Unsafe Control Actions in Autonomous Navigation Systems: A SysML Based Analysis for Enhanced Safety

Raheleh Farokhi, raheleh.farokhi@aalto.fi
Sunil Basnet, sunil.basnet@aalto.fi
Osiris A. Valdez Banda, Aalto University, osiris.valdez.banda@aalto.fi

Research group on Safe and Efficient Marine and Ship Systems, Finland.

Kotka Maritime Research, Kotka, Finland

Raheleh Farokhi

Abstract

The increasing complexity of autonomous navigation systems (ANS) poses significant challenges to ensuring safety and reliability, particularly in dynamic and high-risk environments. This paper presents a SysML-based STPA methodology that enhances hazard analysis efficiency, traceability, and integration within system design. Unlike traditional approaches that rely solely on STPA control structures, this method replaces them with SysML diagrams, providing a more structured and dynamic representation of system interactions over time. Sequence Diagrams are used to explicitly depict control actions and feedback, improving the identification of unsafe control actions (UCAs) and their causal factors, such as software errors, communication failures, and human errors. Additionally, this approach explores loss scenarios, which have not been addressed in previous studies. The proposed methodology is applied to an ANS operating in winter conditions in the Baltic Sea. This integration of SysML and STPA offers a unified framework for system and safety engineering, reducing analysis time while improving scalability and applicability to complex autonomous systems.

Implications for sustainable maritime operation

The proposed SysML-based STPA methodology contributes to sustainable maritime operations by enhancing the safety and reliability of autonomous navigation systems (ANS), particularly in challenging winter conditions. By integrating system modeling with structured hazard analysis, this approach enables earlier detection of potential failures, reducing the risk of accidents, environmental harm, and costly disruptions. The use of SysML diagrams improves traceability and understanding of complex system behaviors over time, supporting more informed design decisions that align with sustainability goals. By addressing software, communication, and human-related risks more effectively, the methodology promotes resilient and adaptive ANS deployment, reducing the need for redundant systems and excessive energy use. Furthermore, the reduced analysis time and scalability of the framework support more efficient development cycles, lowering operational costs and resource consumption.