Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Recommendation 1210 (1993)[1]

Safety-critical computing systems

Parliamentary Assembly

1. The Assembly is aware that the use of computers in safety-related applications is growing, particularly in areas such as control systems of aeroplanes, high-speed trains and nuclear power stations, medical equipment and medical records, anti-lock braking systems for vehicles and machine engineering in general, and last but not least, modern weapons and their guidance systems.

2. Many recent accidents (for example, plane crash due to computer failure, malfunctioning robot killing a mechanic, patient dying because of malfunctioning of computer-controlled intravenous drip, rocket launch failure traced to computer error, software piracy, etc.) cause public concern and raise the question of the reliability of such systems.

3. There is undoubtedly real concern among professionals and scientists to guarantee the safety of these sophisticated automatic systems. The fact remains that economic and budgetary priorities may at times take precedence in industry over other factors. Consequently, the safety issue should be regarded as an area of public interest.

4. Safety is a difficult concept to grasp. It is closely bound up with the idea of danger and risk. Absolute safety does not exist. All human activities involve a degree of risk and technological innovations are no exception to the rule. The important thing is to minimise the risks as far as possible and to keep the public informed.

5. In most cases safety-control systems are not covered by any specific regulations and quality control is carried out only by internal procedures specific to the industrial sector concerned. Moreover, the mathematical codes underpinning the software of such systems are often considered as commercial secrets, thus making investigation difficult.

6. It would actually be much more cost-effective if industry were to put more effort and money into the design stage, which is crucial to the development of sophisticated systems. Failing this, laying down standards, regulations and penalties could nevertheless serve as a deterrent against technological "short cuts".

7. The "Guidelines for the security of information systems", recently adopted by OECD, give evidence of an increased awareness towards problems raised by the diverse use of computers. They focus nevertheless on aspects of data protection in order to ensure that the level of confidentiality, availability and integrity of these systems is not eroded. They should be completed by an up-stream study, namely technological reliability.

8. For the above reasons, the Assembly recommends that the Committee of Ministers call on the governments of member states to undertake an interdisciplinary activity within OECD, and in particular its Directorate of Science, Technology and Industry, whose aim would include:

8.1. determining areas of public interest, including future technologies that are currently being developed such as computer-communications between road and vehicle, the pan-European railway system, etc.;

---

1. See Doc. 6792, report of the Committee on Science and Technology, Rapporteur: Mr Fulvio Caccia. Text adopted by the Standing Committee, acting on behalf of the Assembly, on 26 March 1993.

8.2. instituting a European inventory and analysis of selected major accidents due to computerised systems;

8.3. drawing up a list of existing national and international standards and of any specific legislation in existence;

8.4. compiling a glossary of technical and legal terms so that future legislation can correspond to the extremely complex reality of the technological systems concerned;

8.5. working out general principles of safety-assessment methods in the early design stages of sophisticated products and systems;

8.6. developing the outlines of appropriate training, which should be multidisciplinary and include indepth study of economic parameters, for those with responsibility at national and European levels for assessing and judging safety implications of new technologies;

8.7. carrying out a study that compares legislation on the determination of liability for accidents and suggests ways of improving it;

8.8. providing special measures for scientific and legal investigations in the context of rules for the protection of intellectual property;

8.9. introducing, if need be and once the necessary data has been acquired through the initial research, quality control and certification systems at both national and European levels, prompted by the experience already acquired in the field of electrotechnical standardisation by the work of the International Electrotechnical Commission (IEC) and of the European Committee for Electrotechnical Standardisation (CENELEC).