A Human Factors approach for analysing highly automated systems

Ronald W. McLeod[1], Nora Balfe[2]

[1]Ron McLeod Ltd., [2]Visiting Research Fellow, Centre for Innovative Human Systems, Trinity College Dublin

ABSTRACT

Automation rarely if ever removes people from a system: rather, it changes their role in ways that can sometimes be difficult to predict. Learning from innumerable incidents has shown that organisations involved in developing and introducing highly automated systems must give sufficient attention during the design, development and deployment of automation to the role of people in the system. This paper suggests a structured analysis method that could be used early in the development of potentially any automated system to identify where a focused effort on Human Factors issues is likely to be needed.

KEYWORDS

Automation, Human Factors Analysis, Systems Development

Introduction

This paper outlines an approach to thinking about and describing 'highly automated systems' in a way that highlights and emphasizes the relative roles and responsibilities between the technological and human elements of the system. The objective is to provide a basis for identifying the areas and features of an automated system likely to demand attention to Human Factors issues during its' design, development and implementation[1].

The suggested analysis described here is based on a consideration of a large body of literature and experience, including peer-reviewed scientific papers (most prominently the work of Flemisch et al (2012), Parasuraman et al (2000), and Onnasch et al (2014)), industry-specific guidance (such as SAE J3016, CAP1377, SINTEF, 2015), as well as material produced by government. Space here precludes a detailed explanation of the rationale or relationships between these sources and the proposed method. However, the objective of the approach is to encourage a structured and rigorous consideration of the proposed use of automation in a way that:

- Places the role of the proposed automation in its wider system context;
- Focuses attention on the various operational tasks that need to be performed to deliver system goals;
- Considers performance of the system in terms of which functions automation will support in performing operational tasks (Parasuraman et al., 2000);
- Makes it clear where Responsibility for the performance of each function is expected to lie;
- Focuses attention on whether automation or human elements of the automation system have on the Ability and the Authority to perform any of the functions, as well as where Control is

[1] The work described in this paper is a by-product of work carried out by a CIEHF working group to develop a White Paper on 'Human Factors in Automation'.

expected to lie. (Flemisch et al. (2014), developed a means, known as an "A2CR" diagram, of visually representing automated systems in a way that can explicitly represents differences in Responsibility, Ability, Accountability and Control).

The approach is presented in the form of a method that could be used to conduct a detailed analysis of the relative abilities of the human and technological elements of a proposed automated systems early in its development. It is intended to provide the basis for identifying and address the Human Factors challenges that may need to be overcome. Note that the approach is not intended to perform the kind of detailed analysis or design of the interactions between the human and automated elements of the system that methods such as CoActive Design (see Baber and Vance, 2019) are intended to support. Rather, the intent is simply to raise awareness and draw attention early in the system development process to areas that will demand appropriate Human Factors effort.

Specifying the Context and Conditions of Use

The analysis is intended to be used in the development of systems to be operated in an environment that can be specified to a very high level. Following SAE J3016, this will be referred to as the Operational Design Domain (ODD) [2]. It is important to be clear about the extent to which the intended purpose of any system can be fully specified and controlled in the design of the automated system.

1. Specification of the ODD should include definition of detectable indicators of its limits: i.e., the points when the actual operational conditions become outside the limits of the intended context and conditions of use[3].
2. Specification of limits defining breach of the context and conditions of use provide the basis for what SAE J3016 calls "Object and event detection, recognition, classification and response (OEDR)". If limits defining breaches of the ODD cannot be fully prescribed during design of the automated system, or are not capable of being detected and recognized as breaches by the technology, OEDR is likely to be a critical human function relying on real-time judgement. It can be complex, demanding sophisticated human performance from skilled and situationally aware people.

Specification of the intended purpose will need to include details of the expected state of the automated system itself, i.e. is it able to continue to perform under any failure or degraded states of its sensors or actuators? Critically, what does it assume about the state and characteristics of people required – within the scope of the intended purpose - to assist or support it?

Constraints associated with the intended purpose should also be clear; for example, legal/ regulatory constraints or available resources as well as assumptions about the number, characteristics and abilities of people expected to be available to support the system.

Analysis Method

With reference to Figure 1, there are four necessary steps involved in preparing a description of an automated system in a way that allows proper consideration of the role of the human in achieving the overall system goals.

---

[2] The term 'Operational Design Domain' is taken from SAE J3016 for Automated Vehicles. It is similar to the concept of the 'Intended Purposes' as defined in the recent draft "Regulation on a European Approach for Artificial Intelligence".

[3] For example, in the crash of Air France flight 447 into the Atlantic in 2007, the flight computers lost real-time airspeed data when the aircraft's pitot tubes froze. Loss of airspeed data breached the context of use, and control was handed to the pilot instantaneously.

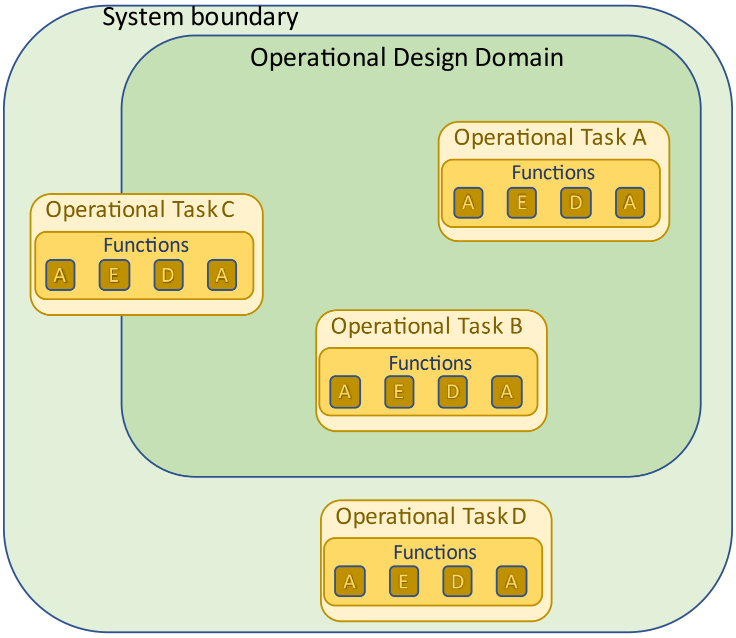

Figure 1: Abstract model of a highly automated System.

Step 1: Locate the automation within the overall socio-technical system it supports. This involves defining four features;

1. The ultimate purpose the automated system supports in terms of its System Boundary. The purpose will always be set by people, and will be broader than the scope of the automated system.
2. The 'Operational Design Domain' for which the automated system is intended by the provider, defining the specific context and conditions of use. Features used to define the ODD will be dependent on the nature of the activity. For example;
   - In an automated rail signalling system parameters might include the control room environment in which it is located, the characteristics of the lines to be controlled and the numbers of trains expected to travel over the area or vehicle-based systems, as well as the physical environment, characteristics of the route and lighting conditions;
   - for a medical system, it might be defined in terms of a patient's condition (e.g. vital signs) and physical location (e.g. in an intensive care setting, or hospital ward);
   - for a drilling system, parameters might include details of the pressure profile of the well, and the characteristics of shut-down and other equipment available at the wellsite;
3. The specific goal the automated system is expected to perform or support. The goal needs to be defined as tightly and specifically as possible, including both what is to be ***achieved***, what is to be ***avoided***, (e.g. injury, spillages, damage, noise, etc.) as well as ***constraints*** around how the objective is to be achieved (e.g. time, power, resources, etc.).
4. The elements and actors (human, technology and others) that collectively define and constrain the scope of the system and the ODD.

Step 2: Identify and analyse the Operational Task(s) that need to be performed to achieve the system goal. Operational task(s) can be defined as "*All of the real-time tasks required to deliver the system goal". Operational tasks need to include tasks that could need to be performed in case of emergency and abnormal situations as well as 'normal' operation within the ODD. Figure 1 illustrates two tasks necessary to achieve the system goal (tasks A and B) that fall fully within the ODD, one task (task C) that crosses the ODD boundary, and one task (task D) that is completely outside the boundary of the ODD. Each task should be analysed to assess its Criticality, expected Level of Automation, and where Responsibility for performance of the task is expected to lie:

- Criticality:
  - Very high: Failing to perform the task to the required standard would be immediately unacceptable under any conditions.
  - High: Failing to perform the task to the required standard could be immediately unacceptable under some conditions.
  - Moderate: Failing to perform the task to the required standard would be inconvenient, though not unacceptable.
  - Low: Failing to perform the task to the required standard would be of minor consequence. EITHER The system would provide sufficient warning and information to allow people or other systems to intervene and take over control without serious adverse consequence, OR; The system can be relied on to fail/ degrade gracefully without negative consequence and with adequate warning.
- Level of Automation: Five levels are suggested (based on the Civil Aviation Authority's CAP 1377);
  1. None: Entirely human, no automated support.
  2. Low level automation
  3. Medium level automation
  4. High level automation
  5. Fully Automated. No human support.
- Responsibility: Responsibility refers to the party that would be held to account if a failure occurred with serious consequences. Responsibility could lie with the consumers or those at the front-line of an operation in closest contact with the system. It could lie with those away from the front-line who manage, authorize, and ultimately control the operation. Or it could lie with suppliers, or others, who develop the automation and declare it as fit-for-purpose.

Step 3: For each Operational Task determine what is needed to satisfy four generic functions (based on Parasuraman, Sheridan, & Wickens, 2000);

1. Acquiring information: Attending to sources of information relevant to achieving system goals, "perceiving" it, and converting the information into a form that is available for use within the system;
2. Extracting meaning: Extracting meaning from the information in a way that is directly relevant to performance of operational tasks in the short or long-term.
3. Making Decisions: Based on the extracted meaning, making decisions about modifying or changing how the Operational Task is performed to continue to satisfy system goals.
4. Taking Action: Effecting change either on the system or – via the system or other agents - on the physical world.

Step 4: For each of the four functions for each operational task, estimate;

- **Ability** (Technology and Human): To what extent do the technology (unaided by a human) and the human (unaided by the technology) elements possess the means and ability (e.g. skill, sensors, etc) to perform the function to the required standard?

  - None: The element is not capable of performing the function successfully under any circumstances.
  - Low: The element can be relied on to perform the function under some limited circumstances;

  - Moderate: The element can be relied on to perform the function under most circumstances defined in the ODD;
  - High: The element can be relied on to perform the function under most – though not all – circumstances within the ODD;
  - Complete: The element is capable of performing the function under all circumstances defined in the ODD.

- To what extent will the technology have the **Authority** to control how each task is performed. Note: Authority is allocated by those who are in ultimate control of the overall system (e.g. company management);

  - Never: The technology will never be given the authority to perform the function;
  - When delegated: The operator assigns or removes authority to the technology on a real-time basis;
  - By default: Unless otherwise constrained, the technology will have the authority to perform the function most of the time within the ODD, unless it is actively removed by the operator;
  - Always: The technology will have the authority to perform the function all of the time as long as the system is within the ODD. The operator cannot remove the authority.

- The proportion of the time the human might be expected to have **Control** over how each function is performed.

Note that inconsistencies between Ability, Authority and Control can be illuminating. For example, assuming the technology would have Control 90% of the time, if it only has Authority “When Delegated” could suggested a weakness somewhere in the system that would flag a need for investigation.

Table 1 contains a worked example of how the analysis described above might look if it was performed on an Automated Lane Keeping system in a vehicle driven on public roads. (The analysis shown in Table 1 is entirely hypothetical and was developed purely for the purpose of illustrating the suggested analysis. It has had no input from anyone professionally involved in the automotive industry).

Table 1: Hypothetical example of suggested Human Factors Automation analysis applied to Automated Lane Keeping

SYSTEM	Automated lane keeping						
Purpose	Transport people safely and efficiently to a pre-defined location over the national highway network within the law.						
System Goal	Keep vehicle within prescribed lanes while travelling at speed. Avoid collisions and passenger physical or emotional discomfort. Remain within speed limits while being energy and time efficient.						
System Elements	Vehicle; Driver; Highway infrastructure; Other vehicles; Other objects on road; Environment.						
Operational Tasks	Control vehicle linear and rotational acceleration	Maintain vehicle position within lane	Maintain safe separation from vehicles in front and	Avoid collisions with other objects	Detect approaching ODD limits.	Monitor driver's ability to perform manual functions.	Monitor state and performance of the system
Task Criticality	Very high	Very high	Very high	Very high	High	High	High
Level of Automation	4	4	4	4	3	2	3
Responsibility	Driver	Driver	Driver	Driver	Manufacturer	Driver	Manufacturer
Acquire Information	Current speed limit. Desired speed;	Current position; Current speed and heading; Lane limits X msecs ahead.	Time/distance of vehicles ahead and behind; Rate of closure.	Presence of objects with potential to enter vehicle path; Rate of closure.	Lane limit markings; Light levels, etc.	Indicators of driver state (wakefulness, distraction, etc)	System state and performance indicators
Ability (Technology / Human)	*Complete / High*	*Complete / High*	*Complete / High*	*Complete / High*	*Moderate / Moderate*	*Low / Moderate*	*Low / Moderate*
Technology has Authority	*By default*	*By Default*	*By Default*	*By Default*	*When delegated*	*Never*	*When delegated*
Expected Human Control	*Up to 25%*	*Up to 25%*	*Up to 25%*	*Up to 25%*	*Up to 25%*	*100% (**)*	*75% (**)*
Extract Meaning	Δ between current and desired speed?	Projected position of vehicle x msecs ahead relative to lane limits.	Zill time-to-collision with vehicles be in target range	Predicted likelihood of collision with object.	Is the situation likely to breach ODD limits within X secs?	Current driver state (alertness etc.).	Are there indicators the system is not functioning
Ability (Technology / Human)	*Complete / High*	*Complete / High*	*Complete / High*	*Complete / High*	*Complete / High*	*Low / Moderate*	*Moderate / Moderate*

Table 1: Continued

Technology has Authority	*By default*	*By default*	*By default*	*By default*	*By default*	*Never*	*When delegated*
Expected Human Control	*100&*	*Up to 25%*	*Up to 25%*	*Up to 25%*	*0%*	*>75%*	*50-75%*
Make Decisions	Need to increase or reduce speed?	Need to vary linear or rotational acceleration to stay within lane limits?	Need to change linear acceleration to maintain safe separation?	Need to change linear acceleration to avoid collision? Need to initiate an emergency	Need to revert to manual control?	Is the driver in a fit state to take control within X secs if needed?	Need to take manual control?
Ability (Technology / Human)	*Complete / High*	*Complete / High*	*Complete / High*	*Complete / High*	*High/ Low*	*Low / Moderate*	*Moderate / Moderate*
Technology has Authority	*By default*	*By Default*	*By Default*	*By Default*	*When delegated*	*Never*	*When delegated*
Expected Human Control	*Up to 25%*	*Up to 25%*	*Up to 25%*	*Up to 25%*	*0%*	*100% (**)*	*75% (**)*
Act	Vary linear and/or rotational	Vary linear and/or rotational	Vary linear and/or rotational	Vary linear and/or rotational	Prepare driver to take manual	Initiate awareness improving	Take manual control (i.e. NOT
Ability (Technology /	*Complete / High*	*Complete / High*	*Complete / High*	*Complete / High*	*Moderate / High*	*Moderate / High*	*Never / Usually*
Technology has Authority	*By default*	*By default*	*By default*	*By default*	*When delegated*	*When delegated*	*Never*
Expected Human Control	*Up to 25%*	*Up to 25%*	*Up to 25%*	*Up to 25%*	*>75%*	*>75%*	*100%*

Conclusion

Automation rarely if ever removes people from a system; rather, it changes their role in ways that can sometimes be difficult to predict. Learning from innumerable incidents has shown that organisations involved in developing and introducing highly-automated systems must give sufficient attention during the design, development and deployment of the system to the role of people. How much, and what kind of attention depends on issues such as the potential criticality of the system, its context of use and the extent of change the system will introduce.

The analysis method proposed in this paper is one approach to carrying out a detailed and rigorous Human Factors focused assessment early in the development of any automated system. Application of the method is intended to draw attention to areas and aspects of the system, including its proposed usage, that demand attention to Human Factors issues.

As with many forms of Human Factors analysis, value is likely to be derived simply from the process of trying to answer the questions necessary to complete the analysis. The detailed content itself will rely on estimates and best judgement, sometimes with significant uncertainty and making many assumptions. Nevertheless, performed competently, the process of examining a proposed system in a rigorous and structured way, using dimensions customised to understanding the balance between the human and technological components of the system, is likely to lead to significant understanding and insight and to provide the basis for planning a program of targeted Human Factors intervention.

References:

Baber, C., & Vance, C. (2019) Design of human-machine teams using a modified CoActive design Method. Contemporary Ergonomics. Eds Charles, R and Golightly, D. CIEHF.

Civil Aviation Authority (2016) ATM Automation: Guidance on human-technology integration. CAP 1377. Safety and Airspace Regulation Group.

Flemisch, F., Heesen, M., Hesse, T., Kelsch, J., Schieben, A.& Beller, J. (2012) Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative situations. Cogn. Tech. Work. 14:3-18.

Norman, D.A., (1990) The ‘Problem’ with Automation: Inappropriate Feedback ad Interaction, not ‘Over-Automation’. Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences. 327 (1241) Human Factors in Hazardous Situations, pp. 583-593.

Onnasch, L., Wickens, C.D., Huiyang, L. & Manzey, D. (2014) ‘Human Performance Consequences of Stages and Levels of Automation: An integrated meta-analysis”. Human Factors, 56(3) May, pp 476-488

Parasuraman, R. & Riley, V. ‘Humans and Automation: Use, Misuse, Disuse and Abuse. Human Factors 1997, 39(2), 230-253

Parasuraman, R., Sheridan, T.B., Wickens, C.D. (2000) ‘A Model for Types and Levels of Human Interaction with Automation’

Society of Petroleum Engineers, DSATS Roadmap

SAE International (2018) Surface vehicle Recommended Practice. Taxonomy and definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. J3016

Wickens, C.D., Huiyang, L., Santamaria, A., Sebok, A, & Sarter, N.B. (2010) Stages and Levels of Automation: An Integrated meta-analysis”. Proc. HFE Soc, 54th Annual Meeting. 389-39