Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

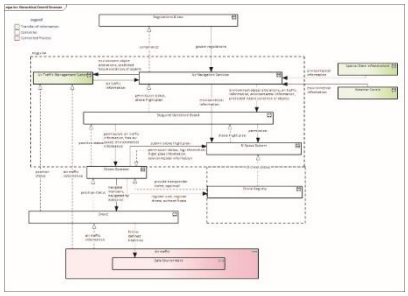
IAMP Institut für Angewandte
Mathematik und Physik

Safety & Cyber-Security Analysis based on Systems-Theory

Diplomandin
Carmen Frischknecht-Gruber

Dozierende
Monika Ulrike Reif
Sven Stefan Krauss

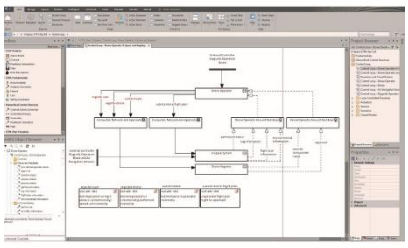
Aufgrund der sich immer schneller entwickelnden Technologie und komplexer werdenden Systeme gelten hohe Ansprüche an die Sicherheit ebendieser. Die Sicherheit vielschichtiger Systeme kann durch präventives und proaktives Handeln gegeben werden. Um Sicherheit zu gewährleisten, werden Sicherheitsanalysen benötigt, welche auf einer abstrakten Ebene funktionale Zusammenhänge und Datenflüsse analysieren können. In dieser Arbeit wird anhand der U-space Fallstudie, ein Registrierungs- und Ordnungssystem für den Luftverkehr von Drohnen und zukünftig auch autonomen Drohnen, die Praktikabilität und die resultierenden Analyseergebnisse der sicherheitstheoretischen Methoden STPA (System-Theoretic and Process Analysis) und STPA-Sec (Security) untersucht.



Die Grafik zeigt die hierarchische Kontrollstruktur des U-space.

Die Ergebnisse dieser Arbeit werfen generelle Fragen bezüglich der Umsetzung des U-spaces auf und zeigen das Fehlen von proaktiven Sicherheitsmechanismen auf. Aus der verwendeten Analysetechnik STPA-Sec ergeben sich zusätzlich zu den Safety Constraints Security Constraints, welche in der regulären STPA-Analyse nicht berücksichtigt wurden. Was mit ein Grund ist, wieso STPA-Sec vielversprechende Ergebnisse liefern kann.

Die Auswertung der Expertenumfrage bezüglich Sicherheitsanalyse-Ergebnisse hat ergeben, dass die vorliegenden Resultate realistische Aussagen machen und mehrheitlich von grosser Relevanz sind. Die Verwendung der Technik STPA-Sec scheint ein guter Ausgangspunkt für die Untersuchung von komplexen Systemen zu sein, jedoch sollte diese mehr als Grundgerüst dienen, und es müssten weitere Methoden aus dem Bereich Safety und Security hinzugezogen werden, um das System in der Tiefe zu untersuchen.



Die STPA-(Sec) Analyse wurde mittels der Software Extension SAHRA für Enterprise Architect gelöst.