Safety Analysis of AWE Systems

Carlos Perez-Damas, Burak Gozluklu, Arlette Reyes

cdamas@mit.edu

Abstract

Safety and Reliability are two of the most important lifecycle properties that any Airborne Wind Energy (AWE) system must exhibit. However like in many areas of technology today, AWE is experiencing a very fast technological progress and an increase in complexity/coupling between subsystems and more complex relationships between humans and automation. Thus traditional safety engineering efforts, such as FTA & FMEA, are strained to keep up with the complex systems we are building today.

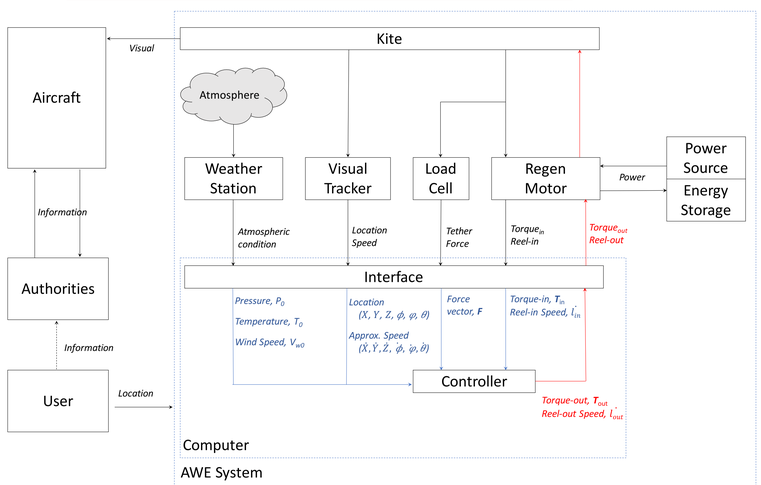
This paper introduces a new approach to building safer systems developed by Prof. Nancy Leveson at MIT [1] that departs in important ways from traditional safety engineering. The new model called STAMP (Systems-Theoretic Accident Model and Processes), changes the emphasis in system safety from preventing failures to enforcing behavioural 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.

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 paper 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.

How STPA Differs?

- Defines safety as a control problem (vs. failure problem)
- Applies to very complex systems
- Includes software, humans, operations, management
- Based on general systems theory + systems engineering
- Expands the traditional model of the accident causation (cause of losses)
  - Not just a chain of directly related failure events
  - Losses are complex processes

General AWE System Architecture



Failure Modes

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order	Stopped too soon/ applied too long
Information From AWE User To Authority	Not information about AWE location	Wrong information about AWE location	Information went to authority **after aircraft takes off**.	
Information From Authority To/From Aircraft	Lost communication	Wrong Information	Too late information about the Kite.	Not-updated info
Location of the AWE	Not determined	Wrong Information	Lately decision on the location	
Visual of Kite to Aircraft Pilot	Kite cannot be seen on course		Too late observation of kite on course	

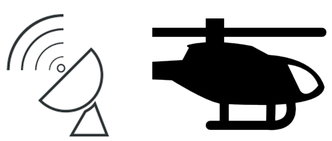
Hazard : Collision of Aircraft with Kite

Analysis

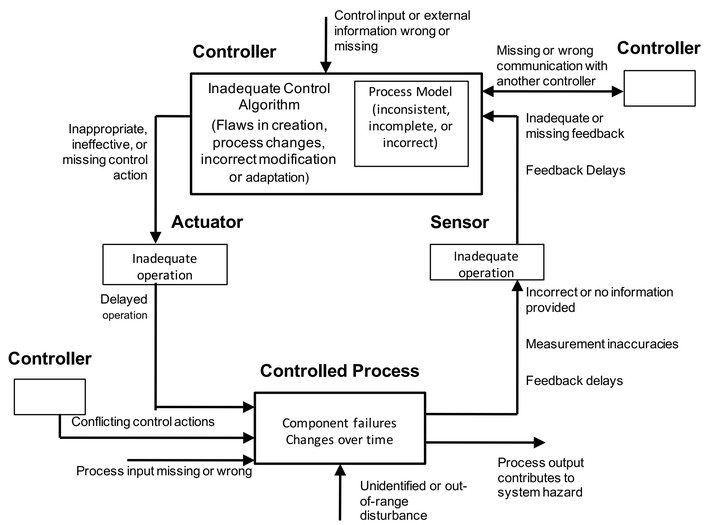
Generated Requirements:

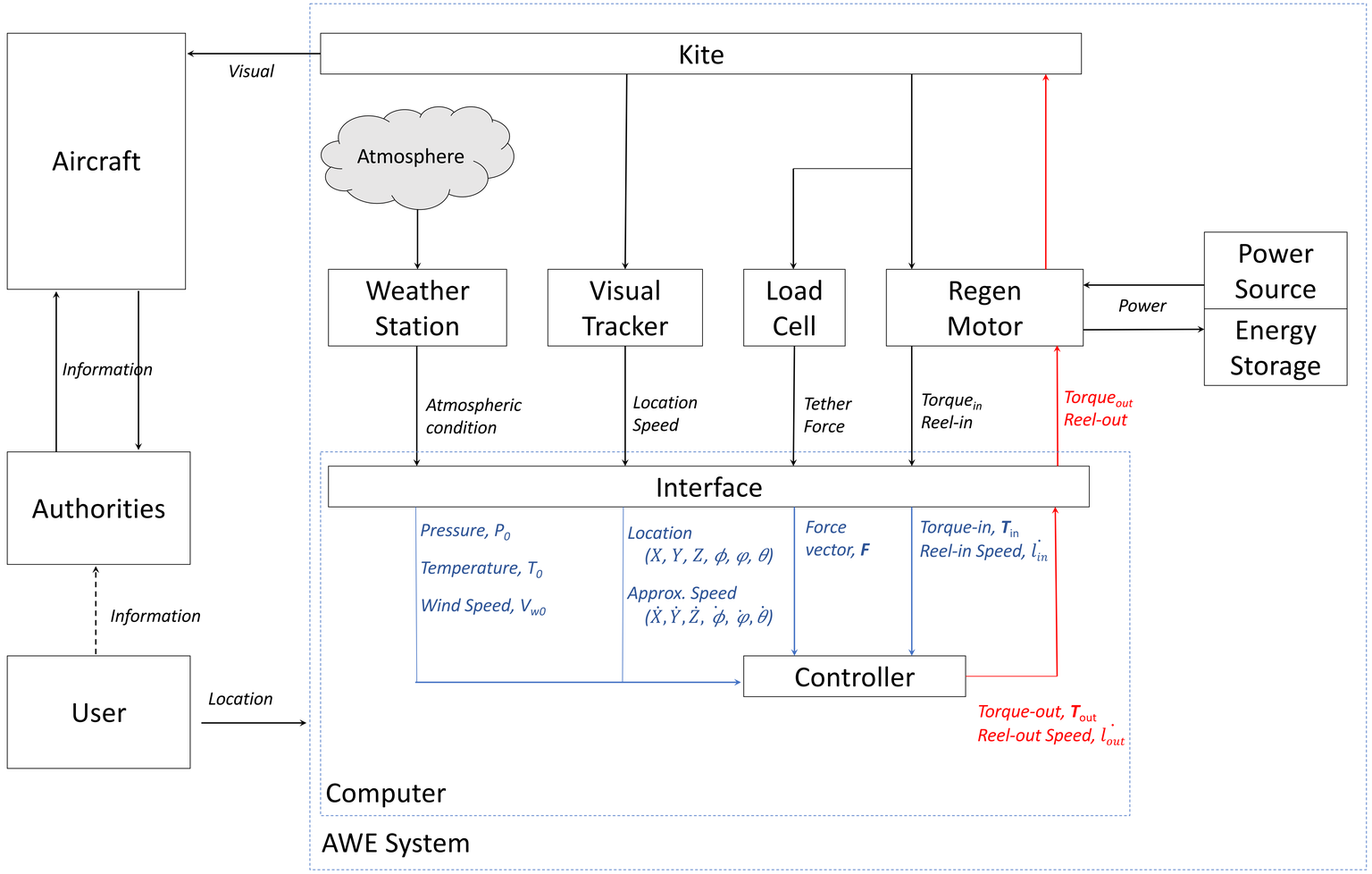
- Inform authorities
  - Attain confirmation before each operation
  - Notify within **X** weeks
- Regular location monitoring
- Illuminate kite and tethers to be visible within **X** m

Result



- Emergency Retraction system
- Release of tension on tethers




Aircraft
Visual
Kite
Atmosphere
Weather Station
Visual Tracker
Load Cell
Regen Motor
Power Source
Power
Energy Storage
Information
Authorities
Information
User
Location
Atmospheric condition
Location
Speed
Tether Force
Torque$_{in}$
Reel-in
Torque$_{out}$
Reel-out
Interface
Pressure, P_0
Temperature, T_0
Wind Speed, V_{w0}
Location
$(X, Y, Z, \phi, \varphi, \theta)$
Approx. Speed
$(\dot{X}, \dot{Y}, \dot{Z}, \dot{\phi}, \dot{\varphi}, \dot{\theta})$
Force vector, $\boldsymbol{F}$
Torque-in, $\boldsymbol{T}_{in}$
Reel-in Speed, $\dot{l}_{in}$
Controller
Torque-out, $\boldsymbol{T}_{out}$
Reel-out Speed, $\dot{l}_{out}$
Computer
AWE System