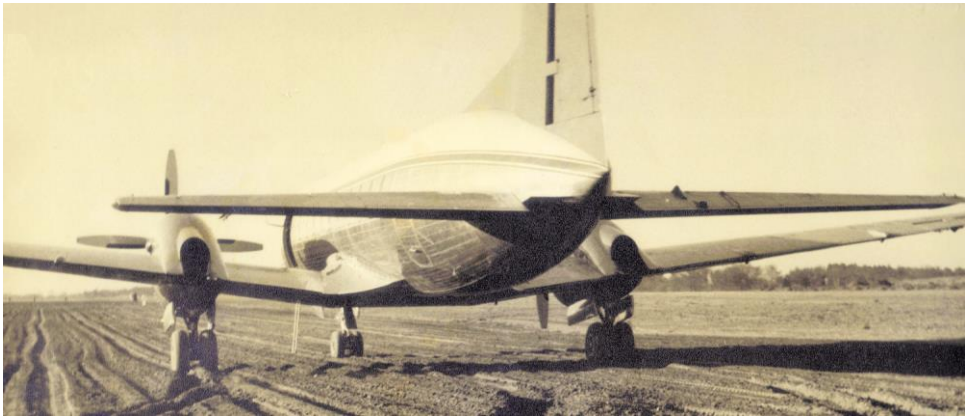
Planes and Computers



Stan Price has recently published his autobiography "Trains, Planes and Computers" chronicling his long career in systems safety, from designing, auditing and testing safety-critical systems through to research into making them safer and even acting as an expert witness in court. Stan shares some of his thoughts and insights from working in the discipline for over 30 years.

The Prehistory of System Safety

Even before systems safety, and in particular, the probity of software, became a specific topic, those involved in such systems, including myself, were well aware that systems could kill and maim. It was around 1968 when I was first responsible for a safety-related system. It was for the production of the Operating Data Manuals (ODMs) for the then current Manchester (AVRO) designed aircraft – the Nimrod and 748. The ODMs, as the name suggests, indicated to pilots how the aircraft could safely be operated and consisted largely of tables. For example, they indicated minimum runway lengths at particular take-off weights, airfield altitudes and ambient temperature. For each phase of flight, e.g. take-off, cruise, or climb, there were three programs in the process of producing the relevant part of the particular aircraft's ODM.

The first of these calculated engine performance, which was then used by the second program to calculate raw aircraft performance data. The final program in the suite sorted this raw data into the table that went into the ODM. This presented unique formatting problems, in particular, as the environment got more arduous – hotter and higher; the aircraft could not operate there, so there was no entry in that part of the table.

Obviously if the data in the ODMs was inaccurate and was acted upon, there was a danger that safety could be compromised. Indeed my ODM system came under suspicion when two aircraft slid off the same runway in the same afternoon. Fortunately for me, the problem was an inaccurate hand-produced correction figure for the landing distance required on wet grass.

A Move to Air Traffic Control

Late in 1972, I moved into the realm of Air Traffic Control (ATC), with its obvious safety implications, and was responsible for judging that a projected system's software was of such poor quality that safety would be again compromised.

It was a system for assisting controllers in knowing more exactly the sequence of aircraft landing at Heathrow. This involved calculating the timing and speed of aircraft leaving the four stacks so that the spacings when they landed on the runway were the minimum commensurate with safety, and hence its use was optimised.

A prototype of the system was being developed by the Royal Radar Research Establishment at Malvern. One of my software engineer colleagues, Dave Neumann, and I visited Malvern and viewed the system. We discovered the software was very poorly written. It had no structure and comments were also non-existent. Its documentation was also very limited. Dave and I therefore reported this, and the project was cancelled. Its quality was so bad that any deep consideration of safety was unnecessary. I feel generally that the quality of software has improved over the years since, and particularly, where relevant, with the focus on safety.

My major involvement in ATC systems was in the UK's acquisition of the US en-route ATC computer system (the 9020 Project). Even though the original system would not, in its US operational life, handle aircraft flying east of the Greenwich Meridian, the specification allowed for the possibility. But it appears that this was never tested before going operational in the US; but upon testing in the UK, it folded the country over at the meridian. For example aircraft flying over Ipswich were being shown as being over Bedford. Hardly safe, defeating the whole purpose of ATC – to stop aircraft colliding. Suffice to say this was corrected before the system went operational. The principal lesson to be drawn was the dangers of assuming that a system that was safe in one domain does not mean it will be safe in another.

An Expanding Role

Later, I was involved in a police command and control system. This would have the purpose of real-time allocation of police assets to incidents requiring their attention on a geographic basis. Misallocation could mean that some safety-critical incidents would not be attended to thus diminishing safety. My role would be a key one in choosing the contractor to implement the system and then oversee its installation.

Next, I was asked to monitor three projects in the DTI/Research Council Safety-Critical Systems Research Programme. I also believe the Programme spawned the SCSC Club. The projects were:

MORSE – A Method for Object Re-Use in Safety-Critical Environments with partners University of Cambridge, Lloyds Register, West Middlesex Hospital, Transmitton, Dowty Controls and British Aerospace Airbus

SPAM – Investigating Security Paradigms Validity for Safety-Critical Environments with partners EDS-Scicon and Lloyds Register

PRICES – Productivity, Integrity & Capability Enhancement for Software, and Human Factors in Safety-Critical Systems Development involving Open University, City University, Lloyds Register, Rolls- Royce, Bae SEMA, G P Elliot Electronic Systems and Analysis Consultants.

By this time (1994) the pro-active consideration of safety using techniques such as HAZOPS etc had become much more structured and mandated replacing the simple "does it meet the spec" criteria of yesteryear.

What goes on out there?

Subsequently I performed a coordination role within the Programme including two initiatives, which I conceived and got funding for. One of these initiatives was a series of workshops devoted to specific topics, which I considered, were of key relevance to successful and particularly safe systems. My judgement on what was key was heavily influenced by my previous industrial experience. To make the workshops manageable, the number attending was restricted to twenty or less, split equally between academia and industry, largely but not exclusively, drawn from participants in the safety-critical programme, participants that I rated.

I chaired the workshops, and each had a rapporteur who produced a report chronicling the proceedings and the conclusions. This was circulated to the attendees for their comments, and a final version incorporating these was then published. The workshops were opened by myself with an introduction that cited the purpose of the workshop and its format.

The latter, after the introduction, consisted of presentations from the safety-critical programme projects that were relevant to the topic of the workshop. These were followed by comments on the presentations from the so-called catalysts (chosen to stimulate discussion), which led into general discussions followed by a summary.

The initial workshop, under the title, 'What goes on out there?' addressed the gulf between what the research community thought happened in day-to-day industrial/commercial practice and what actually happened. As well as the DTI sponsorship of the workshop, it also ran under the auspices of the SCSC, and over the years, I also made contributions to several of its events.

"… the deliberations at these workshops and their proceeds had a degree of influence particularly in the hitherto neglected topics of Human Factors and Data."

The other workshops that followed the initial one addressed the following, in relation to the safety of systems:

- Human Factors
- Software Requirements Elicitation and Capture
- System Assessment
- Artificial Intelligence
- Process Models
- Data

I believe that the deliberations at these workshops and their proceeds had a degree of influence particularly in the hitherto neglected topics of Human Factors and Data.

Expert Witness

My final professional contribution to the safety-critical world came as an expert witness in a court case around 2001.

Electronic Data Systems (EDS) was contracted to supply to the Civil Aviation Authority (CAA) a new computer system at Prestwick in Scotland to support the control of air traffic over the

North Atlantic. The CAA cancelled the contract after the design milestone, citing non-performance on the part of EDS and EDS took the CAA to court for some forty-two million pounds. Because of my air traffic control and computer background, I was approached directly by EDS's solicitors to be an expert witness for them.

Curiously, this was not so much for my system development expertise; a team of three other experts was handling that, but on the safety issues in the case. EDS's legal team believed that the CAA might play the safety card. Unfortunately, my other commitments at the time meant I could not really take up the assignment, and at first, I said no. However, the fee I was eventually offered, a four-figure day rate, plus an agreement that I could employ a researcher, made me change my mind.

The researcher I employed was John Smith, who had been the Plessey manager involved in the 9020 Project during my days with the Civil Aviation Authority, and who had subsequently produced the safety case for the London Air Traffic Control Centre.

Insofar as John's and my inputs to the case were concerned, they were significant in two respects. Firstly we smoked out the fact that the first part of four of the CAA's safety procedures amazingly did not exist, and therefore, their criticism of EDS's safety processes in the case was therefore unrealistic, to say the least. Secondly, in my initial report, I had pointed out that there was no common agreement on how safety should be built into software systems, so their criticism of what EDS was doing was not necessarily valid. The CAA retorted that there was agreement and cited numerous standards. To this, I asked the simple question: if there was a common approach, why was there a need for so many standards, which in some areas were even contradictory.

"… if there was a common approach, why was there a need for so many standards…"

Are We There Yet?

This may not be the situation now, but as a distant observer in retirement of the safety-critical systems scene, I am amazed that unsafe systems are still going operational. Two significant ones that come to mind are the Boeing 737 MAX [2] and the so-called smart motorways [3]. It may well be, at the technical level, that we are now much better at ensuring safety, but until we stand up to the financial and political pressures sometimes put upon us, our detailed work will come to nought.

References

[1] Trains, Planes and Computers, https://www.amazon.co.uk/Trains-Planes-Computers-Executive-Pass/dp/1802271252, Stan Price, 2021, ISBN: 978-1-80227-125-6 and 126-3

[2] Boeing 737 MAX – Safe to Fly? Paul Hampton & Dewi Daniels, Safety Systems Volume 29, Number 1, Feb 2021 https://scsc.uk/scsc-162

[3] How Smart Are Our Motorways? John Ridgway, Safety Systems Volume 28, Number 2, May 2020, https://scsc.uk/scsc-158

Top image: AVRO748 undertaking rough airfield trials at RAF Martlesham Heath now BT Research.

Stan Price spent over 40 years developing, evaluating and researching IT systems – many of them safety-critical principally in the Aviation sector. He is a Chartered Engineer and Member of both the Royal Aeronautical Society and British Computer Society. He has performed visiting posts with Sheffield and Salford Universities and given evidence in over 40 court cases involving IT.