Recommendations of Ada for Safety-Critical Software

The following is a compilation by Russ Paielli of several official recommendations of the Ada programming language for safety-critical systems. Note the statements about C and C++.

Software System Safety Handbook - A Technical and Managerial Team Approach, US DoD Joint Software System Safety Committee, December 1999:

> The Ada programming language provides considerable support for preventing many causes of unpredictable behaviour allowed in other languages. For example, ... implicit constraint checks prevent the classic C programming bug of writing a value into the 11th element of a 10-element array.

Motor Industry Software Reliability Association, *Guidelines For the Use of the C Language in Vehicle Based Software*, April 1998:

> Nevertheless, it should be recognized that other languages are available which are in general better suited to safety-related systems, having (for example) fewer insecurities and better type checking. Examples of languages generally recognized to be more suitable than C are Ada and Modula 2. If such languages could be available for a proposed system then their use should be seriously considered in preference to C.

ARINC Report 613, *Guidance for Using the Ada Programming Language in Avionic Systems*:

> It is the desire of the airline community to reduce the cost and the economic risk associated with avionics software systems. As a means to achieve this, it is recommended that the Ada programming language be used as the standard High-Order Language (HOL) in avionics equipment design.

NASA Guidebook for Safety Critical Software (NASA-GB-1740.13-96):

> 5.3.11.8 Programming Languages. ... The Ada subset we have described is suitable for safety-critical systems. ... The choice of C is to be avoided for our domain of interest because the language lacks the features that permit robust, reliable programming.

CENELEC European Railway Standards, Table A15:

> R = Recommended
> HR = Highly Recommended
> NR = Not Recommended
> - = no position

Safety Integrity Level →	0	1	2	3	4
Ada	R	HR	HR	R	R
Ada subset	R	HR	HR	HR	HR
C/C++ (unrestricted)	R	-	-	NR	NR
C/C++ subset with coding standards	R	R	R	R	R