WORKSHOP FOR SENIOR MANAGERS

ENHANCEMENT OF SAFETY CULTURE

IN THE OPERATION OF NPPs

6 - 9 May 1997, Visaginas, Lithuania

BASIC SAFETY PRINCIPLES: LESSONS LEARNED

By:

Jan B. van Erp

Argonne National Laboratory

Argonne, Illinois 60439, USA

Tel. 630-252-3381; Fax. 630-252-3193

E-mail: <vanerp@dep.anl.gov>
WORKSHOP FOR SENIOR MANAGERS

ENHANCEMENT OF SAFETY CULTURE

IN THE OPERATION OF NPPs

6 - 9 May 1997, Visaginas, Lithuania

BASIC SAFETY PRINCIPLES; LESSONS LEARNED

• The concept of safety culture did not start with INSAG after the accident at Chernobyl

• Safety culture by different names has been recognized earlier than Chernobyl: A prime example is the Kemeny report on the accident at Three Mile Island (TMI)

• The Kemeny report on TMI identified humans as the prime source/defense for/against accidents

• Safety culture and the role of humans in safety have been recognized since a long time in many industries; example: airline industry, etc.
SOME CONCLUSIONS FROM THE KEMENY REPORT
ON THE ACCIDENT AT TMI

AS THE EVIDENCE ACCUMULATED, IT BECAME CLEAR THAT THE FUNDAMENTAL
PROBLEMS ARE PEOPLE-RELATED PROBLEMS AND NOT EQUIPMENT PROBLEMS.

WHEREVER WE LOOKED, WE FOUND PROBLEMS WITH THE HUMAN BEINGS WHO
OPERATE THE PLANT, WITH THE MANAGEMENT THAT RUNS THE KEY ORGANIZATION,
AND WITH THE AGENCY THAT IS CHARGED WITH ASSURING THE SAFETY OF NUCLEAR
POWER PLANTS.

WE NOTE A PREOCCUPATION WITH REGULATIONS. HOWEVER, WE ARE CONVINCED
THAT REGULATIONS ALONE CANNOT ASSURE SAFETY. INDEED, ONCE REGULATIONS
BECOME VOLUMINOUS AND COMPLEX AS THOSE REGULATIONS NOW IN PLACE, THEY
CAN SERVE AS A NEGATIVE FACTOR IN NUCLEAR SAFETY.

THE SATISFACTION OF REGULATORY REQUIREMENTS IS (ERRONEOUSLY) EQUATED
WITH SAFETY. THIS COMMISSION BELIEVES THAT IT IS (ONLY) AN ABSORBING
CONCERN WITH SAFETY THAT WILL BRING ABOUT SAFETY -- NOT JUST THE MEETING
OF NARROWLY PRESCRIBED AND COMPLEX REGULATIONS.
REQUIRE OPERATORS AND SUPERVISORS WHO HAVE A THOROUGH UNDERSTANDING OF THE FUNCTIONING OF THE PLANT AND WHO CAN RESPOND TO COMBINATIONS OF SMALL EQUIPMENT FAILURES.

WHAT THE NRC AND THE INDUSTRY HAVE FAILED TO RECOGNIZE SUFFICIENTLY IS THAT THE HUMAN BEINGS WHO MANAGE AND OPERATE THE PLANTS CONSTITUTE AN IMPORTANT SAFETY SYSTEM.

WE FIND THAT THERE IS A LACK OF "CLOSURE" IN THE SYSTEM -- THAT IS, IMPORTANT SAFETY ISSUES ARE FREQUENTLY RAISED AND MAY BE STUDIED TO SOME DEGREE OF DEPTH, BUT ARE NOT CARRIED THROUGH TO RESOLUTION.

CONTRIBUTING CAUSES:

1. IT IS OUR CONCLUSION THAT THE TRAINING OF TMI OPERATORS WAS GREATLY DEFICIENT.

2. WE FOUND THAT THE SPECIFIC OPERATING PROCEDURES, WHICH WERE APPLICABLE TO THIS ACCIDENT, ARE AT LEAST VERY CONFUSING AND COULD BE READ IN SUCH A WAY AS TO LEAD THE OPERATORS TO TAKE THE INCORRECT ACTIONS THEY DID.

3. THE LESSONS FROM PREVIOUS ACCIDENTS DID NOT RESULT IN NEW, CLEAR INSTRUCTIONS BEING PASSED ON TO THE OPERATORS.
SOME RECOMMENDATIONS FROM THE KEMENY REPORT ON THE ACCIDENT AT TMI

1. THE NUCLEAR INDUSTRY MUST DRAMATICALLY CHANGE ITS ATTITUDE TOWARD SAFETY AND REGULATIONS:
   
   A. THE INDUSTRY SHOULD ESTABLISH A PROGRAM THAT SPECIFIES APPROPRIATE SAFETY STANDARDS INCLUDING THOSE FOR MANAGEMENT, QUALITY ASSURANCE, AND OPERATING PROCEDURES AND PRACTICES, AND THAT CONDUCTS INDEPENDENT EVALUATIONS.
   
   B. THERE MUST BE A SYSTEMATIC GATHERING, REVIEW, AND ANALYSIS OF OPERATING EXPERIENCE AT ALL NUCLEAR POWER PLANTS COUPLED WITH AN INDUSTRY-WIDE INTERNATIONAL COMMUNICATIONS NETWORK TO FACILITATE THE SPEEDY FLOW OF THIS INFORMATION TO AFFECTED PARTIES.

2. ALTHOUGH THE COMMISSION CONSIDERS THE RESPONSIBILITY FOR SAFETY TO BE WITH THE TOTAL ORGANIZATION OF THE PLANT, WE RECOMMEND THAT EACH NUCLEAR POWER PLANT COMPANY HAVE A SEPARATE SAFETY GROUP THAT REPORTS TO HIGH-LEVEL MANAGEMENT.

3. INTEGRATION OF MANAGEMENT RESPONSIBILITY AT ALL LEVELS MUST BE ACHIEVED CONSISTENTLY THROUGHOUT THIS INDUSTRY. THERE MUST BE A SINGLE ACCOUNTABLE ORGANIZATION WITH THE REQUISITE EXPERTISE TO TAKE RESPONSIBILITY FOR THE INTEGRATED MANAGEMENT OF THE DESIGN, CONSTRUCTION, OPERATION, AND EMERGENCY RESPONSE FUNCTIONS.
4. It is important to attract high qualified candidates for the positions of Senior Operator and Operator Supervisor.

5. Substantially more attention and care must be devoted to the writing, reviewing, and monitoring of plant procedures.

A. The wording of procedures must be clear and concise.

B. The content of procedures must reflect both engineering thinking and operating practicalities.

C. The format procedures, particularly those that deal with abnormal conditions and emergencies, must be especially clear, including clear diagnostic instructions for identifying the particular abnormal conditions confronting the operators.

D. Management of both utilities and suppliers must insist on the early diagnosis and resolution of safety questions that arise in plant operations.
CONCLUSIONS AND RECOMMENDATIONS FROM THE ROGOVIN REPORT
ON THE ACCIDENT AT TMI

THE PRINCIPAL DEFICIENCIES IN COMMERCIAL REACTOR SAFETY TODAY ARE NOT HARDWARE PROBLEMS, THEY ARE MANAGEMENT PROBLEMS. THESE PROBLEMS CANNOT BE SOLVED BY THE ADDITION OF A FEW PIPES AND VALVES—OR, FOR THAT MATTER, BY A RESIDENT FEDERAL INSPECTOR AT EVERY REACTOR.

MANY NUCLEAR PLANTS ARE PROBABLY OPERATED BY MANAGEMENT THAT HAS FAILED TO MAKE CERTAIN THAT ENOUGH PROPERLY TRAINED OPERATORS AND QUALIFIED ENGINEERS ARE AVAILABLE ON SITE IN RESPONSIBLE POSITIONS TO DIAGNOSE AND COPE WITH A POTENTIALLY SERIOUS ACCIDENT. THE NRC, FOR ITS PART, HAS VIRTUALLY IGNORED THE CRITICAL AREAS OF OPERATOR TRAINING, HUMAN FACTORS ENGINEERING, UTILITY MANAGEMENT, AND TECHNICAL QUALIFICATIONS.


WE FOUND THAT BEFORE MARCH 28, 1979, AN ATTITUDE OF COMPLACENCY PERVADED BOTH THE INDUSTRY AND THE NRC, AN ATTITUDE THAT THE ENGINEERED DESIGN SAFEGUARDS BUILT INTO TODAY'S PLANTS WERE MORE THAN ADEQUATE, THAT AN ACCIDENT LIKE THAT AT THREE MILE ISLAND WOULD NOT OCCUR.
DURING THE PERIOD IN WHICH MOST LARGE NUCLEAR PLANTS HAVE BEEN DESIGNED, THE NUCLEAR INDUSTRY HAS PAID REMARKABLY LITTLE ATTENTION TO ONE OF THE BEST TOOLS AVAILABLE FOR INTEGRATING THE REACTOR OPERATOR INTO THE SYSTEM: THE RELATIVELY NEW DISCIPLINE OF "HUMAN FACTORS".

A NUMBER OF EXCELLENT STUDIES HAVE FOUND SIGNIFICANT FLAWS IN CONTROL ROOM DESIGN OF OPERATING NUCLEAR PLANTS: INSTRUMENTS THAT ARE DIFFICULT TO MAKE OUT AND DO NOT DISTINGUISH BETWEEN NORMAL AND DANGEROUS READINGS; CONTROLS LOCATED FAR FROM THE INSTRUMENT DISPLAYS; FAILURE TO DISPLAY IMPORTANT PLANT PARAMETERS IN A PROMINENT POSITION; LACK OF FUNCTIONAL INSTRUMENT GROUPING, LACK OF CONSISTENT COLOR CODING AND LABELING.

THE STUDIES ALSO FOUND PHYSICAL HINDRANCES HAD TO BE ENDURED BY OPERATORS. GLARE AND REFLECTION ON INSTRUMENTS, COMPOUNDED BY POOR LIGHTING, MADE METERS DIFFICULT TO READ. INSTRUMENTS WERE PLACED TOO HIGH OR TOO LOW. FAR TOO MANY ALARMS, BOTH AUDIBLE AND VISUAL, INUNDATED THE OPERATORS WITH A NUMBING AMOUNT OF INFORMATION.

CONTROL ROOM DESIGN PLAYED MORE THAN A MINOR ROLE IN CONTRIBUTING TO THE ACCIDENT AT THREE MILE ISLAND.
INSTRUMENTATION DEFICIENCIES (FROM ROGOVIN REPORT)

1. NO VISUAL ALARM SIGNALS THAT THE EMERGENCY FEEDWATER SYSTEM WAS COMPLETELY BLOCKED OFF.

2. THE INDICATOR LIGHT FOR THE STUCK-OPEN PRESSURIZER RELIEF VALVE WAS WIRED TO SHOW WHAT THE VALVE HAD BEEN "INSTRUCTED" BY THE ELECTRICAL SYSTEM TO DO, NOT THE VALVE'S ACTUAL POSITION.

3. THE PLANT DID NOT HAVE INSTRUMENTATION SHOWING THE LEVEL OF REACTOR COOLANT IN THE MAIN REACTOR VESSEL.

4. INCORE THERMOCOUPLES SHOWING TEMPERATURES ABOVE THE REACTOR CORE HAD TO BE READ WITH A HAND-HELD ELECTRICAL METER BECAUSE THE THERMOCOUPLES WERE READING OFF THE COMPUTER'S DISPLAY SCALE.

5. OPERATORS SHOULD HAVE DETECTED THE STUCK-OPEN PORV FROM HIGH TEMPERATURE READINGS IN THE PIPING THROUGH WHICH THE COOLANT WAS LEAKING. THESE READINGS WERE MISINTERPRETED, BECAUSE, WITHOUT A STRIP CHART SHOWING THE READINGS OVER TIME, THEY WERE THOUGHT TO BE "TRENDING DOWN".

6. THE READ-OUT DISPLAY COMPUTER GOT SO FAR BEHIND IN PRINTING OUT ALARMS THAT OPERATORS HAD TO "DUMP" ITS MEMORY IN ORDER TO GET UP TO DATE. INFORMATION THAT MIGHT HAVE HELPED THEM DIAGNOSE THE ACCIDENT WAS CONSEQUENTLY LOST.