Assurance-Based Development (ABD) is the synergistic construction of a critical computing system and its assurance case. The assurance case is an argument that sets out the dependability goal for the system, the evidence needed to support it, and how that evidence is combined to justify the assurance claim. Because the system and its assurance case are developed in parallel, software developers can make technology choices that address the specific dependability goal of each component.

This approach gives developers: (1) confidence that the technologies selected will support the system’s dependability goal and (2) flexibility to deploy expensive technology, such as formal verification, only on components whose assurance needs demand it. ABD simplifies the detection—and thereby avoidance—of potential assurance difficulties as they arise, rather than after development is complete.

In this presentation, I will present the details of Assurance Based Development together with a detailed example of its use.