Workshop (L): **원자력시설의 인간공학기술 적용경험 및 현안**

SMART MMIS 인간공학 설계

2016. 10. 26.

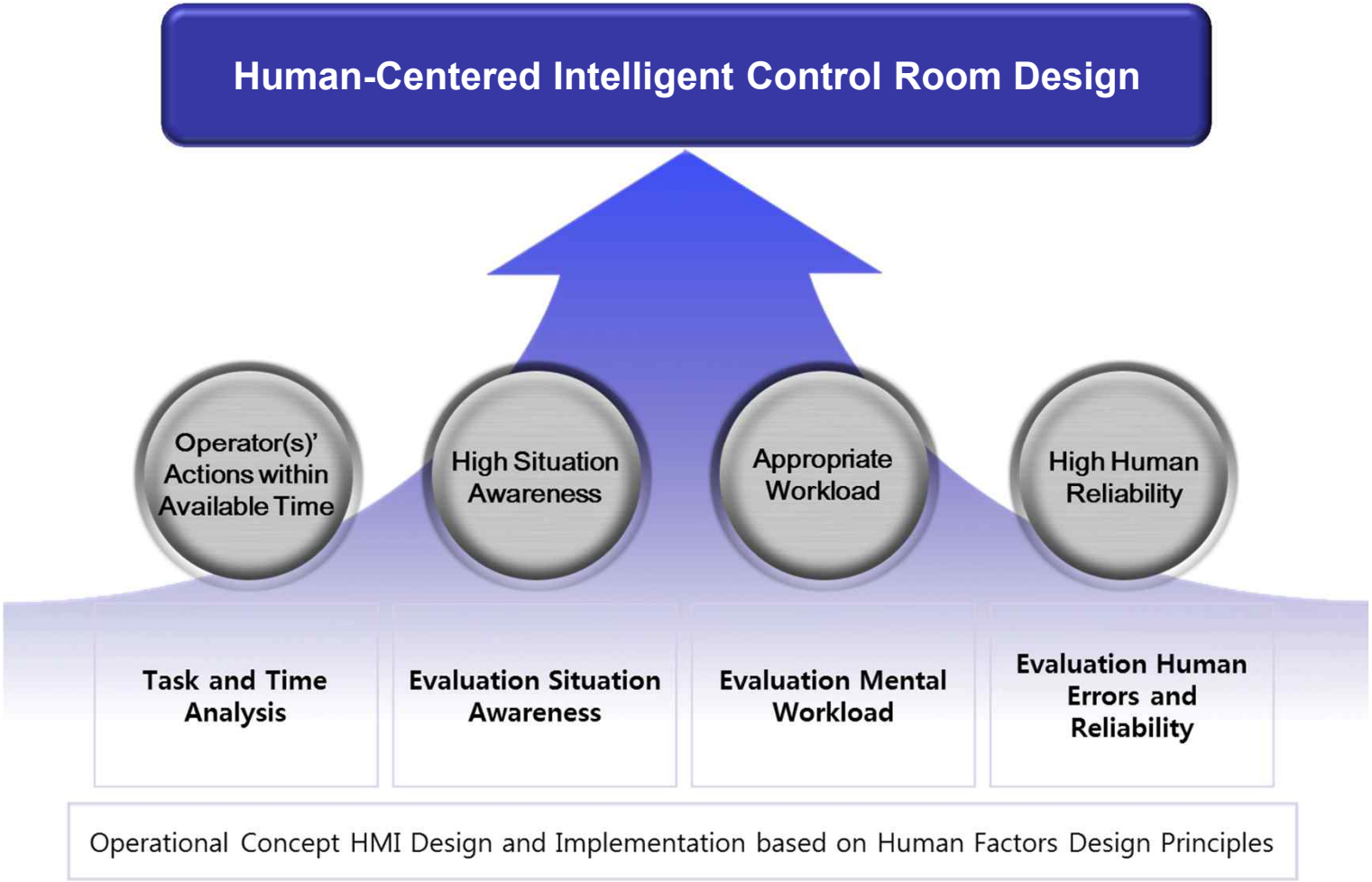
김사길

KAERI
Korea Atomic Energy
Research Institute

HFE Design

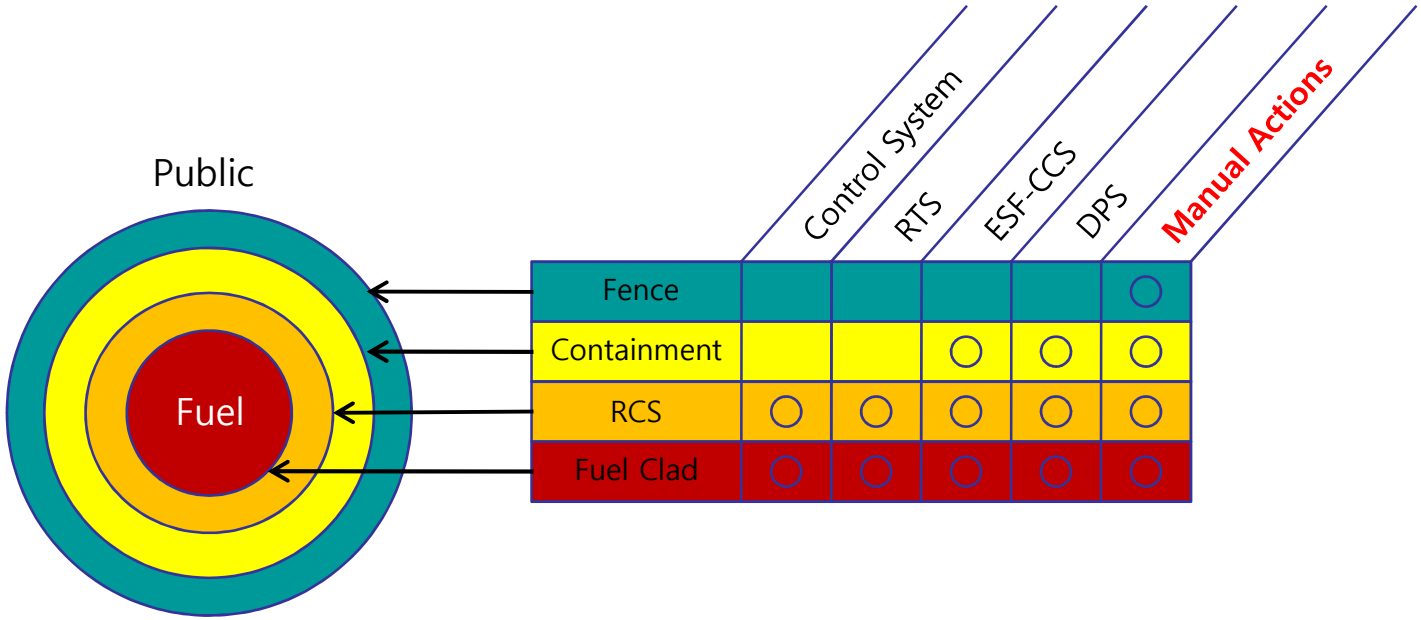
Systems Approach to Control Room Design

Human Factors Design Goal for SMART CR



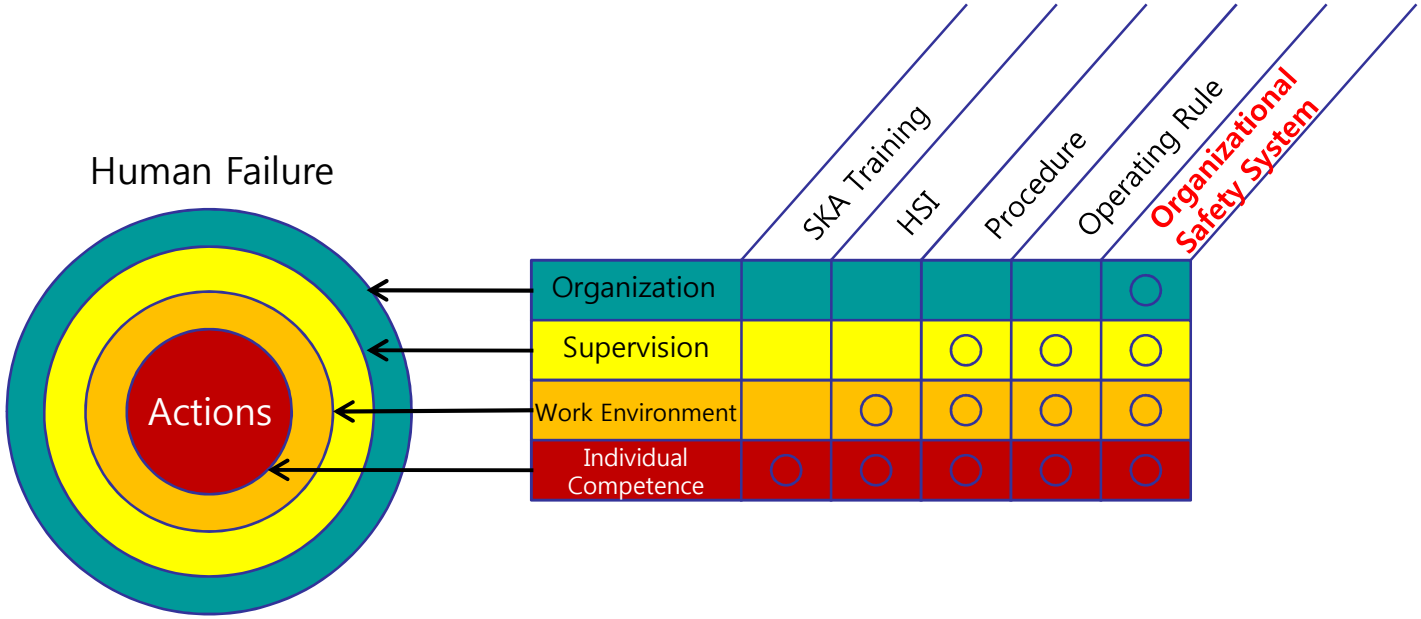
Systems Approach to Control Room Design

- **D3 Concept of MMIS**



Systems Approach to Control Room Design

D3 Concept of Human Factors Design



Systems Approach to Control Room Design

Human Factors Engineering Program Plan

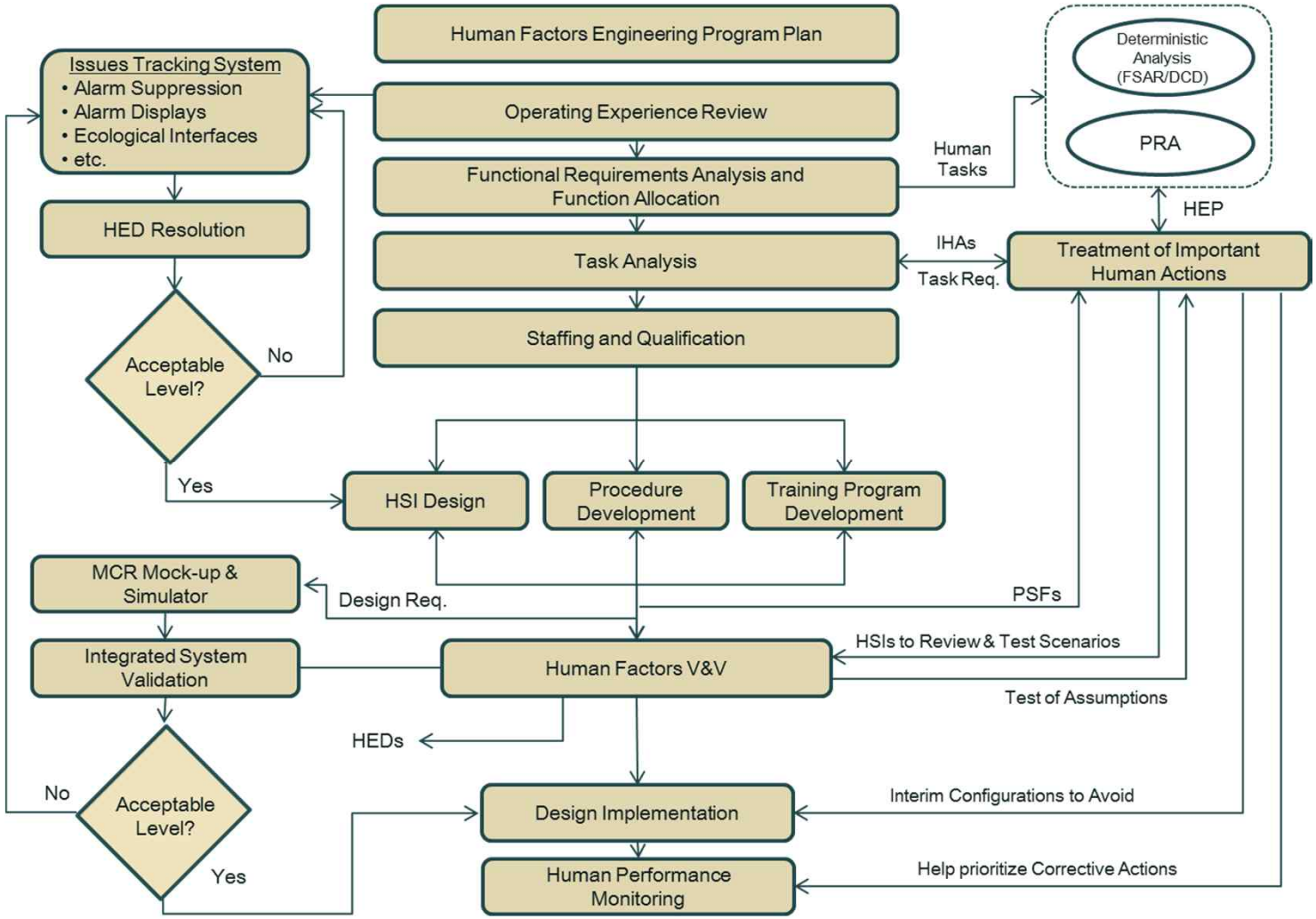
- **Purpose: to increase system performance and productivity while reducing accidents caused by human errors**
  - To make systems **easier understand and use**, thus reducing training and support costs;
  - To improve **user satisfaction** and reduce discomfort and stress;
  - To improve the productivity of users and the **operational efficiency** of organizations;
  - To improve **product quality**, to appeal to the users and to provide a **competitive advantage**.

Systems Approach to Control Room Design

- **Twelve Elements of the HFE program according to the NUREG-0711 (Rev.3)**
  - HFE Program Management
  - Operating Experience Review
  - Functional Requirement Analysis and Function Allocation
  - Task Analysis
  - Staffing & Qualification
  - Treatment of Important HAs
  - Hum-System Interface Design
  - Procedure Development
  - Training Program Development
  - Human Factors Verification and Validation
  - Design Implementation
  - Human Performance Monitoring

Systems Approach to Control Room Design

Overview of HFE Design Process for CR



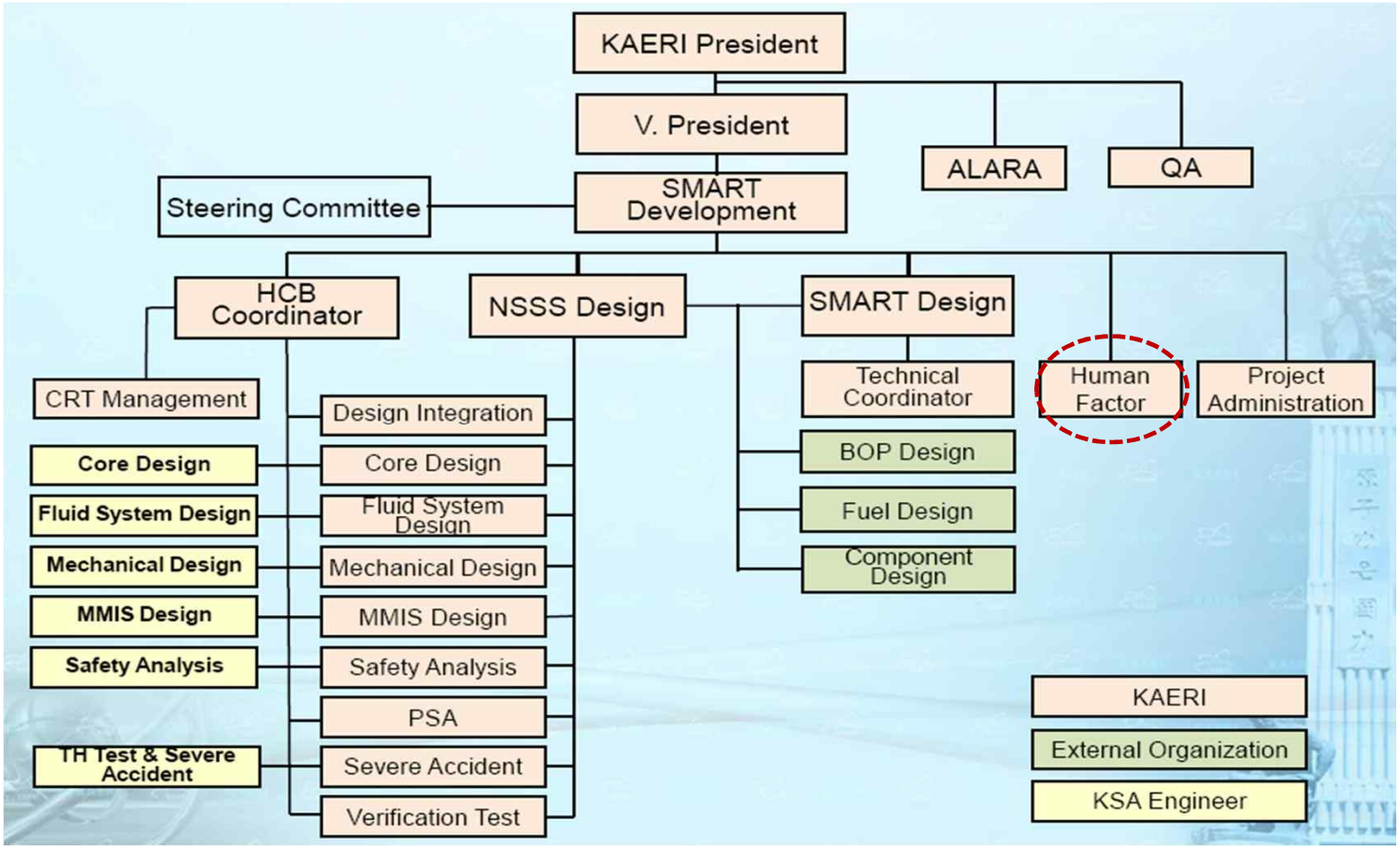
Human Factors Engineering Program

HFE Program Management

- We composed an **HFE design team** with the responsibility, authority, placement within the organization, and composition to reasonably **assure that the plant design meets the commitment to HFE**.
- The HFEPP guides the team to ensure that the HFE program is properly developed, executed, overseen, and documented.
- The HFEPP describes the HFE elements to ensure that HFE principles are applied to the development, design and evaluation of HSI, procedures, and training.
- To effectively accomplish HFE in designing and modifying a plant, the HFEPP implemented the following items by a qualified HFE design team:
  - general goals and scope of the HFE program
  - HFE team, member qualifications, and organization
  - HFE process and procedures
  - HFE issues tracking
  - HFE elements

Human Factors Engineering Program

HFE Design Team



Human Factors Engineering Program

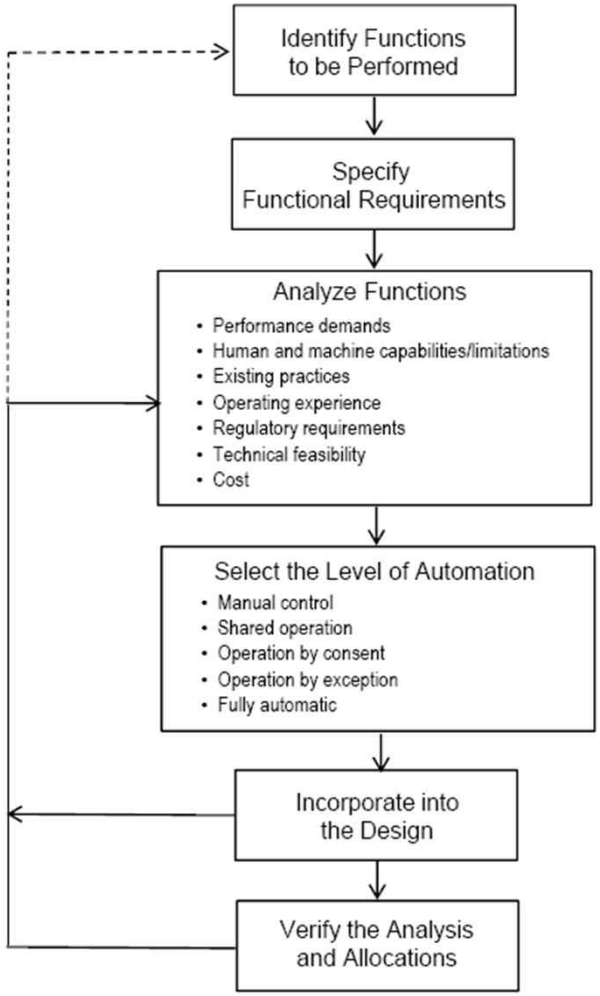
Operating Experience Review

- **The main purpose of conducting an operating experience review is to identify HFE-related safety issues.**
  - The OER should provide information on the performance of predecessor designs.
  - For new plants, this may be the earlier designs on which the new one is based.
  - For plant modifications, it may be the design of the systems being changed.
  - The issues and lessons learned from operating experience provide a basis to improve the plant's design; i.e., at the beginning of the design process.
- **We are identifying and analyzing HFE-related problems and issues in previous designs similar to the current one under review.**
  - In this way, the negative features of predecessor designs may be avoided in the current one, while retaining positive features.
  - The OER should consider the predecessor systems upon which the design is based, the technological approaches selected (e.g., if touch-screen interfaces are planned, their associated HFE issues should be reviewed), and the plant's HFE issues.

Human Factors Engineering Program

Functional Requirements Analysis and Function Allocation

- We have defined functions that must be carried out to satisfy the plant's safety goals and that the assignment of responsibilities for those functions to personnel and automation in a way that takes advantage of human strengths and avoids human limitations.
- A functional requirements analysis identifies those plant functions that must be performed to satisfy the plant's overall operating and safety objectives and goals:
  - To ensure the health and safety of the public by preventing or mitigating the consequences of postulated accidents.
  - This analysis determines the objectives, performance requirements, and constraints of the design, and sets a framework for understanding the role of controllers (personnel or system) in regulating plant processes.



Human Factors Engineering Program

Task Analysis

- The functions allocated to plant personnel are defined the roles and responsibilities that they then accomplish via human actions (HAs).
- HAs can be divided into tasks, a group of related activities with a common objective or goal.
- We have identified the specific tasks needed to accomplish personnel functions, and also the alarms, information, control- and task-support required to complete those duties.
- The results of the task analysis offer important inputs in many HFE activities:
  - (1) The analysis of staffing and qualifications;
  - (2) the design of HSIs, procedures, and training program;
  - (3) criteria for task support verification.

Human Factors Engineering Program

- **Staffing and Qualifications**
  - Initial staffing levels was established early in the process based on experience with previous plants, staffing goals (such as for staffing reductions), initial analyses, and NRC regulations.
  - However, the initial staffing levels' acceptability should be examined periodically as the design of the plant evolves.
  - We has systematically analyzed the requirements for the number of personnel and their qualifications that includes gaining a thorough understanding of the task and regulatory requirements.

Human Factors Engineering Program

Treatment of Important Human Actions

- Over the past several decades, a goal of the NRC's safety programs has been to use **risk analyses to prioritize activities**, and to ensure that regulators and licensees alike focus efforts and resources on those activities that best support reasonable assurance of adequate protection of the public's health and safety.
- HFE programs contribute to this goal by applying **a graded approach** to plant design, focusing greater attention on **HAs most important to safety**.
- We have identified those HAs most important to safety for a particular plant design; this is accomplished through a combination of probabilistic and deterministic analyses through the following activities.
  - (1) identified important HAs
  - (2) considered human-error mechanisms for important HAs in designing the HFE aspects of the plant.
- Ultimately, we have a goal to minimize the likelihood of personnel error, and help ensure that personnel can detect and recover from any errors that occur.

Human Factors Engineering Program

- **Human-System Interface Design**
  - We have developed a process to translate the functional- and task-requirements to HSI design requirements, and to the detailed design of alarms, displays, controls, and other aspects of the HSI.
  - A structured methodology is used for identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations.
  - We also have developed a HFE guidelines tailored to the unique aspects of the our design, e.g., a style guide to define the design-specific conventions.

Human Factors Engineering Program

Human-System Interface Design (HSI Design Principles)

Situation Awareness

- The information presented to the users by the HSI should be correct, **rapidly recognized**, and easily understood (e.g., "direct perception" or "status at a glance" displays) and **support the higher-level goal of user awareness** of the status of the system.

Task Compatibility

- The system should **meet the requirements of users to perform their tasks** (including operation, safe shutdown, inspection, maintenance, and repair). Data should be presented in forms and formats appropriate to the task (including the need to access confirmatory data or raw data in the case of higher-level displays), and control options should encompass the range of potential actions. There should be no unnecessary information or control options.

User Model Compatibility

- All aspects of the system should **be consistent with the users' mental models** (understanding and expectations about how the system behaves as developed through training, use of procedures, and experience). All aspects of the system also should be consistent with established conventions (i.e., expressed in customary, commonplace, useful and functional terms, rather than abstract, unusual or arbitrary forms, or in forms requiring interpretation).

Human Factors Engineering Program

Human-System Interface Design (HSI Design Principles)

Organization of HSI Elements

- The organization of all aspects of the HSI (from the elements in individual displays, to individual workstations, to the entire control room) should **be based on user requirements** and should **reflect the general principles of organization by importance, frequency, and order of use.** Critical safety-function information should be available to the entire operating crew in dedicated locations to ensure its recognition and to minimize data search and response.

Logical/Explicit Structure

- All aspects of the system (formats, terminology, sequencing, grouping, and operator's decision-support aids) should reflect an **obvious logic based on task requirements** or some other non-arbitrary rationale. The relationship of each display, control, and data-processing aid to the overall task/function should be clear. The structure of the interface and its associated navigation aids should make it easy for users to recognize where they are in the data space and should enable them to get rapid access to data not currently visible (e.g., on other display pages). The way the system works and is structured should be clear to the user.

Human Factors Engineering Program

Human-System Interface Design (HSI Design Principles)

Timeliness

- The system design should **take into account users' cognitive processing capabilities as well as process-related time constraints** to ensure that tasks can be performed within the time required. Information flow rates and control performance requirements that are too fast or too slow could diminish performance.

Controls/Displays Compatibility

- Displays **should be compatible with the data entry and control requirements**.

Feedback

- The system should provide useful information on system status, permissible operations, errors and error recovery, dangerous operations, and validity of data.

Human Factors Engineering Program

Procedure Development

- Procedures are essential to plant safety because they support and guide personnel interactions with plant systems and personnel responses to plant-related events.
- In the nuclear industry, procedure development is the responsibility of individual utilities.
- We have **identified HFE requirements** for procedures, along with all other design requirements, to develop procedures that are technically accurate, comprehensive, explicit, easy to utilize, validated.

Human Factors Engineering Program

- **Training Program Development**
  - Training plant personnel is important in ensuring the safe, reliable operation of nuclear power plants.
  - Training programs aid in offering reasonable assurance that plant personnel have the knowledge, skills, and abilities needed to perform their roles and responsibilities.
  - We have **identified HFE requirements** for the training program using a systems approach for developing personnel training considering HFE principles and criteria.

Human Factors Engineering Program

Human Factors Verification and Validation

- Verification and validation (V&V) comprehensively determine that the final HFE design conforms to accepted design principles, and enables personnel to successfully and safely perform their tasks to achieve operational goals.
- This element involves three evaluations, with the following objectives:
  - HSI Task Support Verification - we will verify that the HSI provides the alarms, information, controls, and task support defined by tasks analysis needed for personnel to perform their tasks.
  - HFE Design Verification - we will verify that the design of the HSIs conform to HFE guidelines (such as the applicant's style guide).
  - Integrated System Validation - we will validate, using performance-based tests, that the integrated system design (i.e., hardware, software, procedures and personnel elements) supports safe operation of the plant.
- These evaluations identify human engineering discrepancies (HEDs).
- The HED resolutions verifies that the HFE design team assessed the importance of HEDs, corrected important ones, and that the corrections are acceptable.

Human Factors Engineering Program

Design Implementation

- This element addresses implementation of the HFE aspects of the plant design for new plants and plant modifications.
  - For SMART, the implementation phase will be well defined and carefully monitored through start-up procedures and testing.
- We will verify that as-built design conforms to the verified and validated design resulting from the HFE design process.

Human Factors Engineering Program

Human Performance Monitoring

- The objective of the human performance monitoring program is to verify that a future utility prepares a program to:
  - adequately assure that the conclusions drawn from the integrated system validation remain valid with time;
  - ensure that no significant safety degradation occurs because of any changes made in the plant.
- A future utility may incorporate this monitoring program into their problem identification and resolution program and their training program.

Control Room Design

Control Room Design

Main Objectives of the MCR

- The main control room is provided form which the nuclear power plant can be operated **safely and efficiently** in all plant operational states and accident conditions.
- The main control room provides the control room staff with the human-machine **interfaces** and related **information and equipment**, e.g., the communication interfaces, which are necessary for the achievement of the plant operational goals.
- The main control room provides an **environment** under which the control room staff is able to perform their tasks without discomfort, excessive stress, or physical hazard.

Control Room Design

Functional design Objectives of the MCR

- The principal objectives of the control room design are to provide the operator with **accurate, complete, and timely information** regarding the functional status of plant equipment and system.
- The design shall **allow for all operational states**, including refueling and accident conditions, optimize the tasks and minimize the workload required to monitor and control the plant, and provide necessary information to other facilities outside the control room.
- The control room design shall provide an **optimal assignment of functions** which achieves maximum utilization of operator and system capabilities.
- An additional objective of the control room design is to permit station commissioning to take place effectively and to permit modifications and maintenance.

Control Room Design

Safety Principles of the MCR

- A control room shall be designed to enable the nuclear power plant to be operated safely in all operational states and to bring it back to a safe after the onset of accident conditions. Such design basis events are to be considered in the design of the control room.
- Equipment controlled from the control room should be designed, as far as practicable, so that an unsafe manual command cannot be carried out, e.g. by using a logical interlock depending on the plant status.
- Account shall also be taken of the need for functional isolation and physical separation where safety and non-safety systems are brought into close proximity.
- Appropriate measures shall be taken to safeguard the occupants of the control room against potential hazards such as unauthorized access, undue radiation resulting from an accident conditions, toxic gases, and all consequence of fire, which could jeopardize necessary operator actions.

Control Room Design

Availability Principles of the MCR

- With a view to maximizing the plant capacity factors to assure a satisfactory return on the financial investigation in nuclear power plant, consideration shall be given in the control room design to:
  - facilitating planned operations
  - minimizing the occurrence of any undesired power reduction or plant trip caused by operators' erroneous decision-making and actions, or by local disturbances associated with malfunction or failure of I&C systems.
- The availability-related design specifications shall not violate the adopted safety principles.

Control Room Design

Human Factors Engineering Principles of the MCR

- In order to provide an optimal assignment of functions which assures **maximum utilization of the capabilities of human and machine** and aims to achieve the maximum plant safety and availability,
- the design **shall pay particular attention to** human factors principles and human characteristics of personnel with regard to their **anthropometric, perceptual, cognitive, physiological and motor response capabilities and limitations.**

Control Room Design

- **Main Objectives of the RSR**

  - The remote shutdown room is for a facility outside of the main control room which, in case of abandonment of the main control room (Loss-of-habitability or Loss-of-control), can be used to drive the nuclear reactor down to under-criticality, to keep it in the under-critical state and to monitor and control the heat removal from the nuclear reactor.

Control Room Design

- **Functional design Objectives of the RSR**
  - Plant designs should provide for control in locations **removed from the main control room** that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown.
  - This control equipment should be capable of **operating independently** of (without interaction with) the equipment in the main control room.
  - This equipment may include the **remote shutdown station and other local controls.**

Control Room Design

- **Considering the Seven Categories of Digital HFs Issues (O'Hara & Higgins, 2010)**
  - Change in the overall role of personnel
  - Difficulty in understanding automation
  - Monitoring failures, loss of vigilance, etc.
  - Out-of-the-loop/situation awareness degrade
  - Workload transitions on loss of auto control
  - Loss of skills for automated tasks
  - New-types of human errors

Control Room Design

Digital HFs Issues - Minimum Inventory of HSIs

- The Minimum Inventory as additional HSIs that provide capabilities **not supported by the operator workstations**, and which may be needed in a modern control room design. These include:
  - **Spatially dedicated, continuously visible (SDCV) displays** driven by the non-safety control and information system – for example, a flat panel display that shows alarms in fixed positions, such as a tile-replica display; large group-view displays, visible to the entire operating crew, also may be provided.
  - **Safety-related HSIs** – these may be qualified discrete digital or analog/hard-wired controls and indicators, or qualified computer-based HSIs; these may include SDCV computer-based displays.
  - **Non-safety-related HSIs** that are independent of the main control and information system that drives the operator workstations – again, these may include discrete controls and indicators and/or computer-based HSIs, and may include SDCV HSIs.

Control Room Design

Digital HFs Issues - Minimum Inventory of the MCR

- The Main Control Room minimum inventory includes the human system interfaces that the operator always needs available to:
  - monitor the status of fission product barriers,
  - perform and confirm a reactor trip,
  - perform and confirm a controlled shutdown of the reactor using the normal or preferred safety means,
  - actuate safety related systems that have the critical safety function of protecting the fission product barriers,
  - analyze failure conditions of the normal human system interfaces, while maintaining the current plant operating condition and power level until the human system interfaces are restored in accordance with applicable regulatory requirements,
  - implement the plant's emergency operating procedures,
  - bring the plant to a safe condition,
  - carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment.

Control Room Design

Digital HFs Issues - Minimum Inventory of the RSR

- The minimum inventory at the Remote Shutdown Room should include the human system interfaces that the operator always needs available to:
  - perform and confirm a reactor trip, and
  - place and maintain the reactor in a safe condition using the normal or preferred safety means.

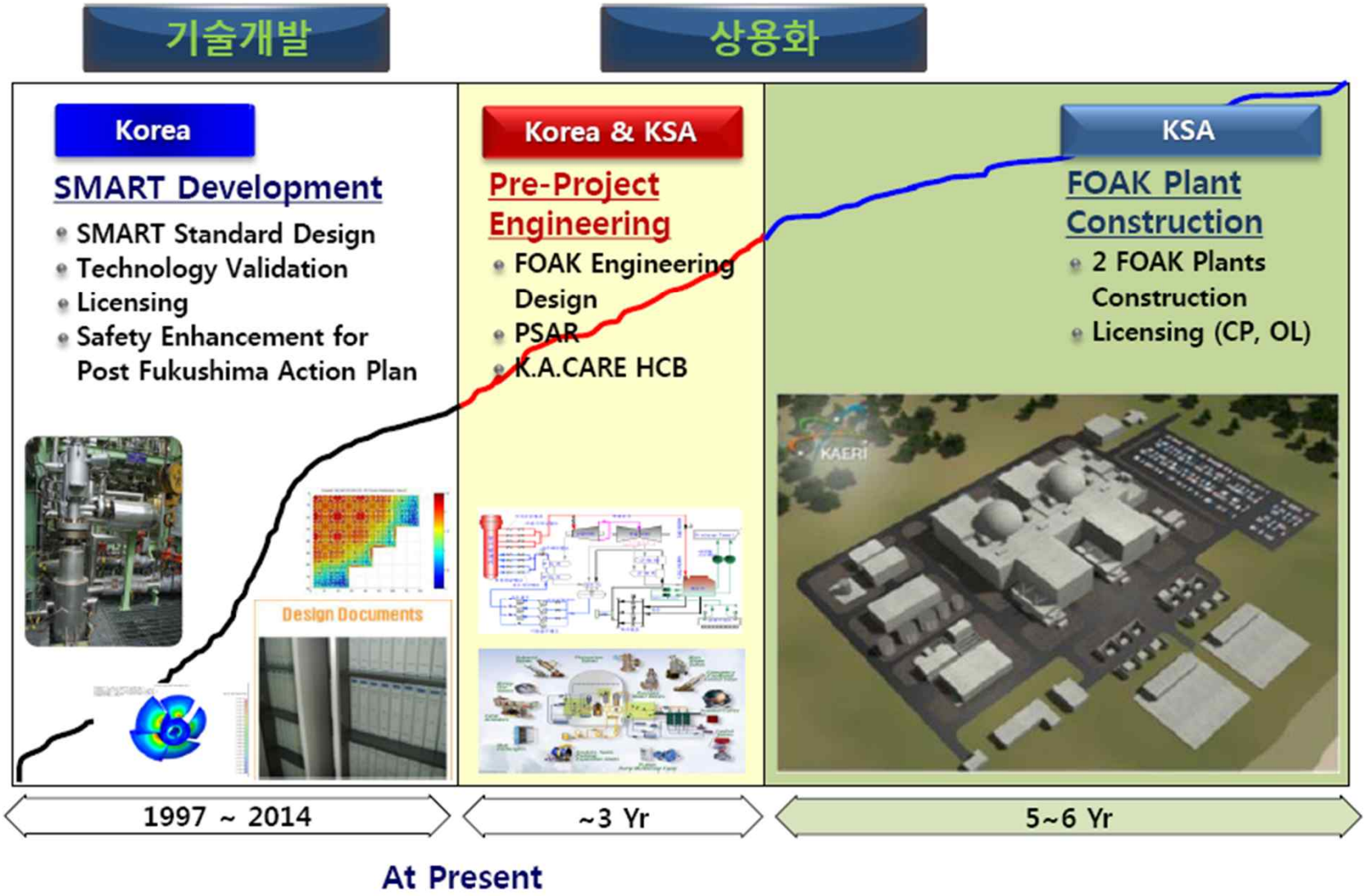
Control Room Design

- **Digital HFs Issues - Crediting Manual Operator Actions**

  - We will **evaluate the acceptability of manual operator action** as a diverse means of coping with Anticipated Operational Occurrences and Postulated Accidents (AOO/PA) that are concurrent with a software Common Cause Failure (CCF) of safety related digital systems.
  - Manual operator actions taken from the Main Control Room (MCR) are acceptable for abnormal operational occurrence or plant accident mitigation concurrent with a BTP 7-19 software common cause failure.
  - This software CCF is discussed in the Background of Branch Technical Position (BTP) 7-19, (March 2007) Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer – Based Instrumentation and Control Systems.

Discussion

Discussion


기술개발
상용화
Korea
SMART Development
SMART Standard Design
Technology Validation
Licensing
Safety Enhancement for Post Fukushima Action Plan
Design Documents
Korea & KSA
Pre-Project Engineering
FOAK Engineering Design
PSAR
K.A.CARE HCB
KSA
FOAK Plant Construction
2 FOAK Plants Construction
Licensing (CP, OL)
KAERI
1997 ~ 2014
~3 Yr
5~6 Yr
At Present

Dialogue

Sa Kil Kim, Ph.D.
Senior Researcher
I&C/Human Factors Division
Korea Atomic Energy Research Institute
E-mail: sakilkim@keari.re.kr
Tel: +82-42-868-4755