Development Methods for Trusted Computer Systems

Martyn Thomas
Praxis Systems plc, 20 Manvers Street, Bath BA1 1PX, United Kingdom

Key words: Safety critical computer systems; Trustworthiness; Good practice; Formal methods

Introduction

Should we trust computers, and if so, to what extent? This is one of the most important questions facing our industry. It will be asked more and more often, and it is highly desirable that we, the professionals, agree on our answer and are able to justify it.

Whether or not we should trust computers, the reality is that we - society - behave as if we trust computers more every year. We trust computers with our privacy, with our money, with the defence of our country, and with our lives. Few of us, perhaps none of us, realise how widespread is the trust we place in computer systems and in the men and women who design and implement them.

In this paper, I shall show that critical computer systems are already widespread and that their use is growing rapidly. I shall describe the main reasons why computers are used for these applications, and consider some spectacular failures and whether or not we should be concerned. I shall then review a few technical approaches to developing critical systems, and attempt to present an overall picture of the state of the industry. Finally I shall suggest that some urgent actions are needed.

Much of this paper involves safety, and this raises a great difficulty. It is not my wish to create public alarm, or widespread fear of computer systems in safety-related applications. Indeed, I want to say at the outset that I do not believe that such alarm or fear is justified. Nevertheless, sensational press reporting of previous public discussions of safety issues has caused problems, which
have greatly reduced the extent to which computing professionals are willing to reveal details of safety-related systems — and especially of failures in such systems. Yet, if we are to decide the degree of trust which can be placed in computer systems, and if we are to understand the contribution which different development techniques bring to the safety of a system, we must have information and the freedom to discuss it.

The examples of failures which I give are not to be taken as criticism of any specific person, company or product.

Some Trusted Systems

I describe below a few of the applications where computer systems are implicitly trusted by society. In each area, the incorrect behaviour of the computer system would significantly increase the risk of a failure, possibly with serious consequences. In most of the areas below, the computer system is only part (and often a small part) of the total system. Often, the designers of the system have provided back-up mechanisms to minimise the effects of a failure in the computer system. I consider later a few of the important ways that system designers seek to ensure the integrity of their systems; the purpose of this section is to illustrate by example the degree to which we already trust systems which contain computers, and the possible consequences if that trust is unjustified. I also attempt to show the rate at which new, trusted computer systems are being developed.

Civil Aviation

Computers are used extensively in civil aviation. On the ground, they are used for a wide range of purposes, from controlling airfield lighting to the air traffic control systems which provide the controllers with radar plots and aircraft details. A new computer system will soon be introduced which will automatically detect and report on potential collisions between aircraft in the controlled airspace over London. It is believed that this will permit the London airspace to become even more congested without compromising its excellent safety record.

In the air, computer systems are used (inter alia) for navigation, engine control, and automatic takeoff and landing. In the Boeing 757 the instrument panel has been replaced by VDUs, with computer-generated instrument displays. In the Airbus A320 (which has recently come into service) the computer systems have full authority over the aircraft’s controls, in three dimensions: the pilot is not moving the ailerons directly, for example, but through a computer which will override the pilot if the control movements are beyond those it has been programmed to accept. The first Airship with a full-authority computer control system was demonstrated in October 1988.

On the A320 Airbus and the next version of the Boeing 747, the three-man crew has been reduced to two by eliminating the role of the flight engineer. To a first approximation, computers are being given the flight engineer’s job of monitoring the vital systems.

Civil airliner systems are among the most safety-critical, as a serious accident to a wide-bodied jet could kill 300-400 people.