ONLINE SYSTEM UPGRADE ON CENTUM CS FCSs

ITO Hiroki [*1]   NISHIDA Jun [*1]   OHSAKO Satoru [*1]   YAJIMA Hideharu [*1]

We have developed the online system upgrade function for CENTUM CS FCSs[*2]. This function operates on hardware with a dual-redundant configuration and can upgrade the system software online. The control function only requires the system to pause for two seconds for upgrading. In conjunction with the existing online application data modification function, this function increases the maintainability and availability of DCSs[*3]. If applied to continuous process control, this function can significantly reduce maintenance costs. This paper describes the features, architecture and operations of the function.

INTRODUCTION

FCSs, the control stations in a CENTUM CS system, have already demonstrated that they are highly reliable, effective and maintainable. These advantages are the result of such features as the dual-redundant hardware configuration, the online modification of application data, and so on. Their excellent record in field operation is proof that they achieved this high level of reliability, effectiveness and maintainability.

On the other hand, the costs involved with maintaining these systems are increasing as the scale of plants grows larger and larger these days. Maintenance work is an extremely crucial factor for ensuring the quality and security of plants. Maintenance costs cannot therefore be readily cut.

The online system upgrade function has been developed with this in mind. Considering the close relationship of a plant with a DCS, it is evident that shutting down a DCS for maintenance work will shut down the entire plant. Maintenance work that does not require system shutdown may provide the solution to users' problem of increasing maintenance costs.

*1 Industrial Automation Systems Business Division
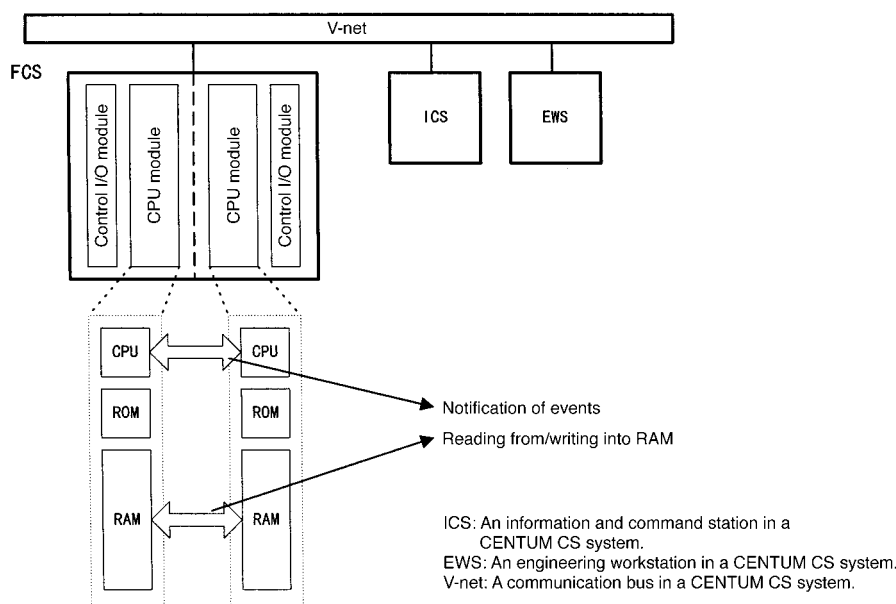*2 Field Control Station
*3 Distributed Control System

FEATURES

(1) Applicable Fields
   The system upgrade function is focused on continuous-control plants where its use is considered most advantageous.
(2) Online System Upgrades
   Systems can be modified while minimizing the effects on the plant under control. The system upgrade function requires the shutdown internal of control I/O updates to be shut down for about two seconds only when it makes changes to the system software.
(3) Objects Being Upgraded
   The object to be upgraded by the system upgrade function is the system software. The software covers most of the functions an FCS provides and, therefore, can deal with virtually all kinds of upgrade requests. The system upgrade function, when combined with the existing online application data modification function, will enable system upgrades to be made flexibly.
(4) Reliability
   The system upgrade function automatically checks conditions relevant to the system upgrades being made, thus ensuring the upgrades are achieved in a more secure way.
(5) Fail-Safe
   The system upgrade function provides a means to revert back to the previous state of the system while online upgrading is in progress or after the upgrading is complete.

Figure 1 Hardware Configuration

HARDWARE CONFIGURATION

Figure 1 illustrates the hardware configuration of an FCS. In order for the online system upgrade function to work, an FCS must have a dual-redundant hardware configuration as shown in the figure.

An FCS in dual-redundant configuration contains two units each of the CPU module and control I/O module. Each CPU module is equipped with a CPU, RAM and ROM—which are sufficient for a single CPU module to implement the required control functions. In addition, the CPU module has capabilities needed for dual-redundant configuration such as sending event messages to the CPU counterpart or reading from or writing into the RAM counterpart.

When the system is in dual-redundant operation, control I/O signals are delivered from only one of the control I/O modules. The control I/O module handling control I/O signals is referred to as the "control-side" module, while the other module is referred to as the "standby-side" module. Should the control-side module shut down for some reason, the standby-side module immediately takes over the control. In other words, an FCS in dual-redundant operation is able to continue control in the event of a module shutdown in the other side, without affecting control.

The online system upgrade function has been realized by taking advantage of the mechanisms needed to implement dual redundancy and the actions that take place when the system is dual-redundant.

For more information on the dual-redundancy configuration of FCSs, see Reference (1) that discusses it in detail.

SOFTWARE CONFIGURATION

Figure 2 illustrates the configuration of software relating to the system upgrade function.
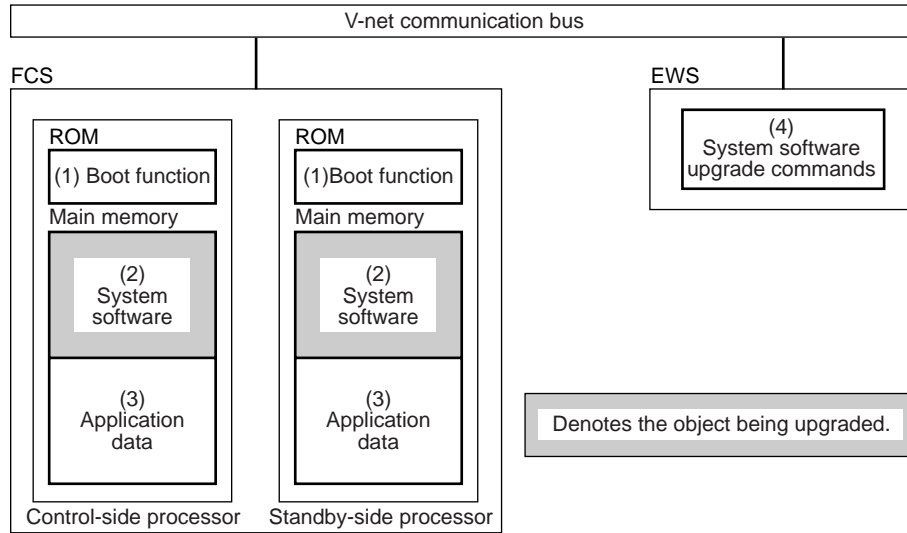
(1) Boot Function

The boot function is a program that executes the start-up (boot) sequence of an FCS. The same program is stored in the ROMs of CPU modules in both lines; these programs can run independently of each other. The boot function is the first among all functions to start working when the module comes into operation. The function is responsible for loading the system software and application data, starting the system software and duplexing the FCS, and so on.

(2) System Software

The same system software program is loaded into the RAMs of CPU modules in both lines. These programs are started from the boot functions and run independently of each other. When in dual-redundant operation, however, these programs run in conjunction with each other. The system software contains most of the functions provided by the FCS, including the operating system, duplexing process, communication bus process, and control I/O process. The purpose of the online system upgrade function is to upgrade these system software programs online. For details on how the system software behaves in relation to dual-redundant control, see Reference (1).

(3) Application Data

The application database is used with the control functions. The data contain computing parameters and the control I/O setpoints and are updated constantly by the system software. In an actual application, control I/O signals are handled by the control side only. However, because of the dual-redundant

```
┌─────────────────────────────────────────────────────────────────────────┐
│                      V-net communication bus                              │
└─────────────────────────────────────────────────────────────────────────┘
     FCS                                          EWS
   ┌─────────────────────────────┐      ┌──────────────────────────┐
   │ ┌──────────┐ ┌──────────┐   │      │    ┌──────────────────┐  │
   │ │ ROM      │ │ ROM      │   │      │    │       (4)        │  │
   │ │ ┌──────┐ │ │ ┌──────┐ │   │      │    │ System software  │  │
   │ │ │(1)Boot│ │ │ │(1)Boot│ │   │    │    │ upgrade commands │  │
   │ │ │function│ │ │function│ │   │      │    └──────────────────┘  │
   │ │ └──────┘ │ │ └──────┘ │   │      └──────────────────────────┘
   │ │Main memory│ │Main memory│  │
   │ │ ┌──────┐ │ │ ┌──────┐ │   │
   │ │ │  (2) │ │ │ │  (2) │ │   │
   │ │ │System│ │ │ │System│ │   │
   │ │ │software│ │ │software│ │  │
   │ │ └──────┘ │ │ └──────┘ │   │      ┌──────────────────────────────┐
   │ │ ┌──────┐ │ │ ┌──────┐ │   │      │ Denotes the object being     │
   │ │ │  (3) │ │ │ │  (3) │ │   │      │ upgraded.                    │
   │ │ │Application│ │ │Application│ │   └──────────────────────────────┘
   │ │ │ data │ │ │ │ data │ │   │
   │ │ └──────┘ │ │ └──────┘ │   │
   │ └──────────┘ └──────────┘   │
   │ Control-side   Standby-side │
   │ processor      processor    │
   └─────────────────────────────┘
```

Figure 2 Software Configuration

control mechanism, the same application data as those of the control side are retained at the standby side. This mechanism makes it possible for the standby side to take over control without breaking the continuity (of operation). It is also necessary for the data to be continuous, in a time-series sense, even during system upgrading.

(4) System Software Upgrade Commands

Users can upgrade the system software using these commands. These commands enable online system upgrading to be carried out in an interactive manner. The following section describes how the online system upgrade function works.

OPERATION

1. How the Online System Upgrade Commands Work

To make it possible for users to carry out online system upgrading on their target FCS, the system software upgrade commands that run on an EWS must be started. These commands first determine whether online system upgrading can be applied to the target FCS. Table 1 summarizes the items checked by these commands regarding the target FCS. If all these items pass the checking requirements, the function carries out online system upgrading, following the procedure described in Subsection 5.2. While the upgrading is in process, users are asked if they want to advance to the next step. Thus, users can safely proceed with their work by confirming the condition of the target FCS. If, for

Table 1 Check Items for Online System Upgrading

Check Item	Verification
Hardware configuration	The FCS must be equipped with the hardware for dual-redundant configuration.
Boot function	The function must be the version having the online system upgrade function.
System software	The software must be the version having the online system upgrade function.
Operating status	The processors in both lines must be online and active.
Memory size	The RAM must have a enough free space for the new system software to be loaded.

some reason, users become unable to continue their work, the function takes interruptive actions appropriate for the current degree of progress in the system upgrading procedure.

2. How the FCS Operates

Figure 3 is the schematic representation of the procedure followed when online system upgrading is carried out, with the focus on the operations of the FCS.

(1) Initial Condition

Before online system upgrading can be carried out, the target FCS must be in a condition where the processors on both lines are online and active, and the application data are being updated.
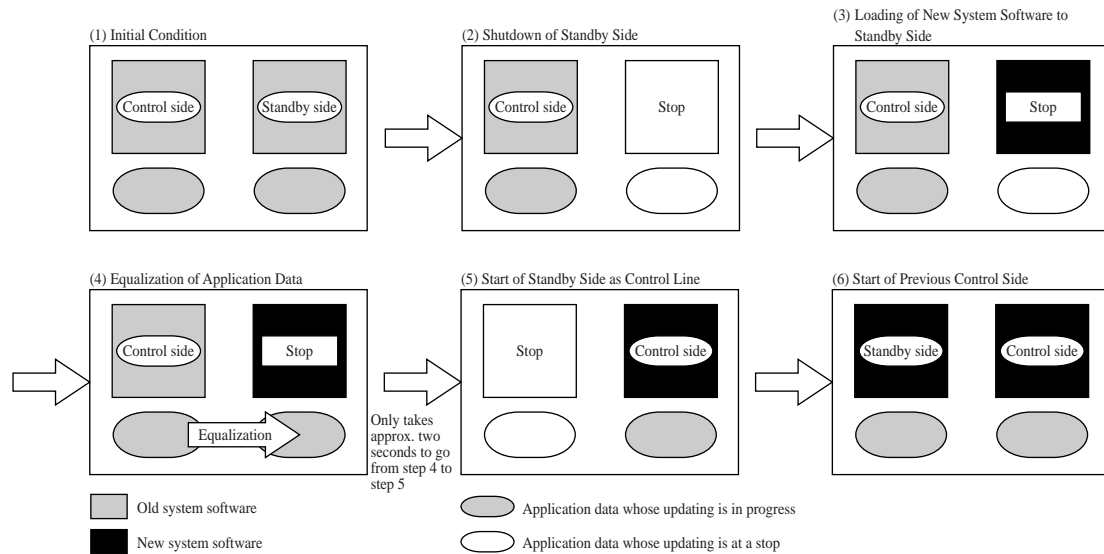
(2) Shutdown of Standby Line

The online system upgrade commands bring the standby-side processor to a stop via the V-net communication bus. This simultaneously stops the application data at the standby side from being updated. Since the control-side processor is still in normal operation, the control functions continue to work without affecting the objects being controlled at all.

(3) Loading of New System Software to Standby Side

The system software upgrade commands tell the standby boot function of the target FCS that it is time to start online system upgrading. Then, the commands start the boot function. Next, the commands and the active boot function cooperatively load the new system software to the standby-side RAM.

(4) Equalization of Application Data

The system software upgrade commands restart the standby boot function when the loading of the system software is complete. The active boot function copies the control-side application data, which are currently being upgraded, to the standby side. This copying is done in cooperation with the control-side system program in order to upgrade the standby-side application data that are no longer being upgraded. Since

(1) Initial Condition
(2) Shutdown of Standby Side
(3) Loading of New System Software to Standby Side
(4) Equalization of Application Data
(5) Start of Standby Side as Control Line
(6) Start of Previous Control Side

Only takes approx. two seconds to go from step 4 to step 5

Old system software
New system software
Application data whose updating is in progress
Application data whose updating is at a stop

Figure 3 Schematic Representation of Online System Updating

Table 2 Extra Actions Taken During the Startup Sequence after Online System Upgrading

Action	Description
Wind-up operation*	No wind-up operation is carried out.
MAN-mode fallback action**	No MAN-mode fallback action is taken.

* Denotes an operation mode in which no control I/Os are provided immediately after the start of initialization in order to tune the control parameters.
** Denotes an action in which the control status is forcibly brought to the manual mode as a result of failure detection.

the control side is in continuous control, the application data are still upgraded after the copying; these upgrades are equally reflected to the standby side by the hardware mechanism.

(5) Start of Standby Side as Control Line

When upgrading of the application data is complete, the standby boot function tells the control-side system software to shut down the control side. The system software in turn brings itself to a stop. The standby boot function, after having confirmed the shutdown of the control side, starts the system software that has already been upgraded to become the new control-side system software. The control I/Os are in a hold state for approximately two seconds—from the time of the previous control side shut down to the time that the previous standby side became the new control line. For this reason, the updating of application data stops temporarily, data values at that point are retained, and then updating resumes after two seconds approximately. The new control line, which is now active, avoids any action that may affect the continuity of control. This avoidance behavior is based on information provided by the boot function that advises that the new

control line will start after the online system upgrading. Table 2 summarizes the extra actions taken during the startup sequence after online system upgrading.

(6) Start of Previous Control Side

The system software upgrade commands start the previous control side as the new standby side. The active boot function then copies the new system software from the current control side to the previous control side so that it acts as the new standby side.

This completes online system upgrading.

CONCLUDING REMARKS

In this paper, we have discussed the features, configurations and operations of the online system upgrade function. We are confident that the inclusion of this additional function will improve the maintainability and serviceability of the CENTUM CS system and help users reduce their maintenance costs. To ensure the problem-free use of this online system upgrade function, users are requested to thoroughly discuss the system with Yokogawa engineers to fully understand the operations of the plant in question before online system upgrading is carried out. ◆

REFERENCES

(1) Matsuda, T., Sano, H., et al. "Fault-tolerant Design of Control Stations." Yokogawa Technical Report vol. 37, no. 4 (1993): 15-18.