

The design of RMT-based IOC redundancy at RCPI experimental platform in TMSR*

YIN Cong-Cong (尹聪聪)^{1,2}, ZHANG Ning (张宁)¹, LI Yong-Ping (李勇平)^{1,†},
HAN Li-Feng (韩利峰)¹, CHEN Yong-Zhong (陈永忠)¹ and GUO Bing (郭冰)¹

¹Shanghai Institute of Applied Physics, Chinese Academy of Sciences, Shanghai 201800, China

²University of Chinese Academy of Sciences, Beijing 100049, China

(Received December 16, 2013; accepted in revised form April 23, 2014; published online December 9, 2014)

In the RCPI (rod control and position indication) system prototype of the TMSR (Thorium Molten Salt Reactor) project, EPICS (Experimental Physics and Industrial Control System) was adopted as instrumentation and control software platform. According to long time running, high availability and safety for the system, RMT (redundancy monitor task) software package for Input/Output Controller (IOC) redundancy was employed, and the driver for redundancy control was realized. Test shows that the system could achieve IOC redundancy switch-over quickly and ensure the IOC running with long-term stability.

Keywords: Redundancy monitor task, EPICS, Thorium Molten Salt Reactor, Rod control and position indication

DOI: [10.13538/j.1001-8042/nst.25.060402](https://doi.org/10.13538/j.1001-8042/nst.25.060402)

I. INTRODUCTION

Instrumentation and control (I&C) system is a nerve center for reactor operation and monitoring, and it is important to ensure safety and reliability of a reactor. The controller hardware platform of RCPI (rod control and position indication) system prototype of TMSR (Thorium Molten Salt Reactor) project [1] is the Advanced Telecom Computing Architecture (ATCA), the availability of which can be 99.999% [2]. With the high-availability hardware, the system software plays a decisive role in the availability of the whole system. Building a distributed redundant system is an effective solution to improve system availability.

EPICS, which is based on standard server/client model and is of high performance and multi-platform supporting, is used worldwide to create distributed soft real time control systems [3, 4]. The basic types of EPICS are Input/Output Controller (IOC), the Operator Interface (OPI) and Channel Access (CA) route [5, 6]. EPICS was adopted in the International Thermonuclear Experimental Reactor (ITER) system in 2011 [7].

Due to high-availability requirements of an instrumentation and control (I&C) software platform of a nuclear reactor [8], RMT (redundancy monitor task) software package, developed originally at DESY (Deutsches Elektronen Synchrotron) [9, 10], was adopted for IOC redundancy solution. The RMT package modification and driver realization for IOC redundancy control were required. In this paper, a redundant IOC system communicating with PLC (programmable logic controller) is designed and performance of the EPICS redundant IOC is tested.

II. HARDWARE ARCHITECTURE

An overview of the EPICS-based RCPI system hardware architecture is shown in Fig. 1. It consists of a pair of IOC-s communicating with remote PLC via network. The upper order computer system of platform consists of 2 ATCA blade computers running Linux operation system, EPICS components and RMT software package.

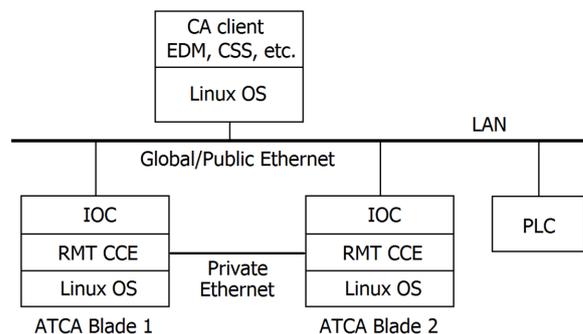


Fig. 1. Hardware architecture of the redundant ATCA/IOC in RCPI system.

The redundant ATCA/IOC pair share two network connections: public/global network and private network. Both are used for monitoring the state of health for each other. The private network connection is used to synchronize the backup to the primary, and the global/public network is used to communicate data from the primary to any other network clients requiring the data. The lower device of the platform is ABB AC-800M PLC component, which controls or monitors the rod operation and communicates with the IOCs by LAN.

III. SOFTWARE COMPONENT

The RMT software components [10] for realizing IOC redundancy purpose mainly includes: RMT main program, data-synchronization component CCE (Continuous Control

* Supported by the Strategic Priority Program of the Chinese Academy of Sciences (No. XDA02010300)

† Corresponding author, liyongping@sinap.ac.cn

Exec) and SNL (state notation language) Executive. The purpose of SNL Executive redundancy is to keep the state programs of the primary and backup synchronized and to select the node on which they execute. There are not state programs in our system, so SNL Executive is not introduced and this module shall be deleted in package optimization.

A. RMT

RMT is the core to realize EPICS redundant IOCs. It is used to gather and examine an overall condition of the IOC, establish and maintain communications with the partner through public/global Ethernet and private Ethernet and control CCE, I/O Driver, Scan Tasks, CA Server and others. The software architecture of RMT is shown in Fig. 2.

The main thread of RMT is a state machine, which defines six states. The state names and transitions are shown in Fig. 3. The state transition is determined by the information of configuration file, Primary Redundancy Resources (PRR) and shell commands. The parameters of RMT are set in configuration file in order to improve the program execution. The PRRs are public/global Ethernet, private Ethernet, I/O Driver, CCE, Scan Tasks, CA Server and others. Shell commands offer a route for operator to change the redundant state of IOCs and start/stop the RMT.

CCE, Device Driver and other components are controlled by RMT and share the same software interface defined in a header file. The RMT calls these functions in the interface by using an entry table to send commands to a driver instance or to get information from it. With the information from the configuration file, the driver instance and the partner, the RMT makes decisions about assuming or relinquishing control.

B. CCE

The main task of CCE is to keep database synchronization of the primary and backup. At CCE initialization, it creates Traverse Task and Exec Task, and calls `rmtRegister()` function to register itself in the RMT. The purpose of Traverse Task is to force a redundant update on every field. After the initial pass, the Traverse Task waits for a signal from the Exec Task to be triggered. The Exec Task attempts to connect the partner and monitors the TCP connection. It is a state machine, the state of which is determined by the command from RMT and the state of the connection to the partner. When a connection is established, each unit transitions state to "synching". They stay in this state until the master has completed sending a full update to the partner. Then the master and slave transit to "in sync state". In this state the master periodically transfers all fields that have changed.

IV. SYSTEM IMPLEMENTATION

A. The RCPI system design

From RCPI system prototype in Fig. 1, ATCA/IOC acts as the controller in the I&C system. Its device support module is a communication driver to ABB AC-800M PLC employed in the project via Modbus/TCP protocol, a fixed size data block that bundles many variables can be transferred, by this method, Control commands and measured value can be mapped between the PLC variables and IOC Process Value (PV) periodically over network for both directions. For multi-level high-availability insurance to the whole system, and the ATCA/IOC pair, the AC-800M PLC in this prototype system is redundancy configured, implemented by PLC vendor. The solution for the PLC pair includes CPU redundancy and channel redundancy. So the PLC pair and IOC pair are independent and switch-over happened in both side would not affect the other side.

B. The design of RMT driver

Redundancy control is to make redundant IOC pair's running status change with RMT state machine. And RMT package provides the same interface in header file "rmtDrvIf.h". The RMT driver mainly consists of several functions called by state machine if the redundant state needs to be changed or to be confirmed for both IOC units. According to engineering needs, functions for ATCA/IOC device support module are written as follows:

`start()`: If redundant state is "MASTER", the state machine would call this function to run the IOC and if this function is processed well, it will return 0.

`stop()`: If redundant state is "SLAVE", the RMT calls this function to pause the IOC and clients can't search for any Process Values from this IOC.

`testIO()`: This function could initiate a procedure to test the driver access to the I/O. With the result of `testIO()` function, the state machine could know whether the driver state is normal or not and determine state transition. This function is always called when error happened in MASTER IOC. If test result is OK the IOC would remain MASTER state, else switch-over would be happened.

`getStatus()`: This function periodically returns the status of the device support module of each IOC unit. The state machine could easily check if the I/O driver is health. If the driver state is abnormal, the RMT can increase a counter or call `testIO()` function and determine state transition.

By compiling the RMT software packet in EPICS environment and writing the redundancy control interface functions for ATCA/IOC called by state machine, the IOC pair realizes fast switch-over and data synchronization. For redundancy solution, it is advised that any redundant implementation should make the system more reliable than the non-redundant one, so the risk for RMT package failure or error should be considered and evaluated. RMT package is configured to start during IOC initialization, it checks the IOC configuration

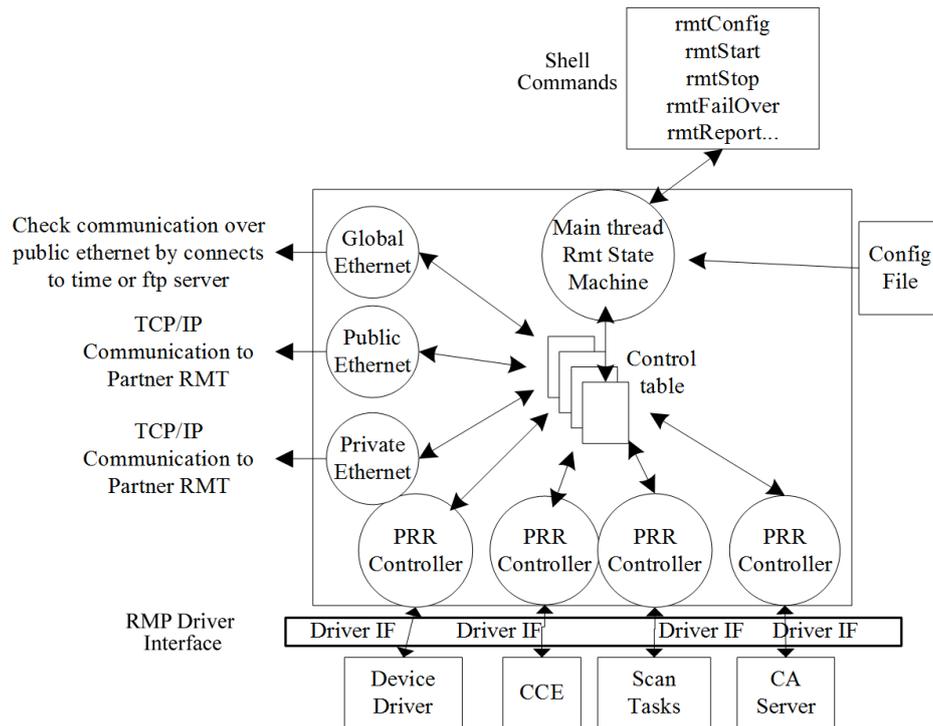


Fig. 2. The software architecture of RMT.

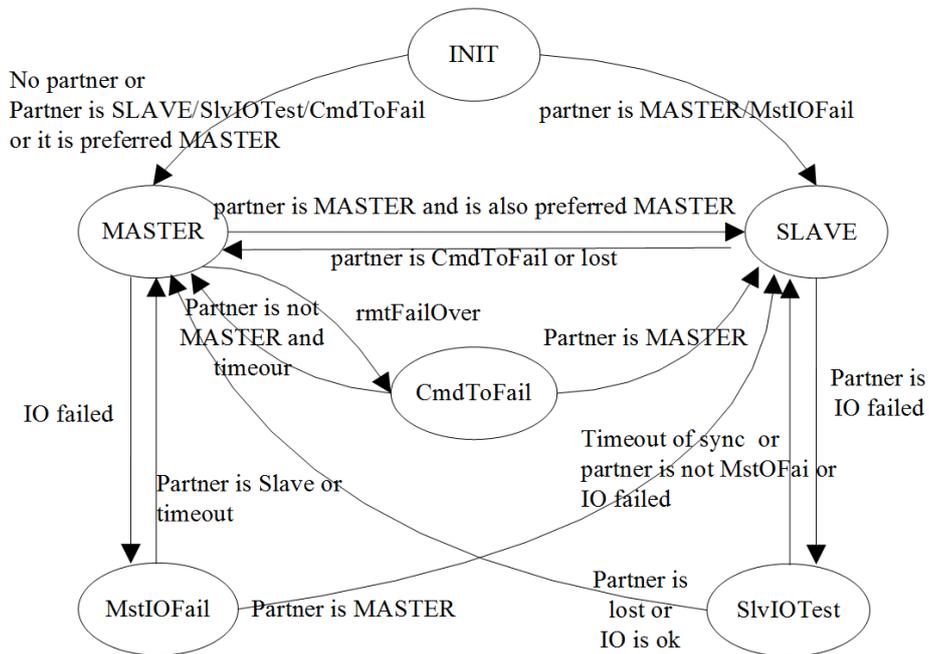


Fig. 3. The RMT state transition diagram.

and running status for both IOC units, and the state machine makes decision for unit redundant state. Normally, there is only one active IOC, if the RMT package fails or one connection breaks up, the redundant IOC pair will run as a single one.

V. REDUNDANT PERFORMANCE TEST

Redundant performance test includes the test for long-term availability and for redundancy switch-over interval. The system was running continuously with 198 records in IOC for

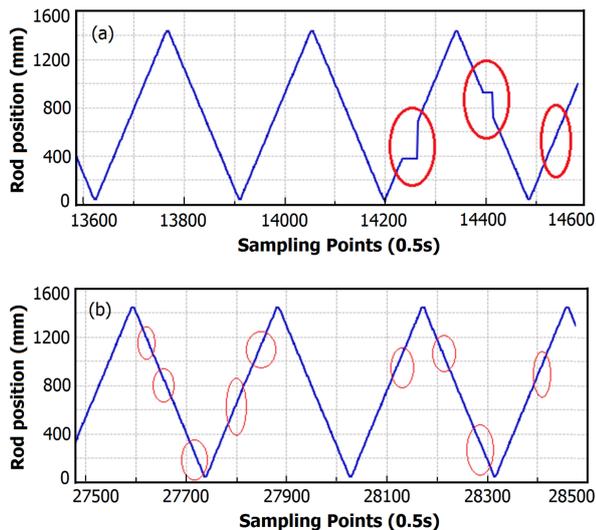


Fig. 4. (Color online) IOC redundancy switch-over before (a) and after (b) optimization.

about three months. The redundant system showed high availability and safety during the time switch-over optimization and testing.

IOC redundancy switch-over can be caused by failures of operator commands and master IOC caused by ATCA hardware or software problems. The implementation method of redundancy switch-over testing was to set control rod range of 1400 mm and speed of 30 mm/s, and to obtain rod position in real time by monitoring the rotating transformer through the Control System Studio (CSS) interface in a CA client terminal. Fig. 4(a) shows the IOC redundancy switch-over inter-

val under EPICS environment before optimization. The first and second switch-over were caused by IOC failure while the third one by operator command. The longest switch-over interval was about 8 seconds and caused by IOC failure.

It shows that the trace of switch-over by IOC failure is obviously in the curve. The switch-over time from CSS interface is too long, which is not allowed for the whole system, but in IOC layer the redundancy switch-over time is faster. It is speculated that this is a result of the CA timeout management mechanism, so the switch-over optimization mainly focuses on modifying the CA server's bacon period to client showing the server existence, and the client's reconnection period to server. If disconnection happens, the redundant pair's data synchronization frequency controlled by CCE increases. The switch-over interval after optimization is shown in Fig. 4(b). The first five switch-over events were caused by master IOC failure, and the last four events were caused by operator commands. The longest interval showed in Fig. 4(b) is less than 1 second in client CSS and this is much superior to the result in Fig. 4(a).

VI. CONCLUSION

ATCA/IOC redundancy in TMSR RCPI experimental platform has been implemented through modifying and configuring the modules of RMT and CCE and writing redundancy control driver for IOC support module. The system based on ATCA standard and IOC redundancy has high availability and could quickly realize the IOC switch-over and data synchronization. IOC redundancy solution would provide technical support for EPICS application for the future nuclear I&C. In future, we will optimize and test the switching time affected by network environment and data increase.

-
- [1] Jiang M H, Xu H J, Dai Z M. Bull Chin Acad Sci, 2012, **27**: 366–376
 - [2] PCI Industrial Computers Manufactures Group (PICMG). Advanced TCA. PCIMG 3.0 Short Form Specification, Jan. 2003.
 - [3] <http://www.aps.anl.gov/epics/>
 - [4] Hu Z, Mi Q R, Zhen L F, *et al.* Nucl Sci Tech, 2014, **02**: 020103.
 - [5] Han L, Chen Y, Zhou D, *et al.* Nucl Tech, 2013, **09**: 090603. (in Chinese)
 - [6] Ding J, Liu S. Nucl Tech, 2006, **05**: 380–383. (in Chinese)
 - [7] Wallander A, Abadie L, Di Maio F, *et al.* News from ITER controls—A status report. Proceedings of ICALEPCS 2011, Grenoble, France, 1–4.
 - [8] IAEA. Implementing digital instrumentation and control modernization of nuclear power plants. Vienna, International Atomic Energy Agency, 2009.
 - [9] Kazakov A, Furukawa K, Satoh M, *et al.* Higher availability with ATCA and redundant IOC. Proceedings of the 5th Annual Meeting of Particle Accelerator Society of Japan and the 33rd Linear Accelerator Meeting in Japan, Aug. 2008.
 - [10] Clausen M, Liu G, Schoeneburg B, *et al.* Redundancy for EPICS IOC. Proceedings of ICALEPCS 2007, Knoxville, Tennessee, USA, 158–160.