AN APPLICATION STUDY FOR THE CLASS 1E DIGITAL CONTROL AND MONITORING SYSTEM

HIROYUKI FUKUMITSU
Nuclear Power Plant Department, EISC
MITSUBISHI ELECTRIC CORPORATION
Kobe, Japan

Abstract

This paper presents an application study for the Class 1E digital control and monitoring system to the next Japanese plants, especially about MMIS. The system architecture of hardware and software is also introduced, which will explain the strategic plan for the necessary software verification and validation according to the latest requirement from Japanese regulatory guide.

1. INTRODUCTION

The Man-Machine Interface System(MMIS)s in PWR plants employ the latest technology, such as human engineering, knowledge-based technology and computer technology in each generation, to reduce operator workloads and to reduce human error.

The first PWR, started its commercial operation in 1970, the first generation Main Control Board have been applied with many hardware switches, indicators. On the other hand, the latest Japanese PWRs employ microprocessor-based(digital) systems for reactor and turbine control and plant monitoring system. The next plants will also employ those proven technology for the Class 1E system; reactor protection system and MMIS.

At present time, the construction schedule of the next PWR plants is in the planning phase, however, the basic development of the digital Class 1E control and monitoring system has been finished. The digital systems have great advantage for the application to MMIS, for example, use of Visual Display Unit(VDU), improvement of system reliability and operability and reduction of maintenance workload and cost. From the view point of the recent regulatory guide, the application of the digital system for Class 1E control and monitoring system will require more investigation concerning plant safety, reliability analysis and verification and validation of software.

2. DESIGN APPROACH

2.1. CONSIDERATION FOR THE DIGITAL INSTRUMENTATION AND CONTROL SYSTEM

As the instrumentation and control system has the role of the center nerve in the nuclear power plant, I&C system was designed to have high reliability and safety from the beginning of the nuclear history.

At the time of construction of the newly designed PWR plant in Japan, we are trying to upgrade total I&C system design.

Digital technology, which is the major upgrading issue in the I&C system, have been applied step by step to Japanese PWR plants from portions of I&C system not important to safety to portions important to safety shown in Fig.1.

Fig.1 History of the I&C Technology

	1970's	1980's	1990's	2000's
Hardware Technology				
- Signal Processing	- Analog (Box Type)	- Analog (Card type)	- Digital (Non-Safety) - Analog (Card Type) (Safety)	- Digital
- Protection Logic	- Magnetic Relay	- Solid State Circuit	- Solid State Circuit	- Digital
- Control Sequence	- Magnetic Relay	- Magnetic Relay	- Digital (Non-Safety) - Solid State Circuit (Safety)	- Digital
Application of Digital Technology		- Rad Waste System	- Main Control System (Control rod, Pressurizer, etc.)	- Main Control Board - Safety System - Non-Safety System

In the next stage PWR plant, totally digitalized I&C system including Class 1E system and soft-operation control room are planned to apply to improve safety, reliability, maintainability and testability, and to reduce plant post.

This newly designed I&C system, especially the digital Class 1E system is carefully designed, and a large scale qualification test was carried out with cooperation of Japanese PWR/BWR utilities and vendors.*

2.2. DESIGN OF THE DIGITAL CLASS 1E CONTROL AND MONITORING SYSTEM

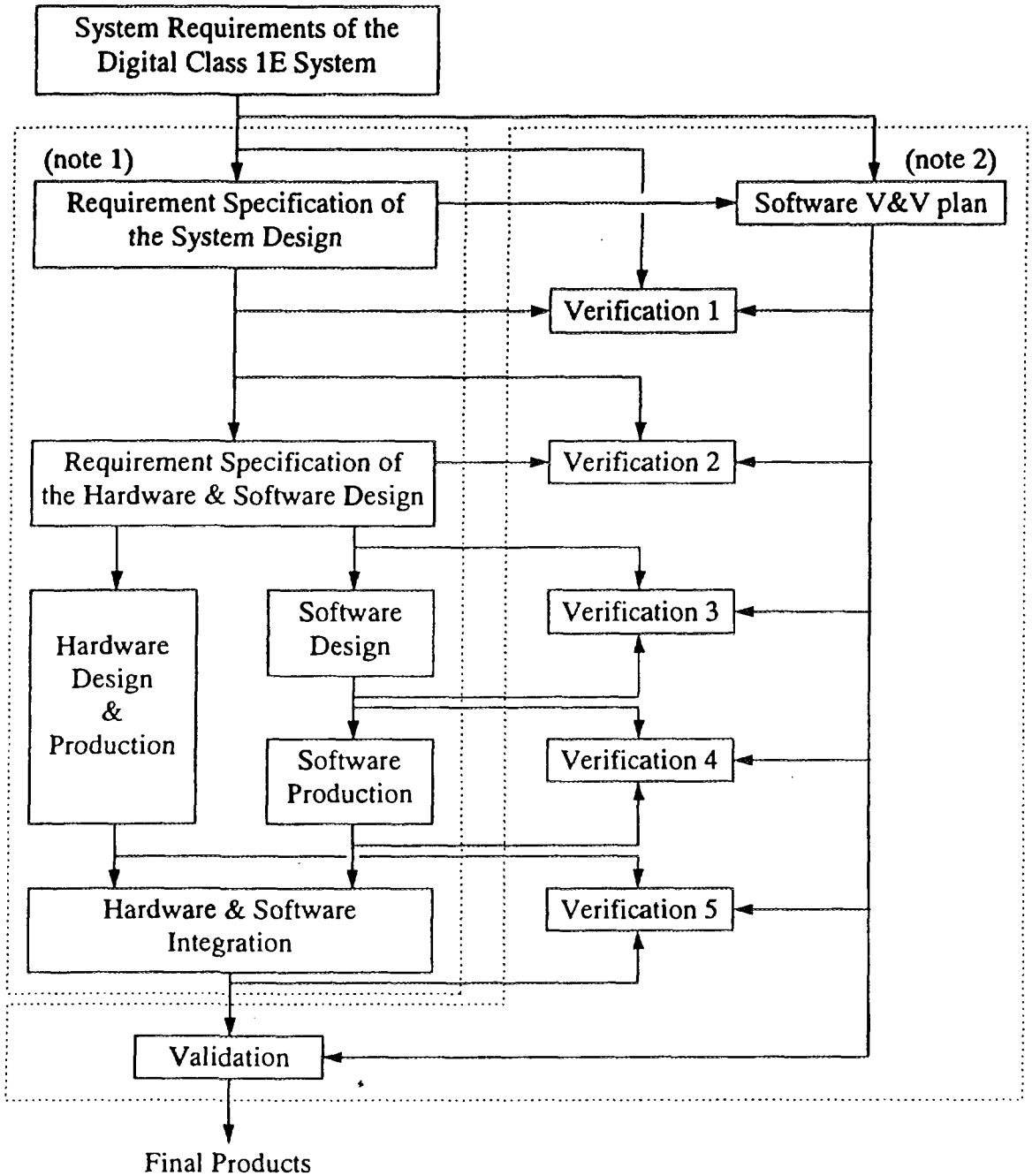
When we apply the digital technology into the Class 1E on system, we have to consider not only conventional design criteria but also newly started design criteria for safety software into design of the system.

Basically, the functional design of the digital Class 1E system is almost the same as the design of the conventional system and conventional design criteria is applied.

But, concerning about the software, recently started domestic design guideline (JEAG-4609) is applied to the design process and the V&V activity.

In this JEAG-4609, design and manufacturing process shown in Fig.-2 is defined and the V&V activity should be applied to each stage of design and manufacturing. (process in JEAG-4609 is similar to the process in ANSI/IEEE-7.4.3.2)

Fig.2 Verification & Validation Flow



Verification 1: Specification verification of system design requirement
Verification 2: Specification verification of hardware & software design requirement
Verification 3: Software design verification
Verification 4: Software production verification
Verification 5: Verification of hardware and software integration

note 1) ⋯ indicates the scope of design and production activity.

note 2) ⋯ indicates the scope of V&V activity.

2.3. CONSIDERATION IN THE ENVIRONMENTAL QUALIFICATION

Environmental withstand capability of the digital Class 1E system is considered in the design according to some domestic standard on seismic, radiation etc.

There are no domestic standard for EMI in the nuclear power plant, but based on some investigation and analysis for magnitude of the noise or surge in the nuclear power plant, we choose some standards about thunder impulse and electro-magnetic surge, and applied them in the qualification test. In addition, some conditions as seismic design are individually checked site by site.

There are no domestic standard for RFI in nuclear power plant also, but we carried out qualification test with some handy talkies used in operating nuclear power plants.

These EMI and RFI qualification is same as the qualification for the non-Class 1E digital I&C system in operating nuclear power plants, so judging from satisfactory operating experiences we think that these qualification is applicable to the digital reactor protection system.

2.4. CONSIDERATION IN THE DESIGN OF THE SOFTWARE

As mentioned before, reliability of the safety software is obtained by tough V&V activity.

But some design criteria shown below are applied to the software design itself to carry out the V&V activity effectively.

(1) Class 1E software should have single task architecture and execute the task in a fixed time interval. Interrupt operation should be inhibited.
(2) The system software which controls or manages the system operating mode should be separated from the application software which describes the function of each system.
(3) The system software should only have required features for the I&C system in the nuclear power plant. (dedicated system software for nuclear application should be used)
(4) The system software should have modular and structural architecture, and each module should be written in high level language.
(5) The application software should be written as combination of functional modules (sub-routines) which represent functional element of the I&C system of the nuclear power plant.
(6) Each functional modules should be written in high level language.
(7) Combination of the functional modules should be visible in a graphical image like CAD. Graphical symbols which represent functional modules are put on the CRT of software tool.

3. DESIGN

Documentation structure same as the conventional system will be applied to equipment specification of the digital Class 1E system.

Important specifications such as system functions, functional boundary between hardware and software, and system interfaces are described in composite block diagrams.

Structure of these diagrams are similar to the non-Class 1E digital applications in the operating plants and have sufficient experiences.

In this composite block diagram, function to be installed is described as the connection of graphical symbols which represent basic functional elements generally used in the design.

This approach enables easy understanding and review of the functions of equipment not only for experts of the digital I&C system but also for the people who has experiences in the conventional I&C system including operational staff or maintenance people.

This documentation is widely effective in the use of design, manufacturing, testing, operation and maintenance.

For the system software which determine basic system operation, the same software is used as the non-safety system in the operating plants which experienced intensive verification tests and sufficient experiences.

There are no need to change the specification of the system software for Class 1E application, so only required specifications for each Class 1E system are described in the specification documents.

3.1. SOFTWARE SPECIFICATION

Software specification of the application software is directly created from equipment specification described in the composite block diagram.

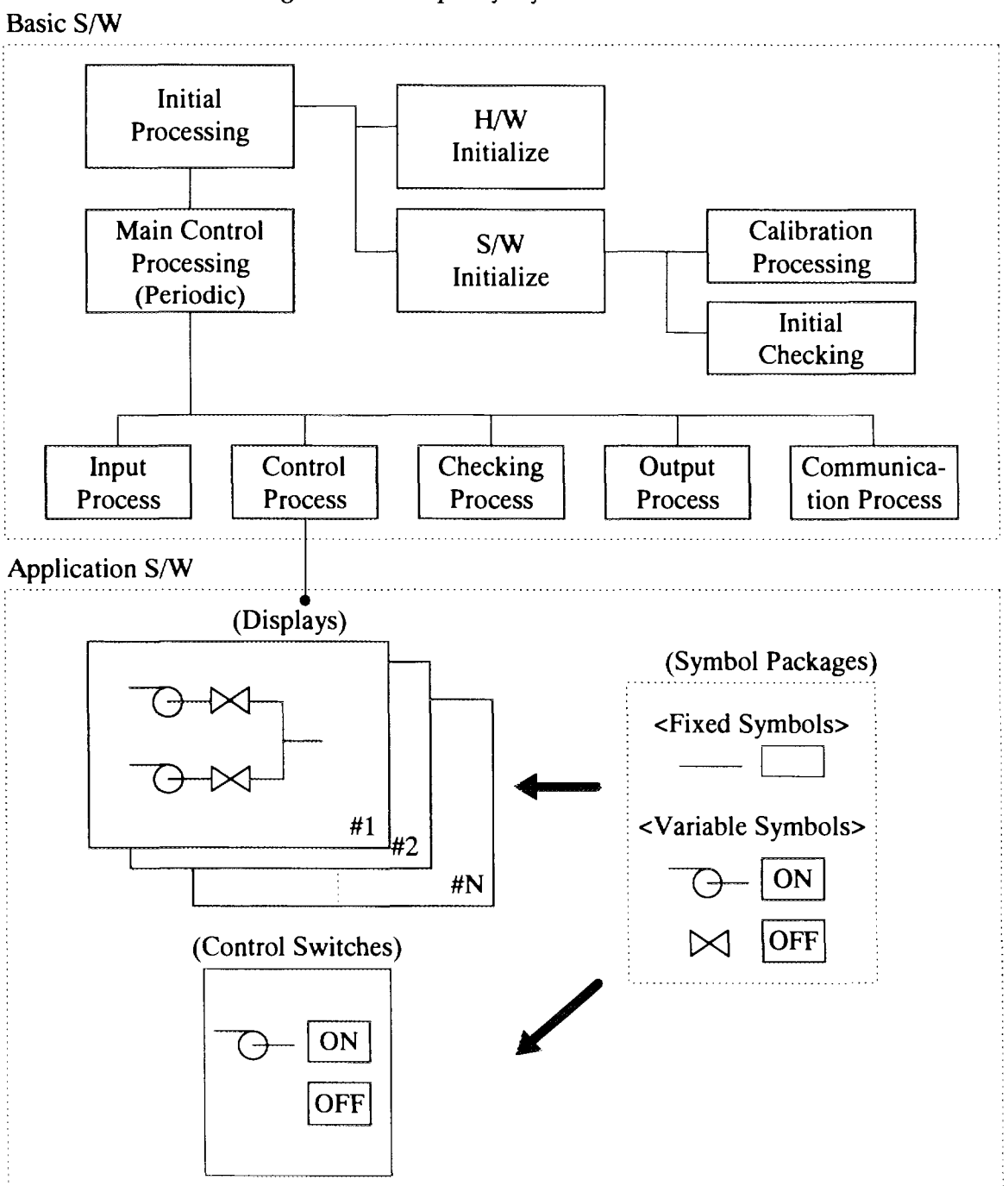
Software modules which correspond to the graphical symbols in the composite block diagram are connected together.

Programming of the application software is achieved at a software design/programming tool like a manner as CAD drawing tool to select each module symbols and connect them.

Completed application software is readable and reviewable not only by the designer of the software but also by the system designer and utility people.

This approach have been applied since the design of the software of the non-Class 1E application for the operating plants, and has sufficient experiences. Fig.3 shows an example of software architecture.

Fig.3 An example of software architecture



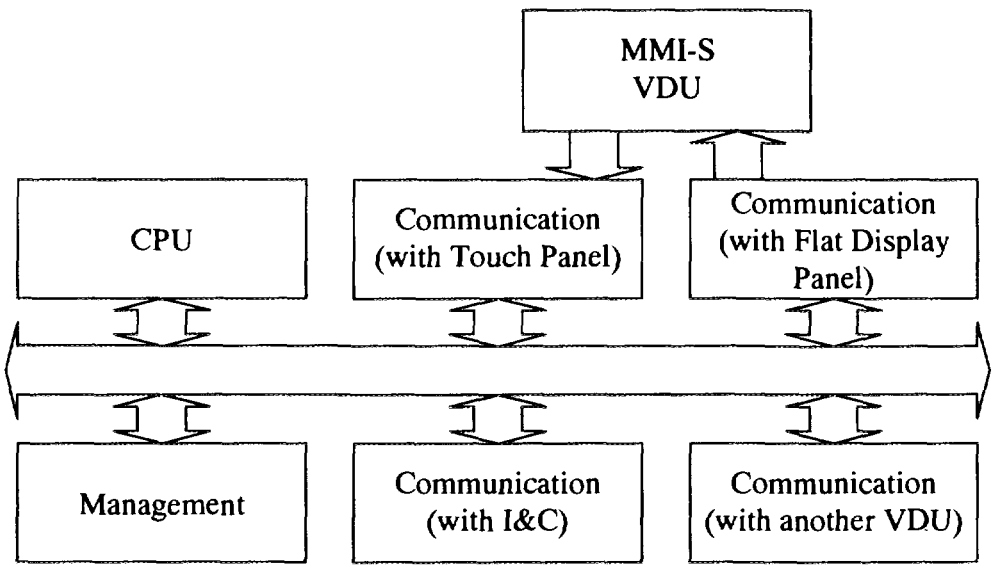
3.2. HARDWARE SPECIFICATION

As mentioned in section 2.3, several measures are alsotaken into the hardware specification.

- EMI/RFI
-seismic

The hardware configuration is shown in Fig.4 below.

Fig.4 An example of digital system for MMI-S



4. SOFTWARE TEST

In the software verification test, the software should be executed on the system which has the same configuration as the target system to verify system function.

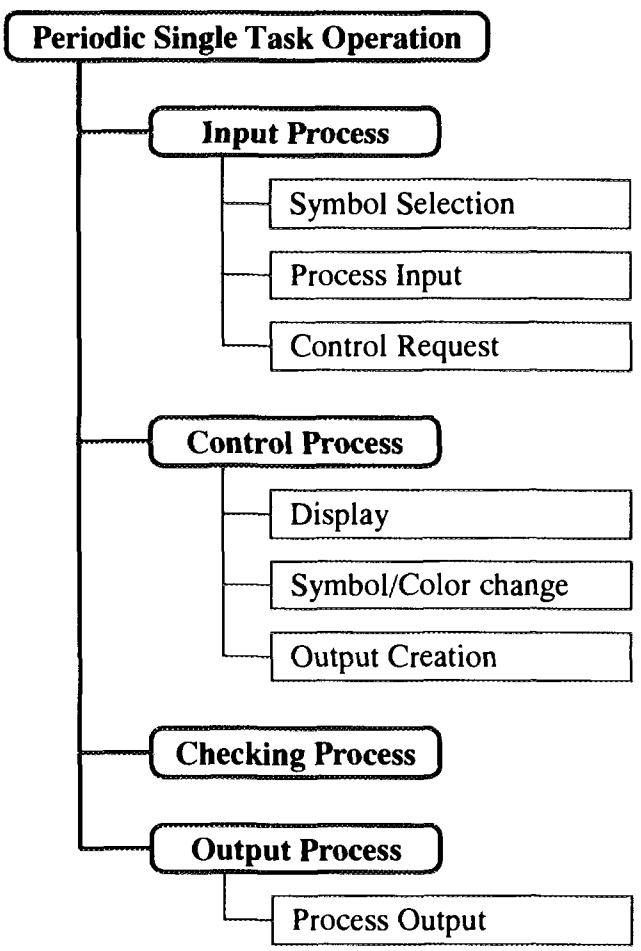
Module of the system software and functional modules are tested in the V&V activity through structural tests (white box tests) and functional tests (block box tests) carried out at object code level.

Total system function of the application software is verified using test bed which has the same configuration as the target system using simulated input signals.

System software of the digital Class 1E system is the dedicated one which is designed for the use of I&C system in nuclear power plants, and this system software operate in single task and fixed time interval without any interrupt operation.

So test condition is able to be established easily without any consideration for the timing of related signals and the operation of the target system to perform sufficient verification test with relatively small numbers of test cases. Fig.5 shows an example of testing procedure.

Fig.5 An example of testing procedure



REFERENCES

[1] INTERNATIONAL STANDARD, "Design for Control Rooms of Nuclear Power Plants", IEC-964.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION IEC STANDARD, "Software for Computers in the Safety Systems of Nuclear Power Stations", IEC-880.

[3] JAPANESE STANDARD, "Guideline of Computer Application for the Class 1E System", JEAG-4609.

[4] K. INUFUSA and others, "Total Instrumentation and Control Systems for Future PWR Plants", Mitsubishi Denki Giho, Vol.64, No.3, p.13-17.

[5] M. MATSUMIYA, "Steps toward Reliability Improvement in Electrical Instrumentation Equipment", Mitsubishi Denki Giho, Vol.69, No.9, p.2-5.

AN APPLICATION STUDY FOR THE CLASS 1E DIGITAL CONTROL AND MONITORING SYSTEM

(1) Digital technology, which is the major upgrading issue in the I&C system, have been applied step by step to Japanese PWR plants from portions of I&C system not important to safety to portions important to safety.

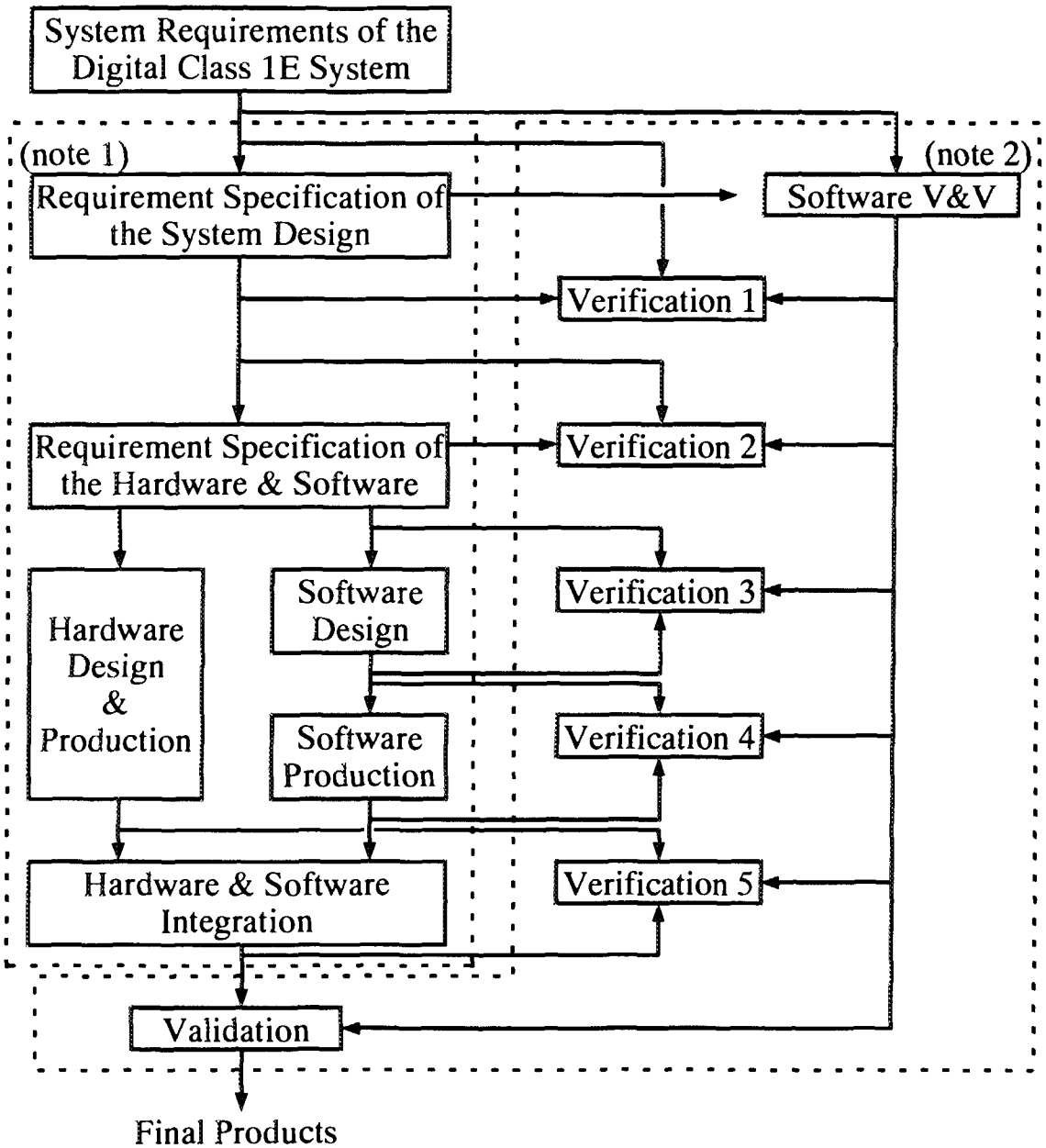
(2) Design and manufacturing process should be defined and the V&V activity should be applied to each stage of design and manufacturing.

(3) Software architecture applicable to V&V

(4) Simplified digital system for MMI-S

(5) Testing procedure of software

	1970's	1980's	1990's	2000's
Hardware Technology				
- Signal Processing	- Analog (Box Type)	- Analog (Card type)	- Digital (Non-Safety) - Analog (Card Type) (Safety)	- Digital
- Protection Logic	- Magnetic Relay	- Solid State Circuit	- Solid State Circuit	- Digital
- Control Sequence	- Magnetic Relay	- Magnetic Relay	- Digital (Non-Safety) - Solid State Circuit (Safety)	- Digital
Application of Digital Technology		- Rad Waste System	- Main Control System (Control rod, Pressurizer, etc.)	- Main Control Board - Safety System - Non-Safety System



Verification 1: Specification verification of system design requirement

Verification 2: Specification verification of hardware & software design requirement

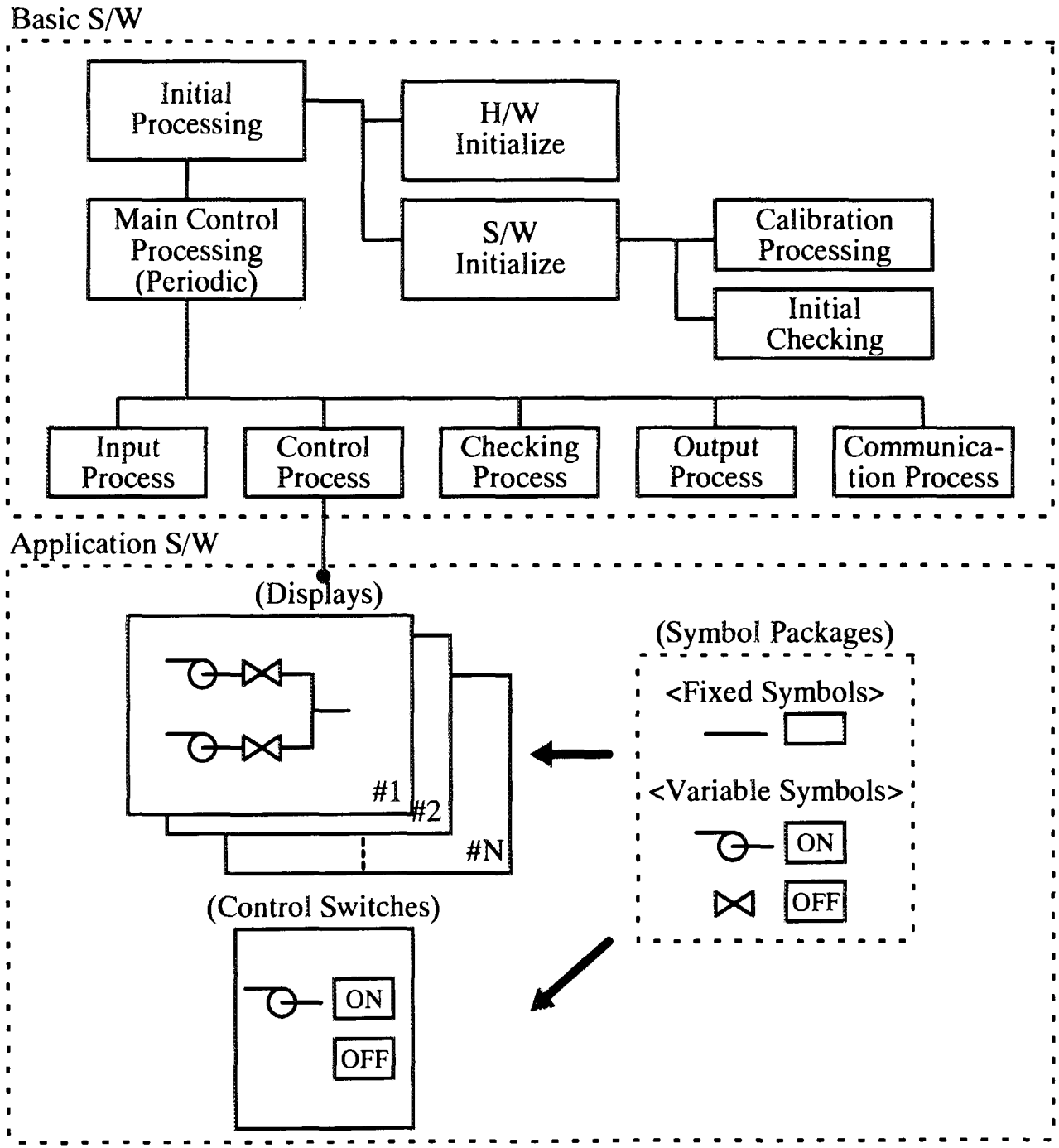
Verification 3: Software design verification

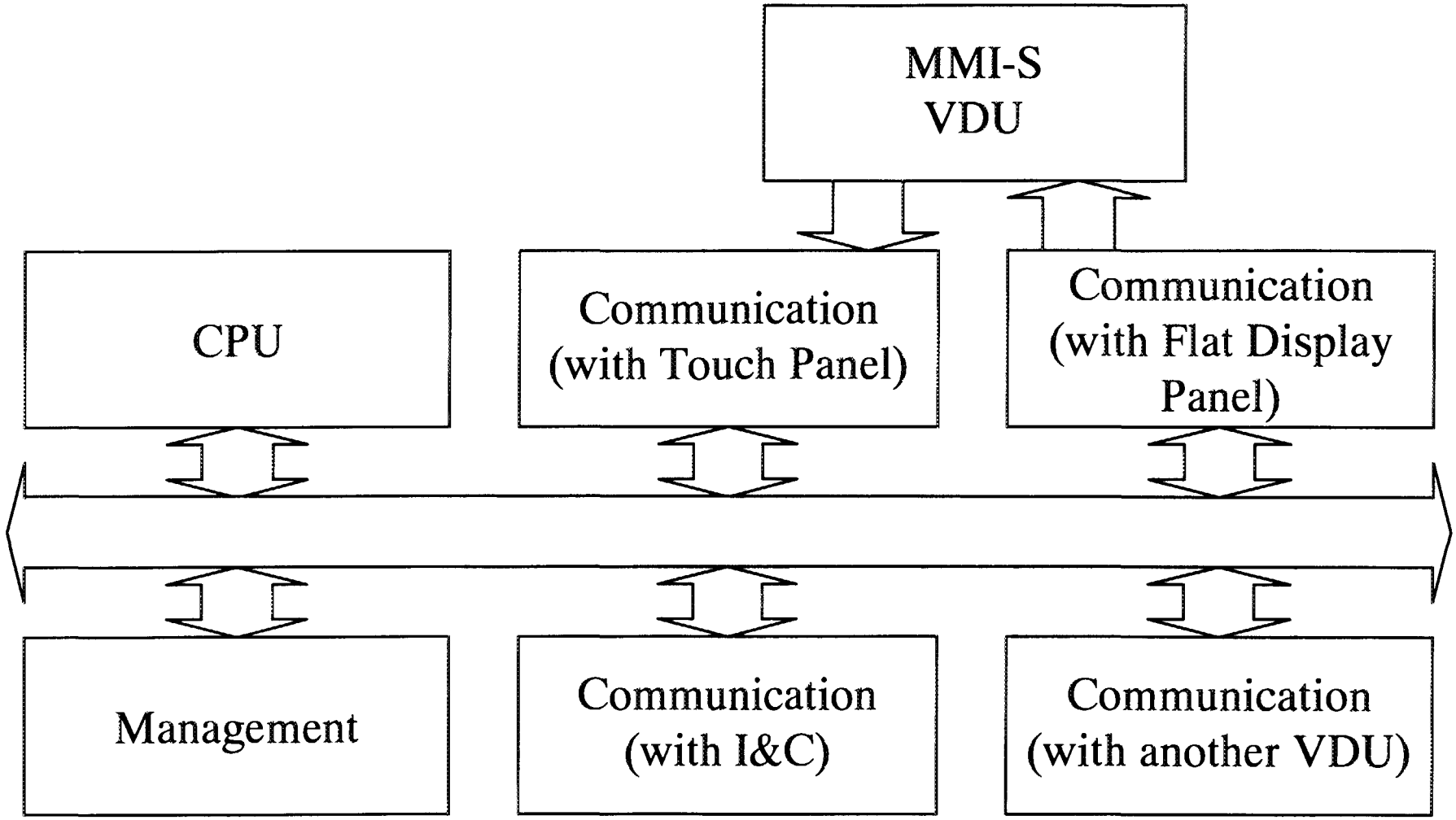
Verification 4: Software production verification

Verification 5: Verification of hardware and software integration

note 1) : : indicates the scope of design and production activity.

note 2) : : indicates the scope of V&V activity.


Basic S/W
Initial Processing
H/W Initialize
Main Control Processing (Periodic)
S/W Initialize
Calibration Processing
Initial Checking
Input Process
Control Process
Checking Process
Output Process
Communica-tion Process
Application S/W
(Displays)
#1
#2
#N
(Symbol Packages)
<Fixed Symbols>
<Variable Symbols>
ON
OFF
(Control Switches)
ON
OFF


MMI-S
VDU
CPU
Communication
(with Touch Panel)
Communication
(with Flat Display
Panel)
Management
Communication
(with I&C)
Communication
(with another VDU)