
Contribution ID: **248** Type: **not specified**

# Throwing Cinderblocks at Safety Engineering

*Friday, 20 September 2024 17:25 (25 minutes)*

If a bug is a violation of expectations, a safety bug is a violation of expectations that places the user at an elevated risk of injury. From this perspective there is little distinction between Safety Engineering and Security Engineering; a safety bug can arise from a failure to perform, regardless of engineering discipline. Yet, the practice of each discipline is driven by opposing philosophical viewpoints. Where Safety Engineering seeks to develop deterministic behavior under specified conditions, Security Engineering is tasked with defending against generally unspecified conditions.

In this talk, Chuck will review the Cinder Block Problem and explore the philosophical underpinnings of Safety and Security Engineering. He will use the distinction between safety hazard and security threat to establish positive (”shall”) and negative (”shall not”) views of engineered systems. Chuck will use these views to show that safe systems are not necessarily secure and secure systems are not necessarily safe. Striking a feasible balance requires an understanding of each view and the independent application of these philosophically opposed engineering disciplines.

**Primary author:** WOLBER, Chuck

**Presenter:** WOLBER, Chuck

**Session Classification:** Safe Systems with Linux MC

**Track Classification:** Safe Systems with Linux MC