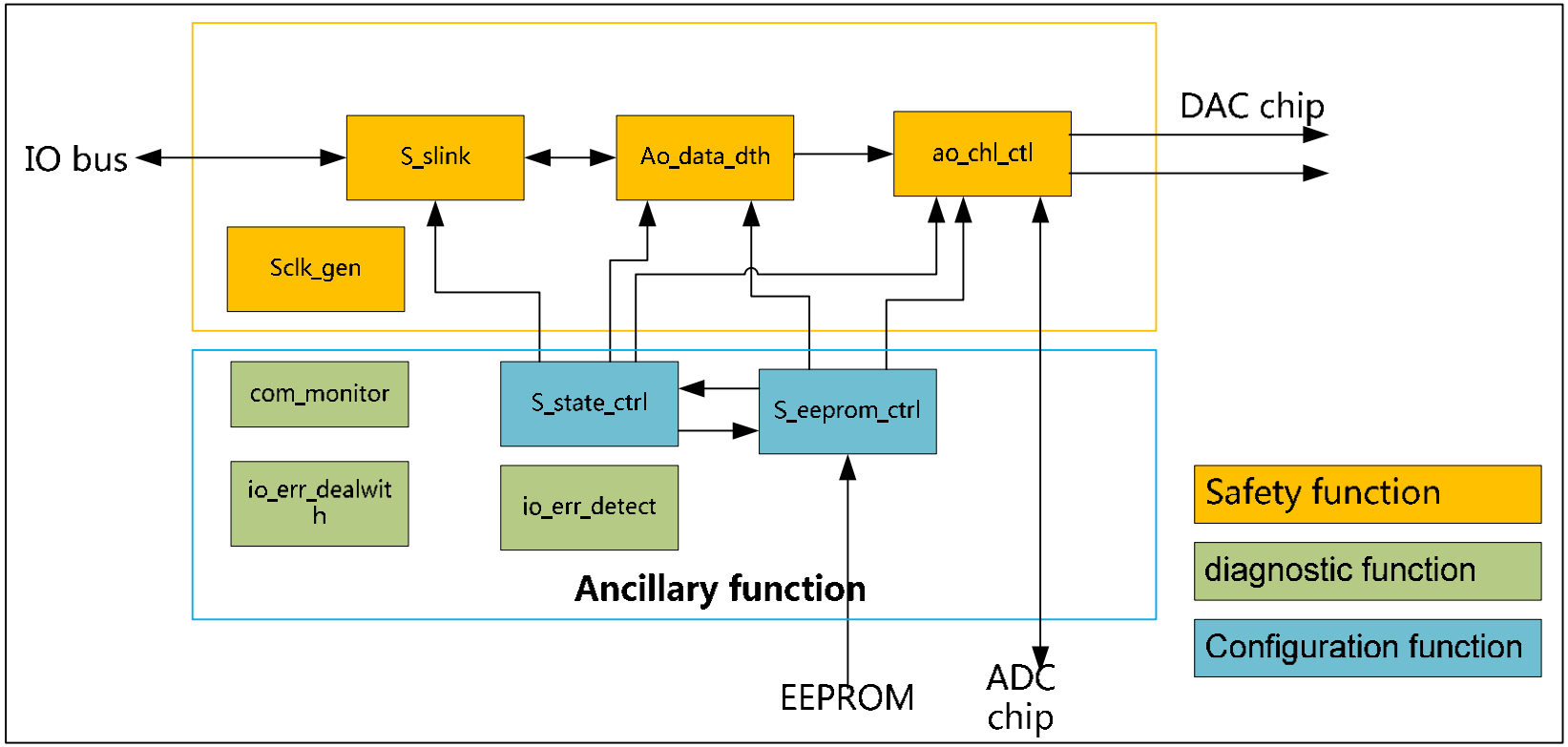
The circuit design should segregate non-interacting functions as much as possible to minimize unnecessary interdependencies, reduce complexity, increase testability and verifiability, and contain the consequences of faults or failures (random or systematic).

-- constraint of place and route.

Care should be taken during synthesis and place & route to ensure that these do not create dependencies between functions meant to be segregated within the design. Post-implementation reviews and analyses should verify that no unnecessary dependencies have been created during implementation.

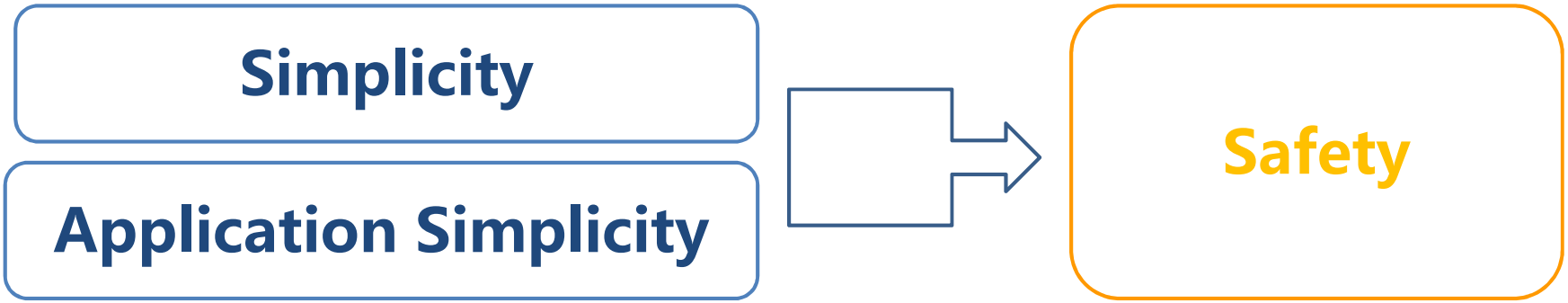
5.1 Measures to practice

3. Case of independence between safety functions and ancillary functions



5.2 Summary

Simplicity is finite, and application simplicity is infinite even for processer based I&C platform. Ordinary, it is difficult to balance the application simplicity and the complexity of system.



Thanks!