Rapporteur's report on Session 2: Human Factors in Dependability and Resilience

This report covers the two papers originally scheduled for this session, by Harold Thimbleby and Roy Maxion. The presentation of the Dr. Thimbleby's paper was delayed until later in the afternoon for personal reasons.

Roy's paper, "Trial by Camera: Are you My Accuser, or is it the Software?" looked at the human factors involved in the acceptance of expert testimony by US judges, who are supposed to act as gatekeepers for such evidence. The rules that judges are instructed to use for deciding on the admissibility of such evidence (the "Daubert" rules) consider five factors: testability, peer review, error rate, standards, and general acceptance. Roy provided details concerning a particular case involving photographs found on a laptop. In this case, software provided by the FBI was used to identify whether a particular camera was used to take particular incriminating photos. This evidence was accepted by the judge, the defendant was convicted, and he faces a lengthy prison term.

Roy found that the FBI software in question was less dependable than the court seemed to appreciate. Specifically, a witness accepted as expert by the court testified to a false positive error rate of one in a million, based on test procedures that were methodologically flawed. Roy's own tests indicated a false positive error rate on the order of one in eight. He concluded that courts that must evaluate the credibility of technical evidence are often ill-equipped to do so. Roy raised the question of what the technical community can do to address this situation. He noted the importance of methodology in research and provided a judicial gatekeeping checklist that could improve matters. He also noted ways in which our community might assist the judicial community to be more effective gatekeepers, for example by providing guidelines for proper testing of forensic software, along with a detailed experimental method for doing so.

Harold's paper, "Human contributions to dependability and trustworthiness," covered a wide range of examples where there have been faults he categorized as human-made, non-malicious, and incompetent that have led to unfortunate problems. He argued that the dependability community needs to acknowledge and deal with these problems. Among them were the infamous British Post Office "Horizon" scandal in which hundreds of innocent postal workers were wrongly charged and in many cases convicted and imprisoned, healthcare examples in which innocent nurses were wrongly accused of neglect, and issues with screen-based automobile interfaces that warn the driver not to look at the screen while driving, but then demand exactly that.

Harold noted the general failure of software manufacturers to provide warranties for their software or certification for their programmers and concluded that without a warranty one can only conclude that the software is not dependable. He concludes that we need dependable systems, in general, and that we have to take unconscious incompetence into account, including our own. He noted the need for us to oppose the popular culture that routinely accepts undependable systems and advocated both for legislation to address these issues and for better underlying theories to facilitate the development of dependable systems. In short, Harold argued that dependability as a field needs work out how to get itself implemented dependably given human nature, both personal human factor problems and sociocultural ignorance —

otherwise we are just talking to ourselves and not achieving the aims of dependability in the real world.

As rapporteur, I see as the primary message of both of these papers the need for the dependability community to increase its involvement with the policy and decision-making communities. The problem is most often that even though there is the know-how to build systems that are more dependable, the marketplace lacks the incentive to produce them. I have been concerned with this problem myself, primarily in the context of cybersecurity, over the past fifteen years. For the 29th Cambridge Security Protocols workshop held in March 2025, I produced a paper that looked for examples of success in aligning public policy with safety and security concerns, entitled "Sparks, Carrots, and Sticks." The paper briefly reviews experience with building codes for physical structures, auto safety regulation in the US, and aviation safety regulation. My conclusion is that both incentives and penalties are important policy tools, but in order for them to be put in place, some kind of "spark" event is required. Although the British Post Office scandal and countless cybersecurity incidents might have been expected to provide such sparks, they have so far failed to kindle the blaze required for effective action.

The proceedings of that workshop are to be produced by Springer Nature, but apparently not until September 10, 2026 (!). For reference: Softcover ISBN 978-3-032-30503-9, eBook ISBN 978-3-032-30504-6. I will be happy to provide preprints to members of this group.

Carl Landwehr