Program on Advanced Technology for the Highway
INSTITUTE OF TRANSI'ORTATION STUDIES
UNIVERSITY OF CALIFORNIA AT BERKELEY

Notes From a Talk on Standards and IVHS Safety

Anthony Hitchcock

PATH Working Paper
UCB-ITS-PWP-91-3

This work was performed as part of the Program on Advanced Technology for the Highway (PATH) of the University of California, in cooperation with the State of California, Business and Transportation Agency, Department of Transportation, and the United States Department of Transportation, Federal Highway Administration, and the National Highway Traffic Safety Administration.

May 1991

ISSN 1055-1417

Notes From a Talk on Standards and IVHS Safety

Anthony Hitchcock

Program on Advanced Technology for the Highway (PATH)
Institute of Transportation Studies
University of California
Berkeley, California

May 1991

1: Introduction

This paper records a personal understanding of some features of the needs for standards and codes of practice in IVHS, and of the present position regarding them, in so far as the author has:

a. perceived them to be relevant to his own studies in the AVCS field in the U.S., mainly in relation to full automation.

b. been able to obtain access to the appropriate documents; he does not have easy access to a library containing defense standards.

The author thought it important, when starting work in the U.S., to discover to what extent standards and practice relating to system safety (specifically, software) differed between the U.S. and the European situation with which he was more familiar. He therefore made a series of visits to various defense, aerospace, chemical, and petroleum companies in California. It appears that the differences in practice are not great, though the documents are naturally not identical, and the U.S. documents are more precise and advanced. This experience forms one source of data for this paper.

A second source is a collaboration of discussions with Mr. Tom Buckley of the Computer Studies Unit at the University of Leeds, England, and his colleagues (1, 2). This group is responsible for software in part of the DRIVE project V1051, "Procedure for safety submissions for RTI [IVHS] systems." The third source is published material from the DRIVE project STAMMI (V1037 - Standards for the Man-Machine Interface) and some discussions with a participant in this group. There is significant work, but little of it is relevant to the themes of this paper.

From this material, three distinct themes seem to emerge which are relevant to IVHS design and evaluation. They are:

a. Hazard analysis and the safety-critical subsystem;

b. Design, verification, and validation of safety-critical software;

c. Configuration management.

These will all be discussed.

In all cases there is a dearth of standards applying directly to IVHS. In many cases there are few standards applying to highways or automobiles. It is possible, however, to examine standards in other branches of engineering where failures of specification or performance have the potential to create catastrophe. This literature may present areas for debate within the IVHS community.

There is, however, one major difference between IVHS and the other situations with which it is being compared. In all the non-IVHS cases there is one single owner/operator of the finished system. Those concerned with design, analysis, operation, etc., are ultimately responsible to the owner. In IVHS there is multiple ownership of vehicles, and roadside equipment in different places may be owned by several different parties. This must have a basic effect on any procedures used to certify compliance with standard, and probably also on the standards themselves. The situation seems unprecedented - there is work for IVHS America here.

2. Types of Standard

Howarth (3) has distinguished between product, performance and procedural standards. The distinction applies also to other documents which share some of the authority of standards; for example, codes of practice, guidelines, and handbooks, all of which are appropriate for consideration here. We will use the word "Standard" hereafter when referring to these titles.

When applied to systems, product standards define physical aspects, i.e. the size of the letters on a screen or the dimensions of an electrical connector. Performance standards are rare, though STAMMI (4) advises that they should be normal practice in man-machine aspects of IVHS. Performance standards define acceptability in terms of user performance. Until recently the only example known to STAMMI was BS 5321: 1975 which defined the acceptability of a child-resistant pharmaceutical drug container in terms of the percentage of children succeeding in getting it open during a specified time period. It is permissible to doubt the impact of such standards and the implied test procedures in a court dispute. Procedural standards describe programs of design, analysis, and testing to be used by a manufacturer in order to provide evidence of reliability and validation. Procedural standards are very common in software applications.

3. Safety-Critical Subsystem - Practice

In most industries (except highway transportation), consideration of system safety begins with a hazard analysis in which possible accidents are identified by determining how often the accident would occur, the negative effects of the accident, and what could be done to avoid such an occurrence.

Some of the components which lead to disasters or accidents may be eliminated by changes in design, or, the consequences could be ameliorated in an iterative design-hazard analysis process. There will remain a safety-critical subsystem on whose integrity freedom from disaster relies. The roles of operational and maintenance procedures and management, replacement planning, and similar matters must also be considered.

Once the hazards have been identified, both designers and analysts will tend to equate system safety with freedom from the defined hazards. The Preliminary Hazard Analysis (PHA) provides the basis for agreement on hazards and is thus an extremely important document. Both the standards and the experience of practitioners emphasize that managerial procedures are significant. Designers and operators must confer with the safety analysts at a senior management level, and the PHA becomes an early member of a very large set of documents which are defined in great detail in the standards.

There are two kinds of existing standards relevant to this process (there are some about hardware, some about software and a few systemwide). There are procedural standards which describe the analytic process, how its management and documentation should be linked to design, and later arrangements for management of the whole if there is maintenance, updated design or new requirements. There are also other process and procedural standards specifying proper methods for using some of the analytic tools used in the analysis, which go by such names as risk analysis, failure mode and effect analysis, and fault tree analysis. A brief listing is included in the Appendix.

Carrying out these techniques may require some knowledge of how drivers perceive and react to warnings in general, or to particular kinds of warnings in various situations. This is not a topic on which there is a systematized body of knowledge. Consequently it is not possible to write product standards. STAMMI (4) proposes performance standards, but there are legal problems as mentioned previously. Further, accidents represent extremes, and may well reflect extremes of behavior at the man-machine interface. Additionally, drivers are not a homogeneous group. Mean behavior is therefore not an appropriate performance criterion, which may mean that the cost of a reproducible measurement of driver performance is prohibitive. There are a great many unresolved problems here. They stretch wider than a concern with standards. However, discussion from a standards perspective can add valuable precision to the whole.

Clearly it is important that the safety-critical subsystem be identified, so that it is not modified without consideration of the effect on safety. Also the rest of the system must be segregated from the safety-critical subsystem.' This must ensure that parts external to the safety-critical subsystem can affect it only in the planned ways. An example may be in order. The control rods in a nuclear reactor should react to a rapid change in coolant pressure, which is a sure precursor of a hazardous condition. If there is an auto-control system within the safety-critical subsystem they might react to a small change in coolant temperature, which it is desirable to maintain constant on efficiency grounds. In no circumstances, however, should they be affected by a negotiation over the price of power exported to another state, even if some communication device develops a fault.

There must therefore be some form of modular design with defined interfaces and communication protocols between components, especially between safety-critical components and all other components. In some cases (particularly defense, avionics and aerospace) it is. in practice, possible to define the safety-critical subsystem at the beginning of the design process and then apply the appropriate procedures to the development of each of its modules. (It needs

to be checked that there are no safety-critical components outside the subsystem as initially conceived.) The standards do not expressly require this, but some seem to be written in terms which assume it. All tacitly assume a modular approach to design and definition of a safety-critical subsystem. In IVHS, where many people active in the field are not familiar with the hazard-analysis approach, it may be wise to delineate this approach expressly in standards.

4. Software

Increasingly, computers enter into the safety-critical subsystem. As hardware, they can be analysed in terms of concepts (e.g., mean time between failures) which apply to other components. But software does not fail: it is either always correct in all ways or it was always faulty (i.e., contained a "bug").

Thus software requires both verification to be confirmed as conforming to specification, and validation, to be confirmed as doing what the customer requires. If, as often happens, the spec does not reflect what is wanted, it may be verified but not validated. (There is also the problem of ensuring that what the customer wants is what he/she needs to ensure safety. Hazard analysis techniques may be beneficial here.)

If the software is at all complex, validation and verification cannot be done by carrying out tests. Until recently, elaborate procedural standards laid down techniques by which code should be written, verified, certified and documented basically by requiring the system or subsystem designer or programmer to justify his/her actions in a formal way and/or describe multiple test procedures at different levels of activity. Once again, the procedures only make sense if a modular approach to system design is employed, but few of the standards require this expressly.

More recently, the advent of formal methods in computation offers the future possibility of mathematical proof whether or not a system conforms to specification. It is not likely that there will be any such possibility of proof that the specification contains what should be specified until a mathematically satisfactory definition of the concept "should" can be written unambiguously. The use of formal methods can reveal some errors, however, because they force specifications to be written in a logically complete language.

It is doubtful if it is now possible to seek formal verification for all large software suites, but the art is advancing rapidly. Some procurement agencies, notably in defense, had issued draft standards as early as 1988 requiring formal verification of all code procured. While this may have been intended more to advance awareness of the need to develop skills rather than as a realistic short-term requirement, it does indicate that some use of formal methods may be appropriate in IVHS standards. Certainly the view expressed in an article (5) found in an authoritative US journal was that formal-method standards were the future pattern.

To date, there is no indication that the elaborate procedures, and in particular the extremely laborious requirements for documentation would be relaxed if formal methods had been successfully employed. There are clearly vested interests here in other fields. However, IVHS suffers no such burden.

Communication protocols are another kind of software where IVHS will need standards and where there is a substantial body of experience elsewhere. Much of what has been previously mentioned applies; however, this field lies beyond the scope of this paper.

5. Configuration Management

Once again, it is only implied in most of the standards that system safety is a function of the whole system. It can be discussed to what extent a traffic stream and the highway on which it lies become a system requiring whole-system treatment because of the presence of IVHS devices. If there is full automation, all elements must be treated as a single system. If most vehicles are fitted with vehicle-vehicle communications which have safety functions, once again it is necessary to treat all elements as a single system. But certainly situations can exist in which there is destructive interaction between IVHS devices without express communication. Different devices, for example, each of which attempts to keep the vehicle a fixed lateral distance from its neighbor in an adjacent lane, could clearly lead to a dangerous, unstable oscillation if each device's dynamic responses were inappropriate.

Where there is single ownership, the technique known as configuration management is widely used to avoid difficulties of this kind as well as some others by ensuring that different actors (contractors, offices, manufacturers, etc.) are appropriately advised of the activities of others. There are many standards which describe how this should be carried out, managed and documented.

Eventually something like configuration management may be needed for IVHS. It cannot be administered like other schemes because there is no single owner responsible for the whole. The need is not urgent. If a future demand for descriptions of devices on the road now can be foreseen, however, it may be wise to collect the information while it is readily available.

6. References

1. Jesty, P.H., Buckley, T.F., Hobley, K.M., and West, M. "Review of Current Standards for Safety Critical Software." School of Computer Studies Tech Rep Series 90.04, University of Leeds, Leeds 1990.

2. Jesty, P.H., Buckley, T.F., Hobley, K.M., and West, M. "Review of Current Practices for Certification of Safety Critical Software." School of Computer Studies Tech Rep Series 90.05, University of Leeds, Leeds 1990.

3. Howarth, C.I. "Psychology and Information Technology," in Technology and People?: Designing for the Future, Cambridge: MIT Press, 1987, pp. 1-19.

4. Parkes, A.M., and Ross, T. "The Need for Performance-based Standards in Future Vehicle Man-machine Interfaces." In Proceedings of the DRIVE Conference, Commission of the European Communities, Brussels, to be published.

5. Gruman G., "Software Safety Focus of New British Standard." IEEE Software Journal, Vol. 6, No 3, 1989, p. 173.

Partial List of Standards

A1. Hazard Analysis - Technique

United States

American Petroleum Institute. "Management of Process Hazards," API Recommended Practice 750, Washington, D.C., 1990.

American Society for Testing and Materials. "Standard Guide for Project Definition for Computerized Systems," ASTM E 1113-86, Washington, D.C., 1986.

European and International

Chemical Industry Safety and Health Council. "Guide to Hazard and Operability Studies," Chem. Ind. Ass., London (undated).

Health and Safety Executive. "Guide to Programmable Electronics Systems in Safety Related Applications: General Technical Guidelines," HMSO, 1987.

Ministry of Defence. "Requirements for the Analysis of Safety Critical Hazards," Interim Defence Standard (Draft) DEFSTAN 00-56, Glasgow, 1989.

A2. Hazard Analysis - Tools

United States

American Society for Testing and Materials. "Standard Generic Guide for Computerized Systems," ASTM E 622-84, Washington, D.C., 1984.

American Society for Testing and Materials. "Standard Guide for Documenting Computerized Systems," ASTM E 627-88, Washington, D.C., 1988.

American Society for Testing and Materials. "Standard Guide for Developing Functional Designs for Computerized Systems, " ASTM E 730-85, Washington, D.C., 1985.

American Society for Testing and Materials. "Standard Guide for Implementing Designs for Computerized Systems, " ASTM E 624-83, Washington, D.C., 1983.

Department of Defense. "Procedures for Failure Mode and Effect Criticality Analysis," MIL-STD-1629A, Philadelphia, 1985.

Office of Nuclear Regulatory Research. "Fault Tree Handbook," Nuclear Regulatory Commission, NUREG-0492, Springfield, Va., 1986.

Office of Nuclear Regulatory Research. "Procedures for Treating Common Cause Failures in Safety and Reliability Studies, " Nuclear Regulatory Commission, NUREG/CR-4780. Springfield, Va., 1988.

European and International

International Electrotechnical Commission. "Analysis Techniques for Failure Mode and Effect Analysis (FMEA)," IEC 56-812, Geneva, 1985.

International Standards Organization. "Information Processing Systems - Open Systems, " IS0 DIS 8807, Geneva, 1987.

Ministry of Defence. "Practices and Procedures for Reliability and Maintainability, " Defence Standard 00-41 (parts 1-5), Glasgow, 1981-9.

B. Software Integrity

United States

American National Standards Institution. "Software Test Documentation, " ANSI/IEEE Standard 829-1983, New York, 1983.

American National Standards Institution. "Software Engineering Standards, Third Edition (SH12534)," IEEE, New York, 1989.

Radio Technical Commission for Aeronautics. "Software Considerations in Airborne Systems and Equipment Certification," DO 178A, Washington, D.C., 1985.

European and International

Health and Safety Executive. "Guide to Programmable Electronics Systems in Safety Related Applications: Introduction," HMSO, 1987.

International Electrotechnical Commission. "Draft - Safety of Programmable Electronic Systems: Generic Aspects." IEC 65A 96, Geneva, 1990.

International Electrotechnical Commission. "Draft - Software for Computers in the Application of Industrial Safety," IEC 65A 94, Geneva 1990.

International Electrotechnical Commission. "Software for Computers in the Safety Systems of Nuclear Power Stations," IEC 880, Geneva, 1986.

Ministry of Defence. "Development of Safety Critical Software for Airborne Systems," Interim Defence Standard DEFSTAN 00-31, Glasgow, 1987.

Ministry of Defence. "Requirements for the Procurement of Safety Critical Software in Defence Equipment," Interim Defence Standard (Draft) DEFSTAN 00-55, Glasgow, 1989.

NATO. "NATO Software Quality Control System Requirements," AQAP 13, Brussels, 1981.

STARTS Public Purchaser Group. "The STARTS Purchaser Handbook: Procuring Software-Based Systems," National Computer Centre Publications, Manchester, 1989.

STARTS Public Purchaser Group. "The STARTS Purchasers Handbook: Software Tools for Application to Large Real Time Systems," National Computer Centre Publications, Manchester, 1986.

C. Configuration Management

United States

Department of Defense. "Procedures for Configuration Management in the Procurement of Defense Materiel," MIL-STD-882B, Philadelphia,. 1985.

IEEE. "Standard for Software Configuration Management Plans," New York, 1983.

Menendez, J.N. "A Guide to Understanding Configuration Management in Trusted Systems," National Computer Security Center, Washington, D.C., 1989.

U.S. Air Force Systems Command. "Systems Management: Configuration Management for Systems Equipment and Computer Programs," Washington, D.C., 1971.

U.S. Army Materiel Command. "Army Programs: Configuration Management, " Washington, D.C., 1965.

U.S. Naval Material Command. "Configuration Management: A Policy and Guidance Manual," Washington, D.C., 1967.

European and International

British Standards Institution. "Code of Practice for Configuration Management of Computer-Based Systems," BS 6488, London, 1984.

Ministry of Defence. "Configuration Management Policy and Procedures for Defence Materiel, " Defence Standard DEFSTAN 05-57, Glasgow, 1985.