The problems of safe technological development

In an article appearing in the USSR in 1987, Soviet academician Valerij A. Legasov addressed issues of industrial and technological safety.* Following are excerpts of that article:

"Nowadays it is a characteristic trend that, whereas the probability of each individual incident (whether it be an air, train or shipping disaster, the destruction of a dam, a chemical works or a nuclear plant) is falling, the magnitude of the consequences if one does occur is, as a rule, growing considerably. Indeed, whereas in the 1940s dozens of air crashes caused the deaths of dozens of people, nowadays one single crash, although such events occur much less commonly, takes a toll of hundreds of lives. Fires have long-since dogged mankind's steps, but with the development of the petrochemical industry and gas power they have begun to be accompanied by explosions which increase sharply the scale of the damage and the affected area...

"Why, for instance, despite efforts to increase the reliability of technology, do accidents occur? Why is the extent of their consequences increasing? Complicated modern means of production and machines are designed so that their reliability is as high as possible from the point of view of our existing understanding of the nature of the dangers they pose, and of the technical and economic means of forestalling them. As a rule, design specifications and operational regulations together might guarantee the safe working of a plant or unit, were it not for equipment production faults, the finite reliability of each separate component and device, or deviations from preordained operational regimes caused by changes of materials, for example, or the running of experiments, or simple human error. Familiar as they are with the inevitability of such defects, designers and project engineers create various systems to forestall the possibility of an accident when normal operational regimes are infringed. But the reliability and efficiency of the protective devices themselves are also finite and subject to technical failure and errors in usage. Therefore, secondary systems are installed, and sometimes tertiary and quaternary duplicate backup systems; but all this redundancy simply reduces the risk of an accident, making the machine or process more complex and more expensive at the same time; it reduces the probability of equipment failure or personnel error having catastrophic consequences, sometimes to very low levels, but the probability is never reduced to zero. A zero risk level is possible only in systems where there is no stored energy, or any chemically or biologically active components.

"A lot of modern, potentially dangerous means of production are designed with an estimated probability of a major disaster of the order of 10^{-4}. This means that through an unfortunate combination of circumstances, taking into account the real reliability of the machinery, the instruments, the materials and the personnel, one plant destruction is possible every 10 000 years of plant operation. If there is only one plant, then it is highly probable that during this time it will represent no danger. If there are a thousand such plants, then every decade one can expect one of them to be destroyed. And finally, if the number of such plants is close to 10 000, then, statistically, each year one of them could be the source of an accident. Here we can see one of the causes of the problems we are discussing. A plant designed on the basis of the technical means available and in accordance with regulatory requirements, which is suitably reliable when produced in small numbers, loses its reliability statistically when produced en masse, although physically it does not change...

"The increased scope of the consequences of accidents is also the result of the nature of modern scientific and technical progress. The energy- intensiveness of our society continues to rise. Plants saturated with energy and using dangerous substances at the same time are becoming more common. Their unit output is constantly being increased in the interests of economic performance. Pressure is growing on basic industrial machinery and the transport network, which is becoming ever more extensive. In the field of power production alone, ten thousand million tonnes of standard coal equivalent are produced, transported, stored, and used every year worldwide. This quantity of potentially inflammable and explosive fuel is comparable, in energy content, to the whole arsenal of nuclear weaponry accumulated in the world over the whole history of its existence. Moreover, the move in fuel supply towards a wider use of liquid gas fuels, and a simultaneous increase in the capacity of the concerns producing and using these fuels, has notably increased the risk of large-scale explosive fires...

"Another significant factor which increases industrial risk levels is the rise in distribution density of different types of plants and industries, and their interaction during accidents. The drive for maximum economy and maximum utilization of prior investment in power production, transport, and the social environment of a given region, leads to a concentration of various concerns within the region without any thorough analysis of their interrelationship and interaction. And it could be that the consequences of an accident in one of these plants would not be so dreadful were it not for the effect on a neighbouring plant which, perhaps, increases the damage many times over...

"A detailed analysis of statistical data shows that, although more than 60% of accidents are traceable to personal error, the lion's share of resources expended on industrial safety goes towards perfecting technical control and warning systems for such situations. The exception to this has been the aerospace industry where, historically, a great deal of attention has been paid to personnel selection, training and re-training using simulators, medical observation, discipline, material incentives, comfortable working conditions, the development of automatic support systems as back-up for crews and ground services... Other branches of activity have made serious attempts to use and perfect the experience of the aviators only since the beginning of the 1970s.

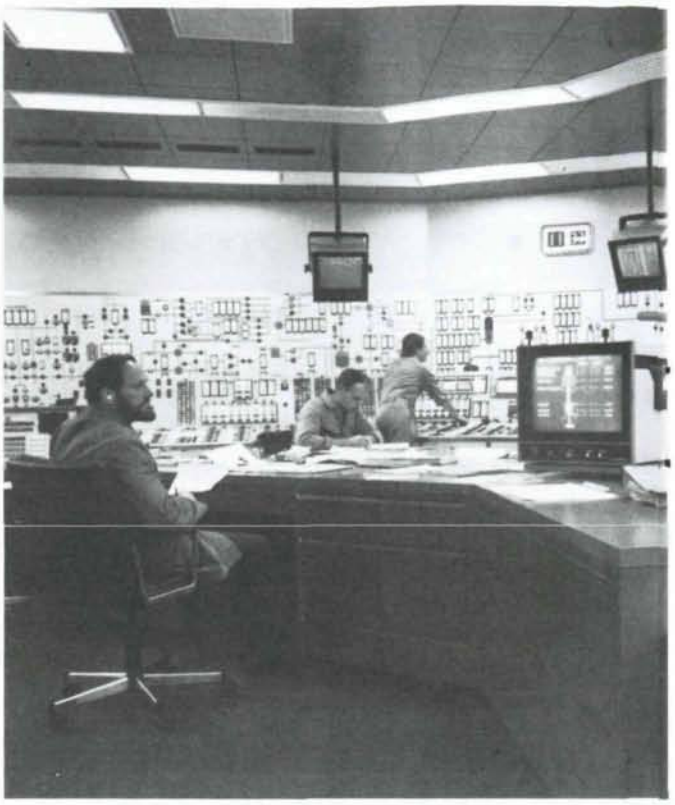
* Valerij Alekseevich Legasov is an Academician, a member of the Presidium of the USSR Academy of Sciences, and the Chief Deputy Director of the I.V. Kurchatov Atomic Energy Institute. In August 1986, he was the head of the Soviet delegation to the IAEA's Post-Accident Review Meeting following the accident at the Chernobyl nuclear power plant.

Usually, when speaking of the human factor and man/machine interaction, people reduce the issue to personnel discipline and training, to personnel responsibility and the exact execution of instructions and orders. All this is, of course, very important, but a close examination of emergency situations reveals that the heart of the problem is in management, where the human factor is most significant. It turns out that the instructions themselves were either not very exact and did not foresee — indeed in certain circumstances could not foresee — rules of conduct for irregular operating regimes, or that no check had been made to determine whether they had been properly assimilated. There are numerous cases where indiscipline and technological error have resulted directly from the established routines, from the absence of effective communication with competent specialists, lack of essential training and a knowledge of personnel potential, and also the lack of a clear understanding of the consequences of incorrect action.

"The high concentration of potentially dangerous industry in our economy makes a qualitatively new approach to safety essential. This new outlook must rely, first of all, on the search for optimum solutions to man/machine interaction problems, and then on putting them into operation with due speed. The provision of simulators with advanced computing facilities, a reduction in the volume of information made available, and variation in the methods of presenting it, an increase in the number of automatic and semi-automatic support systems for operators, the introduction of technical protection systems to guard against unsanctioned procedures, increased vigilance with regard to the condition of equipment by means of remote-controlled diagnostic devices — all this must become the normal concomitant of any complex process.

"Since the end of the 1970s, centres for general industry safety have appeared in many countries. The tasks they have set themselves are essentially to integrate world experience, investigate the role of previously unknown factors, train people and bring to light the most dangerous areas...

"In order that scientific and technical progress, which has already demonstrated its power and enormous potential, may continue to serve man in the future, it is essential that specialists in all disciplines should work together for safer and more reliable utilization of its achievements. Owing to the multiplicity of the problems and of the scientific disciplines employed to solve them, this work must go on not only within the traditional institutions responsible for the development of technology, but also in specially created centres for general industrial safety. The expansion of research in safety, and new approaches to the construction of technological systems, will make possible further technical development with reduced risk. In addition, we must recognize that life in our contemporary technological world places a special responsibility on the shoulders of every member of society. Mikhail Gorbachev, in a speech delivered on Soviet television on 14 May 1986, said: "For us, the lesson of Chernobyl lies indisputably in the fact that further development of the scientific and technical revolution will require questions of the reliability of technology and its safety, questions of discipline, order and organization, to be accorded prime importance. The highest standards are necessary everywhere and in everything".



Above: Control room of Beznau-1 in Switzerland.

Below: Scene from an inspection of reactor equipment in France. (Credit: French Nuclear Newsletter, 1986)