Safety and Reliability are two of the most important life-cycle properties that any Airborne Wind Energy (AWE) system must exhibit. Many hazards can be present during the operation of an AWE system including potential collision of the unmanned aerial vehicle (UAV), failure of the automated control system and entanglement of the tether connecting the UAV to the ground station. These hazards could lead to accidents that result in severe financial losses and harm to people and wildlife. Safety and reliability in the engineering and operation of AWE systems are thus essential to the success of this technology.

Like in many areas of technology today, AWE is experiencing a fast pace of technological progress, an increase in complexity and coupling between subsystems and more complex relationships between humans and automation. These represent significant changes in the types of systems we are attempting to build today and the context in which they are being built. These changes are stretching the limits of safety engineering. Therefore, the technical foundations and assumptions on which traditional safety engineering efforts are based are inadequate for the complex systems we are building today such as AWE systems.

The world of engineering is experiencing a technological revolution, while the basic engineering techniques applied in safety and reliability engineering, such as fault tree analysis (FTA) and failure modes and effect analysis (FMEA), have changed very little.

This paper introduces a new approach to building safer systems developed by Prof. Nancy Leveson at MIT [1] that departs in important ways from traditional safety engineering. The new model called STAMP (Systems-Theoretic Accident Model and Processes), changes the emphasis in system safety from preventing failures to enforcing behavioral safety constraints. Component failure accidents are still included, but the conception of casualty is extended to include component interaction accidents. Safety is reformulated as a control problem rather than a reliability problem. This change leads to much more powerful and effective ways to engineer safer systems, including modern complex sociotechnical systems such as the one in the area of AWE.

We will perform a hazard analysis on an AWE system that is currently being developed by a team of MIT students using a new approach to hazard analysis based on the STAMP causality model, called STPA (System-Theoretic Process Analysis). Our presentation will demonstrate how the application of STAMP and STPA leads to engineering and operating safer and more reliable AWE systems and overcome some of the limitations of traditional safety engineering techniques widely used today including Fault Tree Analysis, Event Tree Analysis and HAZOP.

References: