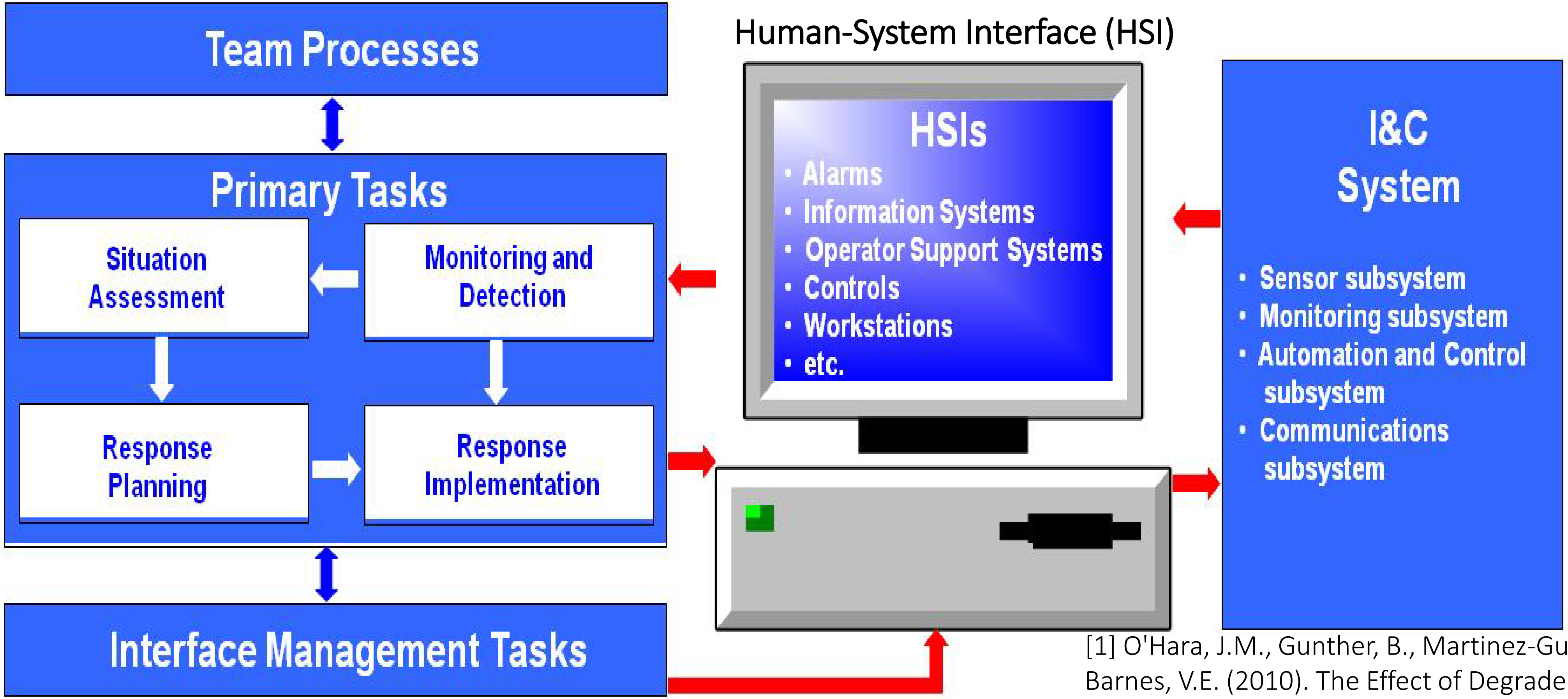
OECD NEA Halden Human-Technology-Organization (HTO) Project

Digital I&C Safety Assurance and Human Performance

Andreas Bye, Bjørn Axel Gran,
Sizarta Sarshar, Yonas Zewdu Ayele

Digital Instrument &Control (DI&C) - Human Performance Framework



[1] O'Hara, J.M., Gunther, B., Martinez-Guridi, G., Xing, J.F., & Barnes, V.E. (2010). The Effect of Degraded Digital Instrumentation and Control systems on Human-system Interfaces and Operator Performance.

Operator performance in digital vs traditional control room

Research question:

Analog HSI may be used as backup for digital HSI in safety systems, e.g., for plant shutdown. What are the effects on the operators when changing between different types of interfaces?

Experimental results:

- Radical HSI transitions did not degrade human performance.
  - Less workload and the overall task performance was improved when a digital HSI was substituted with a panel-based HSI during the scenario.
  - No observed effects for response time, situation awareness or self-rated performance. No serious impact of the radical HSI transition on expert-rated human performance.
  - Two crews considered radical HSI transitions as quite unproblematic – given a sufficient amount of training. The third crew recognized many benefits of both HSI solutions, but they were generally sceptical to radical HSI transitions (possible acceptance challenges).

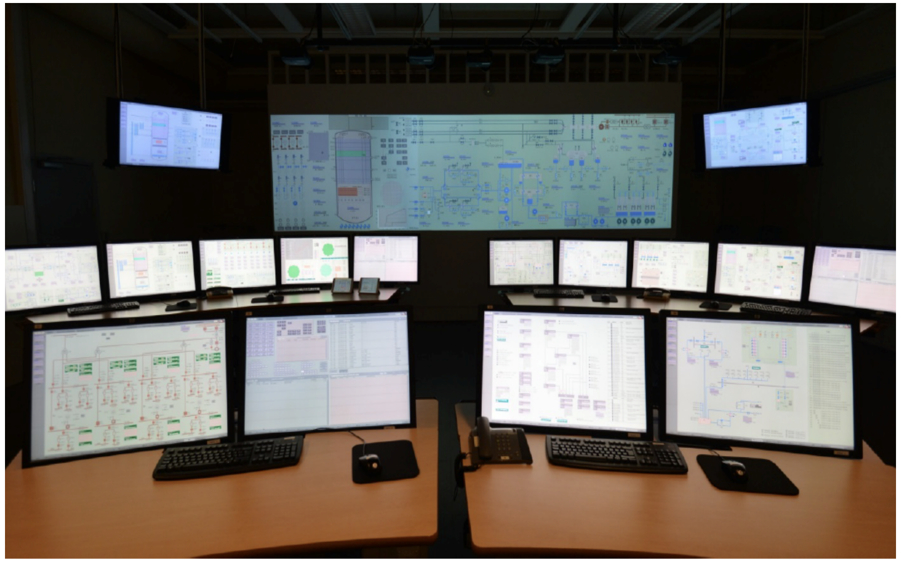


Figure 7. HAMMLAB set-up for the digital HSI.

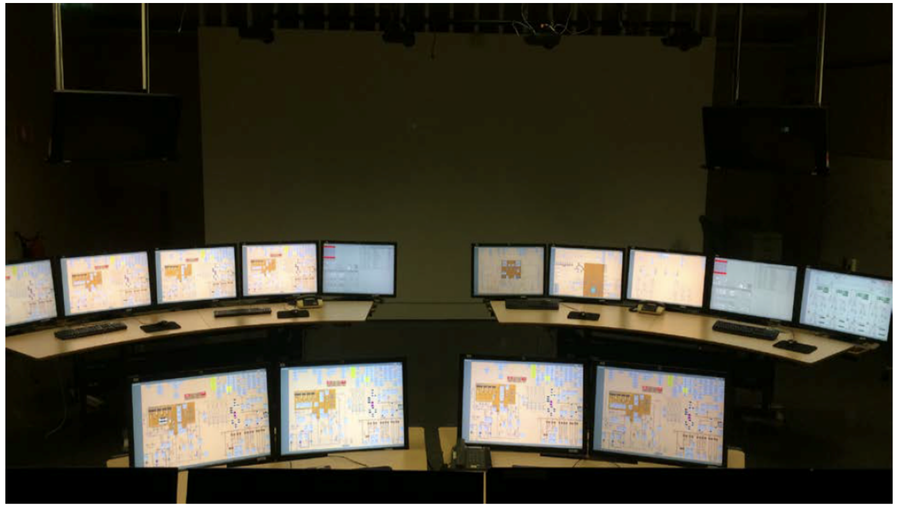
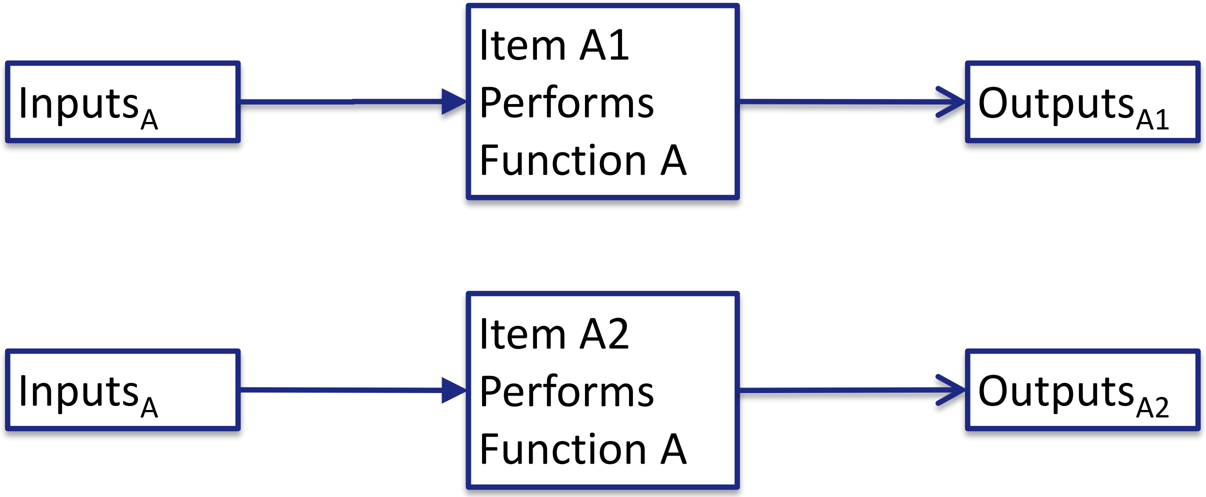


Figure 8. HAMMLAB set-up for the panel-based HSI.

Diversity in Design



Inputs_A

Item A1 Performs Function A

Outputs_{A1}

Inputs_A

Item A2 Performs Function A

Outputs_{A2}

A1, A2 are diverse, if **The same common cause does not degrade the performance of A1, A2**, e.g.:

- Latent design defects.
- Unwanted interactions.
- Shared resources.

Assume items A1, A2 are implemented on FPGA

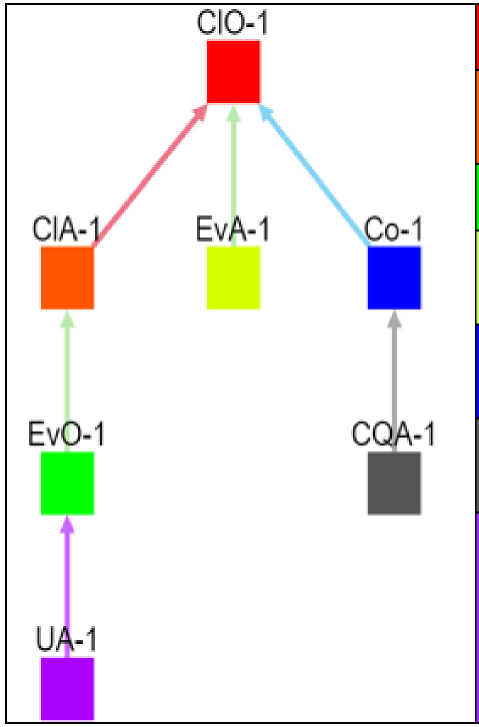
Question: Is it technical feasible to achieve a level of assurance at least comparable to current practice without requiring diverse designs?

Challenge: How can we prove “nothing will go wrong”? If we don’t know what can go wrong, how can we prevent it?

Problem: how to specify the requirements and constraints in natural language.

Structured Safety Argumentation Approach (SSAA)

We developed a prototype tool for structured argument. In this tool, the notation can be self-defined. The nodes can be specified to different users.



ClO-1	Claim by Owner (of the system and argument) – *extracted text*
ClA-1	Claim by Assessor (e.g. when an implicit claim is made explicit, or when a logical link is missing) – *added text*
EvO-1	Evidence by Owner – *extracted text*
EvA-1	Evidence suggested by Assessor (i.e. what kind of evidence the assessor would expect) – *added text*
Co-1	Context (references to further information, definitions, explanations, etc.) – *usually extracted text*
CQA-1	Comment or Question by Assessor (so the assessor can make notes for himself/herself) – *added text*
UA-1	Uncertainty by Assessor (specifically expressing potential problems of the argument) – *added text*

- Self-defined notation (nodes and reasoning logic)
- Specified nodes for different users

Key messages

- Digital I&C and human performance are closely linked
- Digital systems have the potential improving human performance
- Failures in digital systems may be difficult to handle for humans
  - Especially failures in automation systems
- Safety assurance of digital systems is necessary; and evaluation of the roles of new digital systems should be performed together with the evaluation of human performance.