SYSTEM GENERATION AND MAINTENANCE FUNCTIONS FOR THE ProSafe-RS SAFETY SYSTEM

SATO Masahito [*1] *KUWATANI Motoichi* [*1]

We have developed system generation and maintenance functions for our ProSafe-RS safety system which forms the core of safety instrumented systems (SIS). The system generation function is designed to create application logic (logic solver) accurately and efficiently using IEC61131-3 (IEC standard)-compliant function block and ladder diagrams which are most commonly employed in the safety instrumentation area. The maintenance function has a "maintenance override" function which allows easy maintenance and inspection from the CENTUM CS 3000 HIS without affecting the safety functions of the ProSafe-RS. In addition, it accurately informs the operator of the status of safety controllers (SCS) when a fault is detected, annunciating device or process faults before they prove fatal. Furthermore, the maintenance function is systematized to promptly restore normal operation in case of a system failure or process shutdown.

INTRODUCTION

The CENTUM CS 3000, a reliable distributed production control system, has been introduced worldwide with the objective of operating plants efficiently 24 hours a day, every day. The CS 3000 handles abnormal conditions in a plant appropriately and minimizes the chance of them developing into faults. In contrast, there is a growing need for safety instrumented systems (SIS) which comply with international safety standards and which, if an abnormal condition is detected that cannot be prevented by a production control system such as the CS 3000, shut down the plant without injuries or fatalities, damage to the environment, surroundings, equipment, or devices. Our safety system, the ProSafe-RS, has been developed to meet these demands. The ProSafe-RS shuts down a plant in response to a shutdown signal or activates fire protection and/or gas protection equipment; application logic (logic solver) is required in safety controllers (SCS).

The ProSafe-RS has a safety engineering function that allows the user to create application logic accurately and efficiently and download it to SCSs. Also, the ProSafe-RS's maintenance function includes a "maintenance override" function that allows easy maintenance from the CS 3000 HIS without affecting the safety functions of the ProSafe-RS. In addition, to check that SCSs have been operating without fail, an SCS maintenance support function provides alarm notification in the event of a fault, and then performs restoration or recovery accurately and efficiently. In this system, a PC equipped with both the safety engineering function and SCS maintenance support function is referred to as "SENG" (Figure 1).

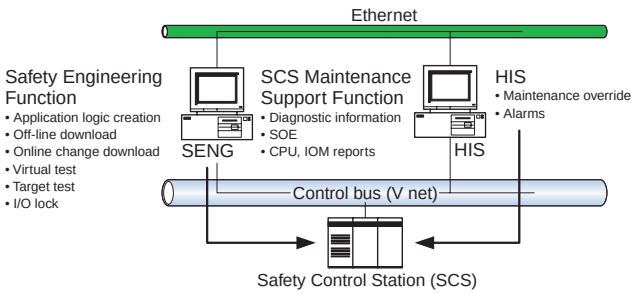

Figure 1 ProSafe-RS System Configuration

*1 IA Systems Business Division, IA Business Headquarters

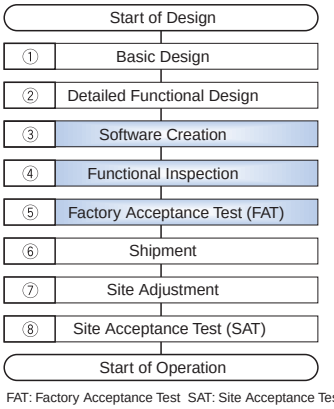

Figure 2 Engineering Procedure

SAFETY ENGINEERING FUNCTION

Figure 2 shows the general engineering procedure of the ProSafe-RS safety system. The ProSafe-RS safety engineering function was developed on the assumption that it is used in ③ software creation, ④ functional inspection, and ⑤ factory acceptance test (FAT) in Figure 2.

Features

To create and manage application logic accurately and efficiently, the software creation and functional inspection is implemented in the safety engineering function (Figure 3). This section discusses the main features of the safety engineering function in light of this procedure.

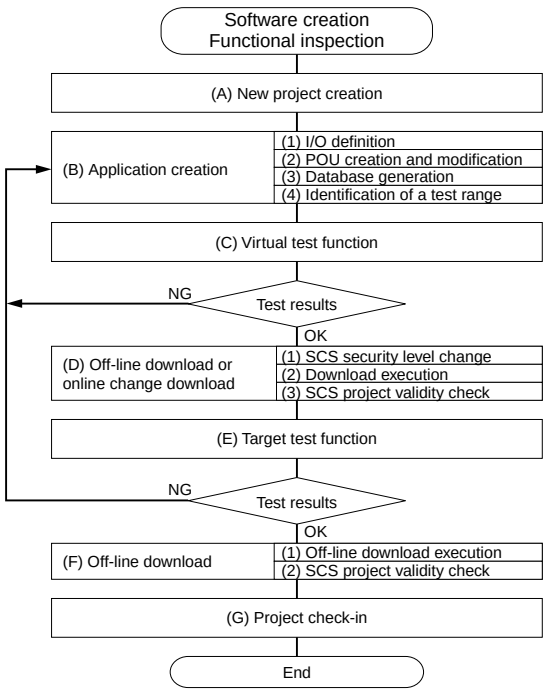

Figure 3 Software Creation and Functional Inspection Procedure

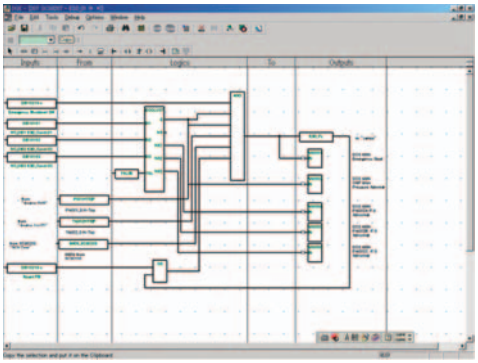

Figure 4 Multi-language Editor

(1) Adoption of the standard functions

Application logic is created using the compliant function block diagrams (FBD) and ladder diagrams (LD) of the IEC 61131-3 international standards. Particularly, the multi-language editor used to create FBDs allows description of FBDs so that the operations from input to output can be understood at a glance. In reality, the areas of Inputs, From (program organization units: POU input), Logics, To (POU output), and Outputs can be described by dividing them (Figure 4).

This flow chart is generally used in the SIS area and has the following features:

- FBDs created in the design phase can be input in a form almost as-is.
- Printout using the self-document function allows FBDs to be used as design documents as-is.

(2) Enhanced test function

The safety engineering function provides a function for testing FBDs/LDs using a standalone PC (virtual test) and a function for conducting tests using the SCS (target test).

In the virtual test function, the simulator for executing application logic is run on a PC, and the test function's screen operations, etc. have almost the same user interface (UI) for the virtual test and target test.

The test function allows application logic data-value referencing (online monitoring function) or setting (forcing

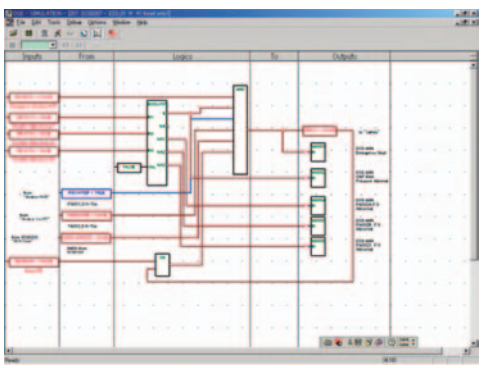

Figure 5 Example of a Test Window

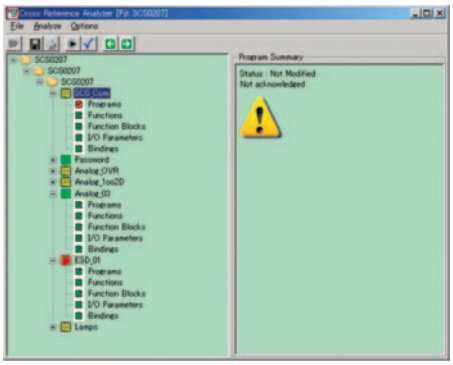

Figure 6 Example of Cross Reference Analyzer

function) and breakpoint setting or one-shot running (debugging function), etc. Figure 5 shows an example of online monitoring that displays true Boolean values in blue and false Boolean values in red.

(3) Online change

Application logic can be modified without stopping the SCS CPU (online change function). To test modified application logic accurately and efficiently, the modified areas and areas affected by the modification should be identified so that only the identified areas are tested.

This safety engineering function uses a tool known as "cross reference analyzer" (Figure 6) that automatically reports modified areas and affected areas. The cross reference analyzer can display modified application logic in red and application logic assumed to be affected by modification in yellow, thus confining the range to be tested. Application logic in green means it has not been modified or affected, and so no re-testing is required.

(4) Documentation

The self-document function allows created application logic, etc. to be printed on A3 with a specified footer, etc. assigned.

(5) Easy database management

The created application logic is managed for each database known as an "SCS project" on an SCS basis. For version management, the database can be history-managed accurately and efficiently on an SCS project basis.

MAINTENANCE FUNCTIONS

In order to perform safety functions properly, safety instrumentation systems must not be affected by other functions such as distributed control systems (DCS), yet they are required to be fully integrated with DCS HMI for operation and monitoring. The ProSafe-RS offers an SCS maintenance support function designed for SCS maintenance and the CS 3000 HIS function as a function intended for DCS operators.

SCS Maintenance Support Function

The SCS maintenance support function was developed to simplify SCS maintenance work. It has a user interface for identifying faulty areas easily and displays maintenance data required for analysis as diagnostic information messages (UI) in order of occurrence of events. This function allows maintenance personnel to act quickly in the event of SCS failure and promptly restore SCS.

The SCS maintenance support function incorporates a function for retaining maintenance-required data in an SCS internal memory and transferring it to a disk in the SENG as necessary. The SCS retains data required for maintenance work (such as diagnostic information, maintenance history, and SOE (Sequence of Event) data) in the SCS internal memory. This data is loaded as necessary into the PC as cache data. This feature is a message cache function (Figure 7), and it allows the data necessary for maintenance to be captured without fail even if the SENG has gone down.

The following shows the window for speeding up maintenance work (Figure 8).

(1) SCS status management window

The SCS status management window displays each module of the SCS hierarchically. For example, if an I/O module fails, a diagnostic information mark is assigned to the location of the I/O module concerned. Since the I/O module has a hierarchical structure, its higher-level node is also assigned a diagnostic information mark. This allows maintenance personnel to understand the presence or absence of failures, including low-level components, at a glance by simply observing the high-level hierarchy.

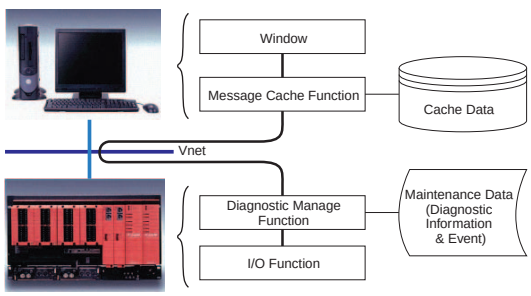

Figure 7 Message Cache Function

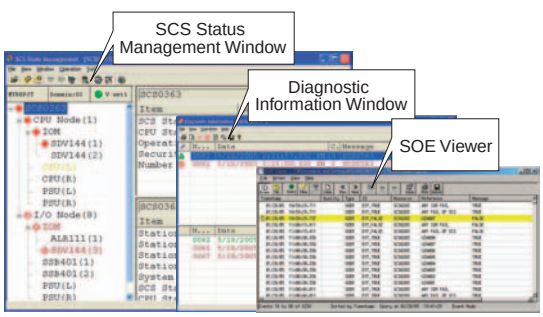

Figure 8 Window for Speeding up Maintenance Work

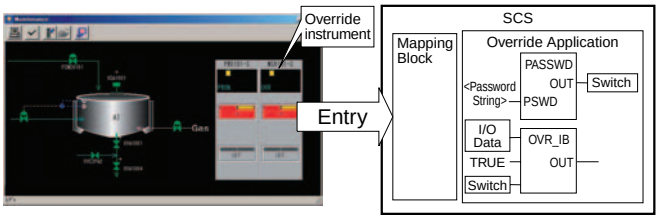

Figure 9 Overview of Maintenance Overdrive

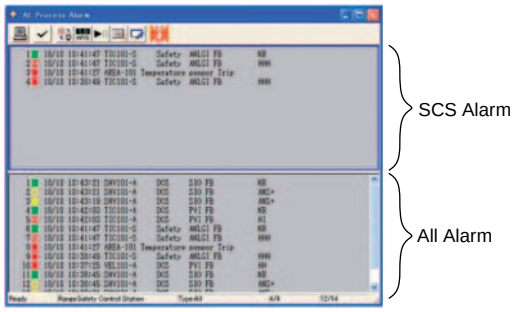

Figure 10 Integrated Display Alarm Window

(2) Diagnostic information window

This window displays the results of diagnosing the SCS itself, and information on maintenance performed in the SCS as a diagnostic information message. Maintenance personnel can check diagnostic information messages to see if work carried out in the SCS is correct. When the maintenance personnel checks and deletes a diagnostic information message, the corresponding diagnostic information mark is deleted from the SCS status management window, so the user interface allows the person to determine that SCSs are operating without failure. If a deleted message needs to be referred to again, pressing the Historical button displays the deleted diagnostic information message(s) in the lower view. This mechanism allows the maintenance history to be viewed easily.

(3) SOE viewer

The SCS has an event recording function that records operation history in order of occurrence. Execution history before and after a trip is stored in non-volatile memory in SCS, and can be uploaded to SENG so that the cause of tripping can be analyzed.

CS 3000 HIS's ProSafe-RS Support

The CS 3000 HIS is required to give SCS-output alarms prominence and to distinguish SCS tags and field control station (CS 3000 FCS) tags easily for the operator. This is because alarms output by SCS are important for maintaining the safety of the plant itself and they are more urgent than DCS alarms.

(1) Maintenance override

Figure 9 shows an application that fixes logic variables temporarily to separate safety-related device(s) (bypass input values from safety-related device(s)) and a window for using this application. Because the ProSafe-RS and CS 3000 are connected seamlessly on the V net, it is possible to display FCS and SCS tags on the same window. Therefore, maintenance personnel can separate safety-related device(s) by monitoring the entire system status on the window. Because this operation separates safety-related device(s), requested data in the communication frame is assigned CRC, so the validity of data can be checked on the SCS side from the safety point of view. This mechanism allows the SCSs to remove erroneous requested data.

(2) Alarm window

When the safety instrumentation system outputs an alarm, it is conceivable that a large number of alarms are also output from the DCS. Alarms output from the SCS are displayed in the upper views so that the operator can surely see them (Figure 10). This mechanism allows the operator to check alarms without overlooking the more urgent ones.

CONCLUSION

In this paper we have outlined the safety engineering function and maintenance function. It is crucial that these functions work accurately in the safety system. We intend to implement and develop functions for improving the efficiency of work and preventing misidentification or malfunction, features for coordinating with Plant Resource Manager (PRM) and plant engineering tools, etc. ◆

REFERENCE

(1) Sato Masahito, “Engineering Function on CENTUM CS 3000,” Yokogawa Giho, Vol. 43, No. 1, 1999, pp. 17-20 in Japanese

◆◆◆