RAS Safety Framework:
A Digital Twin-Based Approach to Assurance of Complex Systems

Johnson Needle N[1]., Douthwaite J[1]., Emre Y[1]., Law J[1]., Hall N[2].

1 Sheffield Robotics, University of Sheffield
2 Health and Safety Executive, UK

KEYWORDS: safety assurance, cobot safety, structured assurance case, digital twin, regulatory compliance

ABSTRACT

There are several standards and regulations that aim to govern the safety of robotic and autonomous systems (RAS), especially where work is done collaboratively with a human. In response to these regulations, new approaches have been developed to maintain an acceptable level of risk in systems with novel human/robot interactions. These approaches apply technologies such as Digital Twins and Machine Learning in new ways to promote safety.

Current state of the art includes methodologies for creating safety cases for autonomous systems, process automation design and monitoring using digital twin, use of a digital twin to collect and process real-time data in safety critical systems, and assessment methodologies that provide structured arguments for reliability.
However, even with these advancements, there is a lack of information or guidance of how to bring these technologies and approaches together to present a clear and convincing argument about the safety of a particular industrial process or system that complies with the regulations.

In this paper, we tackle this challenge head-on, and present a novel RAS Safety Framework which is the first end-to-end Framework to

- Assist with the development of a system safety assurance argument (safety case) using a Digital Twin
- Provide a clear structure for identifying and addressing risks
- Develop the reasoning and provide supporting verification and validation evidence

The RAS Safety Framework consists of three major parts – the overall assurance process, the assurance argument (safety case) and the Rule-Based implementation in the Digital Twin. This Framework solves the problem of lack of RAS safety guidance by providing the structure and processes needed to bridge the gap between safety assurance, systems development, digital twins and industrial automation. In addition, the advantages of this approach, such as adaptability to dynamic risk data, are particularly observed in highly complex environments where a traditional approach to risk management would be limited.

To demonstrate its utility, the Framework was applied to an industrial case study with a collaborative welding process (CSI:COBOT). The process consists of a human putting a part on a shared workspace where it is moved by a UR10 robotic arm to a welder. The part is welded and returned to the shared workspace. This process has several known hazards such as burns from the welding and collision with the robotic arm.

Using the Framework we were able to explicitly define the context of the process, including entities and actions. A standard system safety risk assessment approach (STPA) was used to identify the potential hazards. The safety case was then developed with claims that each of the hazards were addressed – this included ‘behavioural’ hazards such as a collision hazard that only occurred if the human was in a particular area during a particular phase of the process. These rules were implemented and monitored in the Digital Twin.

As well as adhering to the requirements and recommendations in ISO 10218 and ISO 15066, using the Framework, we were able to identify a set of additional ‘safety rules’ that constrained the behaviour of the system during operation to prevent any emergent causes of the known hazards.

The key results of the case study were

- An end-to-end traceable safety risk assessment of the dynamic scenario
- A complete structured safety case with evidence to support each safety claim

- A Digital Twin with the capability to assess rule violations before running the process, and to monitor rules during operation
- An augmented reality visualisation of the safety of the process

Unlike many other approaches that consider just one aspect of risk, the RAS Safety Framework allows us to understand the behavioural hazards that arise during operation to a greater degree, and develop better mitigations thereby improving the overall safety of the system or process.

Another significant advancement of this approach over existing methods is that this end-to-end Safety Framework directly facilitates the development of a clear, structured safety case. It also allows safety claims to be substantiated with traceable verification and validation data from the Digital Twin, therefore improving the efficacy of communicating safety and risk information to regulators, system operators and other stakeholders.