1.2 – Identifying hazardous system behaviour

Practical guidance – healthcare

Author: SAM demonstrator project

One of the main mechanisms for identifying hazards and error prone conditions are the methods used to help identify hazardous system behaviour. Methods shape thinking and dialogues, and influence what can be "seen" in the context before the robotic and autonomous systems (RAS) intervention and what may happen when the RAS intervention is deployed. Methods will influence requisite variety, i.e. the ability to foresee issues that may arise in future systems that do and do not yet exist.

Understanding the coverage, strengths and weaknesses of a method is important for determining its adequacy for identifying hazardous system behaviour. However, it is impossible to run method comparison studies that do not suffer from confounding variables. For example, there is always the "evaluator effect", and even if you keep the same evaluator then they learn over successive applications of different methods to the same area, which means that the study is then confounded. Furthermore, where some methods engage with stakeholders and subject matter experts (SMEs) then their contributions do not necessarily have to be aligned with the method, serendipity may help discover insights. Accepting these limitations, we may still compare the foundational theory, concepts and representations that are tied up in the use of methods, which has consequences for understanding system safety.

Functional Resonance Analysis Method (FRAM)

FRAM [1] focuses on the performance variability of system functions, so what it does rather than its actual parts and composition. It has Safety-II foundations and so should be more aligned with how everyday safety is created the majority of the time, rather than trying to identify low frequency – high consequence events. It views deviations, goal conflicts and inherent trade-offs as necessary and normal. It tries to build a better understanding of work-as-done, not how work can fail.

From this perspective an exemplar FRAM issue would be why a written prescription is rarely complete despite official guidance that says it should be. This issue is not written off as an error or non-compliance issue, but represents an opportunity for learning: to understand how this variability depends on the type drug, the experience of the doctor and the nurse, the context, time pressure, etc. and why this adaptive behaviour happens for good reason.

Systematic Human Error Reduction and Prediction Approach (SHERPA)

SHERPA [2] focuses on a detailed task analysis, human failure analysis and Performance Influencing Factors (PIF) analysis to understand what is driving human failure risks. This is very error orientated. However, consensus groups of SMEs are an explicit part of the method, so the task analysis is grounded in frontline worker experience while being informed by management and safety engineers. So, going beyond error management, this

technique also looks at optimising system design and developing best practice. This method has cognitive science and task analysis as its foundation.

From this perspective an exemplar SHERPA issue would be something like "right action on wrong object" (e.g. a label printed and placed on the wrong syringe). The method would then inspect the PIFs that influence this and seek to design the situation to eliminate these risks or make them less likely. Non-compliance would also be of interest, but more to understand the PIFs from the frontline that influence this rather than bluntly trying to reinforce the rules. Something more out of scope of SHERPA would be technical issues like the autonomous infusion pump fails to communicate with the health IT system because the network is down, or updates to health IT software meaning current request for authority to operate outside of clinical guidelines (extended autonomy) is cancelled.

Safety Modelling, Assurance and Reporting Toolset (SMART)

SMART focuses on identifying hazards and their prevention barriers and mitigation barriers using the bowtie method. This looks at the number and quality of barriers to prevent the hazard and stop the ultimate outcome we are trying to avoid. Barriers can have degradation factors and controls. SMART also uses process diagrams to build up picture of the task as this is not captured in bowtie analyses. The main hazards and barriers can be identified without going into the details of a fine-grained task analysis. This type of analysis should be familiar to safety engineers and can be quite technical.

From this perspective an exemplar SMART issue would be something like the autonomous infusion pump wrongly assumes it has authority to operate outside of clinical guidelines when in fact no authority has been granted. Typically, SMART is less likely to engage with the more intricate issues to do with trade-offs identified in FRAM and the psychological details that SHERPA engages with.

The choice of method will impact the understanding of system safety, which will in turn impact design and safety management.

References

[1] Hollnagel E. FRAM, the functional resonance analysis method: modelling complex socio-technical systems: Ashgate Publishing, Ltd.; 2012.

[2] Embrey D. SHERPA: A systematic human error reduction and prediction approach. Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems. Knoxville, Tennessee: American Nuclear Society; 1986. p. 184-93.