Development of digital I&C system in HTR-PM

Shi Guilian

CTEC
1. CTEC Profile - Organization

Providing full-life-cycle and end to end digital I&C system solution and service to NPPs

10 departments

708 employees
1. CTEC Profile-products
1. CTEC Profile-Certificates

<table>
<thead>
<tr>
<th>Year</th>
<th>Certificate Description</th>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>Independent 3rd party V&amp;V certificate on Firmsys</td>
<td>ISTEC</td>
</tr>
<tr>
<td>2013</td>
<td>design/manufacturing license on 1E panels &amp; civil 1E electric equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NRC preliminary evaluation on Firmsys</td>
<td>SIl3</td>
</tr>
<tr>
<td></td>
<td>Function safety certificate by SIl3</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>3rd party V&amp;V evaluation by TUV</td>
<td>TUV</td>
</tr>
<tr>
<td></td>
<td>CMMI L4</td>
<td>CMMI L4</td>
</tr>
<tr>
<td></td>
<td>EDF supplier qualification for electric, I&amp;C</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Design license on civil nuclear safety electric equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manufacturing license on civil nuclear safety electric equipment</td>
<td>ISO14001/OHSAS18001</td>
</tr>
<tr>
<td>2009</td>
<td>enterprise standard</td>
<td>Q/GLHJ</td>
</tr>
<tr>
<td>2008</td>
<td>CMMI L3</td>
<td>CMMI L3</td>
</tr>
<tr>
<td>2006</td>
<td>ISO9001</td>
<td>ISO9001</td>
</tr>
</tbody>
</table>
1. CTEC Profile- Projects

Projects covering all the in-service NPPs and majority new builds, the reactor types including CPR1000, ACPR1000, M310, EPR, HTR, CNP, CEFR, etc.

- **CPR1000**: 14 unit DCS
  - HYH 1-4, ND 1-4, YJ 1-4, FCG 1-2
  - 13 delivered to NPP
  - 5 under commercial operation

- **ACPR1000**: 4
  - 2: Integration in CTEC (YJ56)
  - 2: in contract negotiation (HYH56) (Big step, FirmSys)

- **NC-DCS, Safety-DCS, BOP I&C, DCS simulator in FSS, Emergency system etc.**
2. HTR-PM DCS - contracts

<table>
<thead>
<tr>
<th>No.</th>
<th>Project</th>
<th>Contract time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>HTR-PM digital RPS prototype</strong></td>
<td>2009.09</td>
</tr>
<tr>
<td>2</td>
<td><strong>HTR-PM digital RPS supply</strong></td>
<td>2009.09</td>
</tr>
<tr>
<td>3</td>
<td><strong>HTR-PM non-safety DCS prototype</strong></td>
<td>2010.04</td>
</tr>
<tr>
<td>4</td>
<td><strong>HTR-PM non-safety DCS supply</strong></td>
<td>2010.07</td>
</tr>
<tr>
<td>5</td>
<td><strong>HTR-PM DEH(Digital Electric Hydraulic Control System)</strong></td>
<td>2012.09</td>
</tr>
</tbody>
</table>
## 2. HTR-PM DCS - contracts

<table>
<thead>
<tr>
<th>UNIT</th>
<th>Safety DCS</th>
<th>NC-DCS</th>
</tr>
</thead>
</table>
|      | ➢ System Design  
      | ➢ SW V&V    | ➢ NI design  
      |              | ➢ purchaser  |
|      |            |       |
|      |            | ➢ Contract  
      |              | ➢ NI BOP design |
|      |            |       |
|      |            | ➢ DEH purchaser |
|      |            |       |
|      | ➢ Equipment development  
      | ➢ Safety Equipment qualification  
      | ➢ Basic / Detail design  
      | ➢ Manufacture, integration, test.  
      | ➢ Technical support |
2. HTR-PM DCS - roadmap

- First engineering prototype, then real system manufactured
- Same software and hardware with the actual DCS
- Safety DCS: 1:1 engineering prototype
- NC DCS: verify key design, DCS Architecture, new control logic, MMI etc.

With almost all level2 configuration and 30% of level1 input/output
2. HTR-PM DCS - roadmap

➢ The safety-DCS equipment is dedicated for HTR-PM Safety-DCS.

Customized safety-DCS Engineering prototype development lifecycle used in HTR-PM

Activities of the system safety lifecycle (as defined by IEC 61513)
2. HTR-PM DCS – system structure
2. HTR-PM DCS R&D-System Scale

<table>
<thead>
<tr>
<th></th>
<th>HTR-PM Safety DCS</th>
<th>HTR-PM NC-DCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Station</td>
<td>28</td>
<td>45</td>
</tr>
<tr>
<td>Cabinet</td>
<td>38</td>
<td>108</td>
</tr>
<tr>
<td>Input and output signal</td>
<td>3458</td>
<td>13679</td>
</tr>
<tr>
<td>Operator station</td>
<td>Total 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 in MCR *2</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>2 in RSS *2</td>
<td>5 ENG</td>
</tr>
<tr>
<td></td>
<td>4 in cabinet *2</td>
<td></td>
</tr>
<tr>
<td>Display</td>
<td>300</td>
<td>200</td>
</tr>
<tr>
<td>Safety functions</td>
<td>14 RTS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 ESFAS</td>
<td></td>
</tr>
</tbody>
</table>

- HTR-PM Safety DCS: simplified and reliable;
- HTR-PM NC DCS: enriched, completed functions, of similar scale to a ACPR1000 unit.
三. Engineering Prototype development Process

### Design
- NPP and system requirements
- Computer-based system requirements
- Computer system requirements
- Other components

### Development
- Protection system specification
  - Computer system design
  - HW system design
  - Structure design of cabinets and modules
- SW requirements
- HW requirements
- SW design
- HW design
- SW implementation
- HW realization
- HW integration
- Engineering prototype integration
- Function test
- Continuous running test
- EMC test
- Environment test
- Seismic test

### Qualification
- Protect system periodic test device
- Protection system integration test device

#### Protection cabinet X, protection cabinet y
- channel monitoring cabinet, safety display device
- signal isolation cabinet, safety control cabinet, ESFAC

#### Qualify control
- routine test report
- continuous running test report
- EMC test report
- Environmental test report
- Seismic test report
3. HTR-PM safety-DCS – overall requirement

1. Function requirements:
   Signal isolation distribution, reactor trip, engineering safety features actuation, MCR ventilation, post accident data monitoring

2. Structure requirement: 4 channels redundancy, 2 layers of 2/4 voting structure, with consistency logic, 2 diversity group in each channel.

3. Main performance:
   Response time: delay from monitoring variable signal input to ESFAS/trip actuation signal output (ESFAC side) ≤ 300ms
   Analogue acquisition precision: 0.1%
3. HTR-PM Safety DCS R&D – System Structure

- Signal isolation device
- Signal process device x/y
- Logic voting device x/y
- PAMS display
- Channel monitoring device
- Safety actuation device A/B
- MCR ventilation control

- Signal isolation cabinet
- Protection logic x/y cabinet
- Channel monitoring cabinet
- MCR ventilation cabinet
- Safety actuation cabinet
- Safety display unit
2. HTR-PM DCS – equipment List

Including: Isolation, IO signal, control & protection arithmetic equipment, safety display and control equipment, safety communication network, communication gateway, power supply, cabinets. 42 HW equipment, 15 mechanical equipment, 13 Software, 70 in total.
3. HTR-PM Safety DCS Development - Equipment Technical Features

- In accordance to safety I&C standard: SW design: HAD102/16, IEC-60880, HW design: IEC-60987
- Deterministic software: No Commercial OS, break is not used in the normal running. Fixed Memory allocation, Fixed task scheduled
- Reliability design and analysis through the whole process
- Point-to-point communication technology
- High-coverage self-diagnostic design technology
- Safety information display design technology without commercial OS.
3. Safety DCS – Software V&V

- Responsible by INET;
- V&V implemented in all phases of safety SW life cycle;
- in accordance with IEEE 1012, L4 (the highest);
- executed under the principle of three independence

<table>
<thead>
<tr>
<th>Stage</th>
<th>Nun</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic design</td>
<td>186</td>
<td>closed</td>
</tr>
<tr>
<td>Software Req.</td>
<td>16</td>
<td>closed</td>
</tr>
<tr>
<td>Software architecture Design</td>
<td>18</td>
<td>closed</td>
</tr>
<tr>
<td>Software detail design</td>
<td>21</td>
<td>closed</td>
</tr>
<tr>
<td>Unit test</td>
<td>44</td>
<td>closed</td>
</tr>
<tr>
<td>System test</td>
<td>8</td>
<td>closed</td>
</tr>
<tr>
<td>Total</td>
<td>293</td>
<td>closed</td>
</tr>
</tbody>
</table>
3. HTR-PM Safety DCS

Equipment Qualification Process
3. HTR-PM Safety DCS - Equipment qualification Progress

2013-9-24 鉴定大纲专家会
Qualification plan expert review

2014-3-24 环境试验通过
Environmental test passed

2014-5-28 EMC试验通过
EMC test passed

2014-7-8 抗震试验通过
Seismic test passed

HTR-PM 安全级控制保护系统设备鉴定大纲专家评审会

评审意见

2013年9月24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“HTR-PM 安全级控制保护系统设备鉴定大纲”专家评审会。

与会专家在听取了广利核公司对HTR-PM 安全级控制保护系统工程样机研制、设备鉴定大纲的工作汇报基础上，经过充分讨论，形成如下意见：

1. HTR-PM 安全级控制保护系统设备鉴定大纲文件内容完整，设备鉴定标准选取、鉴定试验项、试验顺序、试验等级符合核安全级仪控设备鉴定相关法规和标准要求；

2. 鉴定试验样机的典型性分析合理，所选取的鉴定试验样机及配置对HTR-PM 安全级控制保护系统设备具有代表性；

3. 针对国内典型物项（COTS）的鉴定原则满足核安全级仪控设备鉴定法规和标准及工程应用要求。

与会专家认为可在《HTR-PM 安全级控制保护系统设备鉴定大纲》基础上，开展后续工作。
3. HTR-PM Safety DCS – Progress

Engineering prototype qualification tests finished.
Go all out to ensure the actual system delivery!

![Diagram showing project progress]

- Finished task
- On going task
- Not started task

2015 SEP.
4. HTR-PM non-safety DCS R&D-Overall Requirement

Function requirements:
Non-safety DCS is used to monitor operation, control and analyze data of reactors, BOP, CI, DEH, and DAS.

Main performance:
- Min. control cycle ≤ 50ms
- SOE time resolution ≤ 1ms, inter-station SOE time resolution ≤ 2ms
- System availability ≥ 99.99%
4. HTR-PM NC-DCS-system structure
4. HTR-PM NC-DCS-HOLLiAS-N

HOLLiAS-N:

- **Software NPP specialized function:**
  - HMI system compatible with nuclear Human factor engineering standard
  - Alarm system compatible with IEC 62241
  - Digital procedure
  - Specialized graphic symbols, function block and SPDS calculation.
  - Authorization Management customized to NPP operator shift.

- **Hardware:**
  - Metal shell, increase anti-Seismic and EMC capability
  - Environmental adaption intensified
  - NPP specialized hardware: priority logic module, etc.
4. HTR-PM NC DCS - Progress

NC-DCS prototype:
In the end of 2011, the prototype was delivered to INET.

Actual NC-DCS:
Integration of software and hardware finished in this month. After 9 months of system factory test and factory acceptance test, The System will be ready to be delivered in Jul. 2015
5. Conclusions

HTR-PM DCS has been under execution for 5 years (2009-2014). It has taken CTEC 150 man/year so far. With close cooperation with INET, Chinergy and Shanghai Electric, CTEC overcame difficulties, like iterative design, voluminous customization work, new technology, and lacking of drawings. However, the accomplishment of the planned milestones prepared CTEC for the following work in HTR-PM DCS.
5. Conclusions

1. The 1\textsuperscript{st} integrated DCS, including safety DCS, non-safety DCS, DEH supplied by Chinese supplier. Rod control system and DEH are integrated in non-safety DCS. Simplified interface, integrated platform, and easy to use and maintenance.

2. CTEC obtained knowledge of 4\textsuperscript{th} generation HTR-PM digital I&C, key design technology, and enriched its DCS products by participation in HTR-PM. HTR-PM Safety DCS project provided valuable experience for CTEC’s development and application of FIRMSYS, a safety protection control system platform.

3. The qualification solution by customized HTR-PM safety DCS prototype helps simplify safety DCS design, V&V, qualification and safety review of the actual system, but results in some problems in system upgrade and maintenance. With the satisfactory application of FIRMSYS in 1000mw PWR and platform qualification, the future HTR-PM safety DCS could be provided based on a qualified safety DCS platform.
Thank you for your attention