Constructor Autonomy

Design. Software Safety.[1]

Details Diane Wiltse was an experienced systems designer working for the Acme Software Company. A year ago Wiltse was assigned to work on a project[2] which involved building a system that monitors radar signals and launches missiles in response to these signals.

Wiltse initially had some reluctance about working on a military project[3]. When the project was approaching completion Wiltse had some grave reservations about the adequacy of the design. Wiltse was doubtful about the system's capacity for making fine distinctions (e.g., distinguishing between a small jet aircraft and a missile). It would be catastrophic, Wiltse reasoned at the time, if the system responded to a non-threat as a threat (a "false positive").

Wiltse documented these concerns[4] carefully, including an explanation of analysis and design weaknesses and naming specific modules to be revised to strengthen software safety against false positive target identification.[5]

Wiltse took the documentation and concerns to their immediate supervisor, Heather Michelfelder, the project director; but Michelfelder dismissed these concerns quickly[6]. Michelfelder tells Wiltse to put their concerns into a memo entitled "Future Enhancements," and suggested that this will become part of Acne's bid for an anticipated second phase of development.

Wiltse was convinced that it would be a serious error to let the system go to trials as is. They were especially concerned that Acme might never get to do the necessary improvements because another company might win the bid for the second phase.[7]

Having weighed up the consequences[8] of speaking out, Wiltse did write the memo, filed it with the project documentation, and finished the design and build. The software was duly completed for trials and put onboard the vessel *Wabash Val-de-Marne*.

During the sea trials the software registered a small unidentified aircraft slightly before the testing drone was due to appear; a missile was launched.

A private light aircraft that had inadvertently flown into the testing area, Yan Fuzi, Kong Zhengzai, Sima Hui, and Yen Qian[9] on their way to a nearby island for a holiday were killed.

A false positive.

Cast	Role
Yan Fuzi	Kongzi family
Sima Hui	Kongzi family
Heather Michelfelder	Project Director
Yen Qian	Kongzi family
Diane Wiltse	Systems Designer
Kong Zhengzai	Kongzi family

Table 1: C_1 Cast

[1] Based on an actual event related to me and eerily similar to: Johnson, D.G., 1985, Computer Ethics, p.163, Scenario 7.1.

[2] Acme and Wiltse have signed secrecy agreements but the word in the industry is that it was the U.S. Department of Defence. We tried to find out the names of the actual people that Michelfelder dealt with but were unsuccessful.

[3] But put this out of mind because the project was technically challenging and that if they didn't work on it, someone else would. The money was alright as well.

[4] Which included the fact that the system designer's did not take into account the actual users of the software (partly because Wiltse was denied access to them) nor the conditions in which it would be used.

[5] Wiltse estimated that the detailed analysis, design, implementation, and testing of these changes could be done in approximately six months with the existing staff.

[6] Acme was already behind schedule and had exceeded their budget.

[7] The system was (mostly) a success in terms of budget, schedule, and requirements satisfaction.

[8] For themselves, they might get fired, and besides, surely the weakness would be obvious during sea trials and be corrected then.

[9] The Kongzi family.