INTEGRATED SIMULATION ENVIRONMENT FOR ProSafe-RS SAFETY SYSTEM

MURAKAMI Takeshi [*1] *MATSUDA Souichirou* [*1] *NISHIDA Jun* [*1] *OOSAKO Satoru* [*1]

In recent years it has become increasingly common for plants to be provided not only with the control layer of a production control system (DCS, etc.), but also with the protection layer of a safety instrumented system (SIS) to reduce the risk of industrial accidents.

The safety instrumented system is indispensable for avoiding risks to a plant failure. Inevitably, however, the system rarely operates in an actual plant and operators have few chances to use it, so a training system for operators has been strongly awaited. We have therefore developed a simulation environment that offers integrated training through which operators can learn how to handle both DCS and SIS properly in the event of a critical situation.

INTRODUCTION

In recent years it has become increasingly common for plants to be provided not only with the control layer of a production control system (DCS, etc.), but also with the protection layer of a safety instrumented system (SIS) to reduce the risk of industrial accidents. The safety instrumented system is indispensable for avoiding risks to a plant failure. Inevitably, however, the system rarely operates in an actual plant. We have therefore developed a simulation environment that offers integrated training through which operators can learn how to handle both DCS and SIS properly in the event of a critical situation.

Figure 1 shows an example configuration of an integrated system comprising a Yokogawa ProSafe-RS safety system and CENTUM (CENTUM CS 3000 and CENTUM VP) production control system[(1)].

*1 Industrial Automation Business Headquarters

ProSafe-RS INTEGRATED SIMULATION ENVIRONMENT

Figure 2 shows a ProSafe-RS and CENTUM integrated simulation environment configuration. A ProSafe-RS safety

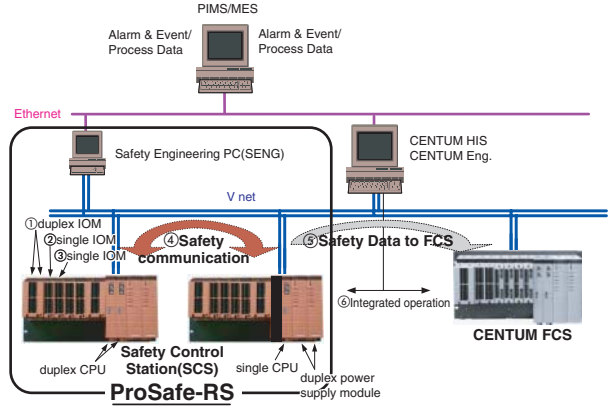

Figure 1 Example of a ProSafe-RS and CENTUM Integrated Production Control System Configuration

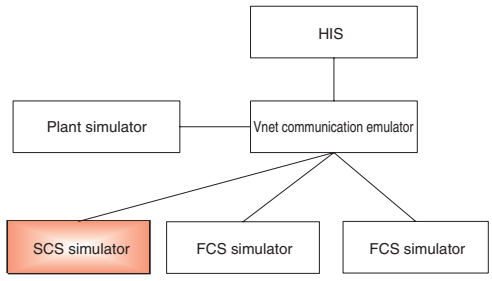

Figure 2 ProSafe-RS and CENTUM Integrated Simulation System

control station (SCS) simulator, a CENTUM control station (FCS) simulator, and a plant simulator (from Omega Simulation) that can simulate the dynamic characteristics of an actual plant are connected to each other via a communication bus Vnet emulator. This configuration enables the SCS simulator and FCS simulator to perform safety logic operations and control computations based on input data from the plant simulator, and output the results to the plant simulator. The plant simulator changes its internally held pressure, temperature, and other data according to dynamic characteristics equivalent to those of an actual plant. Since the SCS and FCS simulators can be operated and monitored from the CENTUM operation/monitoring station (HIS, or human interface station), these components can be combined to simulate the overall actual operation environment of a plant operation through the use of the DCS, SIS, and HIS for operators.

Since the SCS simulator, FCS simulator, and Vnet communication emulator are implemented on a PC and the internal conditions of the simulators are stored, they can be restored. For example, conditions immediately before a plant failure occurs can be stored and training for handling these critical conditions can be carried out repeatedly. The training simulator includes the DCS and SIS functions, so it is possible to carry out integrated training that otherwise would be impossible in an environment which comprises a combination of simulators from different vendors.

- HIS: CENTUM HIS (existing component)
- Plant simulator: OmegaLand (existing component)
- FCS simulator (existing component)
- SCS simulator (newly developed component)
- Vnet communication emulator (existing component)

SCS SIMULATOR

When designing an SCS simulator, we reused the FCS simulator software resource that is already available for CENTUM.

Specifically, we took the application execution function (safety logic engine) from the SCS (actual device) and implement it on the FCS simulator (Figure 3).

We used the FCS platform for the SCS (actual device) and partially modified the operating system to meet the safety

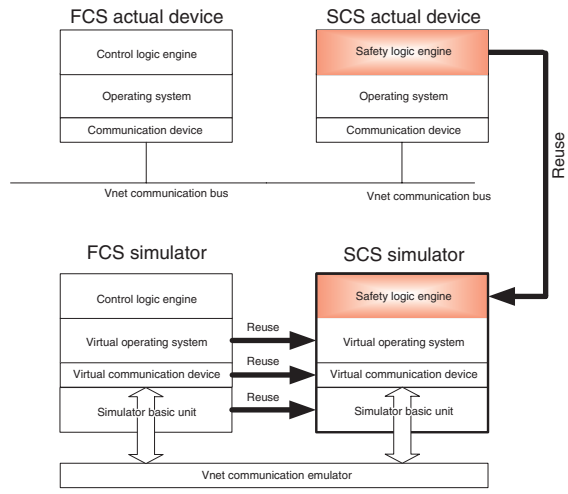

Figure 3 FCS Simulator and SCS Simulator

requirements. Since self-diagnosis of the SCS actual device hardware is out of the scope of simulation, we did not implement these modifications in the "virtual operating system" shown in Figure 3, and instead used the virtual operating system of the FCS simulator as is.

Since the communication device is basically the same in both the FCS and SCS, the "virtual communication device" of the FCS simulator can also be used as is.

ENGINEERING FUNCTION

For ProSafe-RS, operations are already integrated in the actual device environment, whereas the engineering has not been integrated yet. Each of ProSafe-RS and CENTUM has, therefore, an engineering function with a totally different architecture. To ensure an integrated simulation environment is implemented in these conditions, two different architectures need to work in a coordinated manner. We therefore designed so that the SCS simulator is started from the ProSafe-RS engineering function via the CENTUM test function (Figure 4). This design enables the SCS simulator to be started from both the ProSafe-RS engineering function (SENG) and CENTUM engineering function (System View). That means both the CENTUM engineers and ProSafe-RS engineers can use the SCS and FCS integrated simulation environment. Moreover, since this structure internally uses the CENTUM test function from within the ProSafe-RS engineering function, the operation user interface such as that for starting and stopping the SCS simulator is common with that of CENTUM, thus the operation procedure of the test function has been shared for ProSafe-RS and CENTUM.

The SCS simulator is connected with the HIS and ProSafe-RS engineering function via a Vnet communication emulator that is provided by the CENTUM simulation environment. This enables the performing of an online change download for the SCS simulator, debugging of the application logic design, or the performing of the same operations as those of the actual SCS device from the ProSafe-RS engineering function.

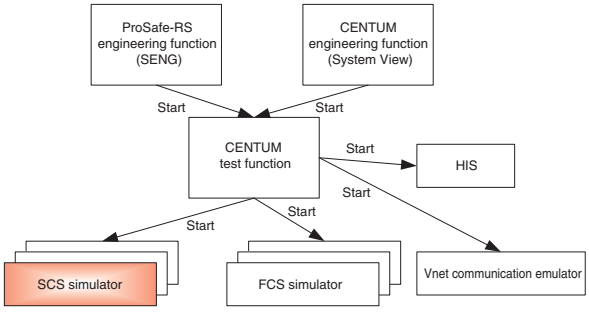

Figure 4 Engineering Functions and Simulators

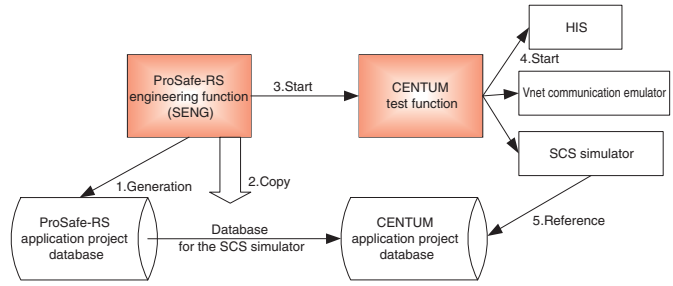

Figure 5 Reduction of Adverse Impact from CENTUM to ProSafe-RS

KEY POINTS ON SAFETY STANDARDS CERTIFICATION

ProSafe-RS is a product conforming to the international safety standard IEC61508. The integrated simulation environment described in this paper is software running on a PC. However, to release it as part of ProSafe-RS, the IEC61508 safety certification needs to be obtained. What is important in obtaining the safety certification is to ensure that the safety function (the shutdown logic that is performed in the SCS) is not adversely affected.

Since the integrated simulation environment runs on a PC, no operation in the simulation environment has a direct impact on the SCS actual device.

As previously mentioned, however, the SCS simulator is started by the CENTUM test function. The CENTUM test function acquires the data necessary to execute the SCS simulator from the ProSafe-RS application project database and then calls up the SCS simulator. If the CENTUM software including the test function were to change the ProSafe-RS application project database on a PC, the SCS safety function would be subject to an indirect adverse impact.

To avoid such a risk, we designed so that the CENTUM test function does not directly refer to the ProSafe-RS application project database when it starts the SCS simulator (Figure 5). That means:

(1) The ProSafe-RS engineering function generates a database for the SCS simulator in the ProSafe-RS application project database.
(2) The ProSafe-RS engineering function copies the database for the SCS simulator to the CENTUM application project database.
(3) The ProSafe-RS engineering function starts the SCS simulator via the CENTUM test function.
(4) The CENTUM test function starts the HIS, Vnet communication emulator, and SCS simulator. When starting the SCS simulator, the test function informs the SCS simulator of the location of the database for the SCS simulator that is located in the CENTUM application project database.
(5) The SCS simulator refers to the database for the SCS simulator, the location of which is informed by the CENTUM test function, and executes its own control operation.

Thus the CENTUM test function can start the SCS simulator without knowing the existence of the ProSafe-RS application project database, which reduces the possibility of mutual interference.

Another problem concerning the safety standard certification is how to avoid the confusing of operation objects by the operation and monitoring function.

When the CENTUM test function is started, the HIS also starts in simulation mode. A visual means is provided for operators to clearly recognize the simulation mode by, for instance, displaying the window frame in red.

The ProSafe-RS engineering function (SENG) also has a function to operate and monitor the conditions of application logic performed in the SCS. Even when the CENTUM test function is started on the same PC while the SENG operates and monitors the SCS actual device, the operation and monitoring function of the ProSafe-RS SENG continues to communicate with the SCS actual device. That means the same PC is shared by a program running in simulation mode and a program running in actual device mode. When the CENTUM test function is started and the window frame turns red, it looks as if the SCS simulator performs operation and monitoring; however, the ProSafe-RS SENG actually operates and monitors the SCS actual device (Figure 6).

This may cause an error operation signal to be sent to the actual plant. A safety system is required not only to rely on the operation procedure of an engineering PC, but also to be protected automatically against such an event. We designed, therefore, so that the CENTUM test function cannot be started while the ProSafe-RS SENG is communicating with the SCS actual device. This prevents an operation signal from being sent to the SCS actual device accidentally when an operator had intended to operate the SCS simulator.

These safety measures enabled the whole ProSafe-RS product including the SCS test function to obtain the IEC61508 SIL3 certification.

APPLICATIONS OF ProSafe-RS AND CENTUM INTEGRATED TEST ENVIRONMENT

The integrated simulation environment is useful not only for the purpose of plant training, but also as a test environment for the

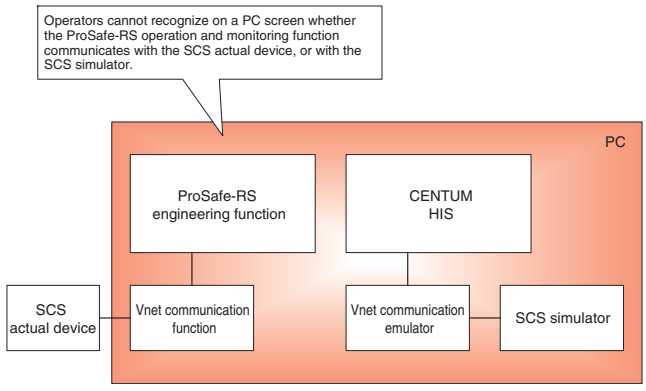

Figure 6 Confusion of Operation Objects by Operation and Monitoring Function

whole DCS and SIS system. Specifically, when the SCS simulator and FCS simulator communicate with each other, and the overall operation is controlled, all applications can be tested without any actual devices.

Previously, when each shutdown logic was tested to make sure it works correctly, plant error signal patterns had to be input manually for testing. This method is indispensable for testing each logic one by one systematically, but takes a lot of time and effort to verify the validity of the whole logic including the SIS and DCS.

The integrated simulation environment enables the plant simulator to generate error signals equivalent to those of an actual plant and verify the validity of the whole logic linkage including the DCS and SIS without the need to input error signal patterns manually.

CONCLUSION

The development of this integrated simulation environment will enable total operation training including a control layer and protection layer. These functions will help effectively improve operator skills and allow for training not only for routine operation but also for handling in the event of an accident. Moreover, since user applications in both the control layer and protection layer can be tested in an environment that is separated from the actual plant, engineering efficiency will be improved.

The further development of the simulation environment will make it possible to perform simulation training not only for routine plant operation but also for maintenance of both the production control system and safety instrumented system throughout the plant lifecycle such as plant startup, servicing and repairs, upgrading, and modifications. ◆

REFERENCES

(1) NISHIDA Jun, “Aims and Features of the ProSafe-RS Safety System,” Yokogawa Technical Report, No. 40, 2005, pp 35-38
(2) ODA Shinji, “Control Functions of CENTUM CS 3000,” Yokogawa Technical Report, No. 29, 2000, pp 15-18
(3) KUMAGAI Hiroshi, WAKASUGI Hiroshi, “CENTUM CS 3000 Operator Training System,” Yokogawa Technical Report, No. 31, 2001, pp 22-25

◆ ◆ ◆