Presented by:

Dr Chris Harper

Senior Research Fellow

Robotics & Autonomous Systems Safety Engineering

Bristol Robotics Laboratory (BRL)

Perspectives on Functional Safety Assurance of Construction Robots and their Human-Robot Interaction (HRI)

11th November 2022

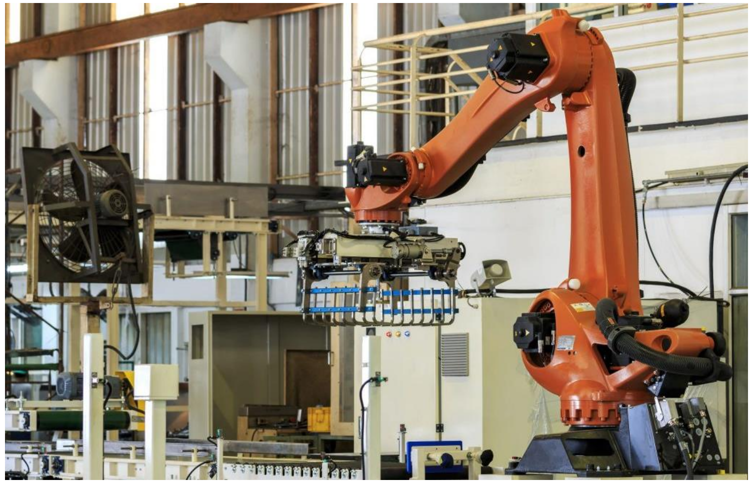
UWE, Bristol

Robotics & Autonomous Systems (RAS) in Construction

- Masonry
- Heavy lifting
- Remote inspection (drones)

https://www.edgeprop.my/content/1316054/i-robot-builds-your-home

- 3D Printing
- Demolition
- Bricklaying



https://safetyteksoftware.com/article/construction-robotics-creating-safer-worksites/

https://www.inceptivemind.com/spot-robot-ready-site-inspection-large-construction-site/10359/

- Concrete recycling
- Earth-moving
- Façade cleaning & painting

https://engagek12.robotlab.com/lesson/STEM/Lesson-5:-Construction-Robots/Robotic-Arm/a1tD000000885eCIAQ

Problem!

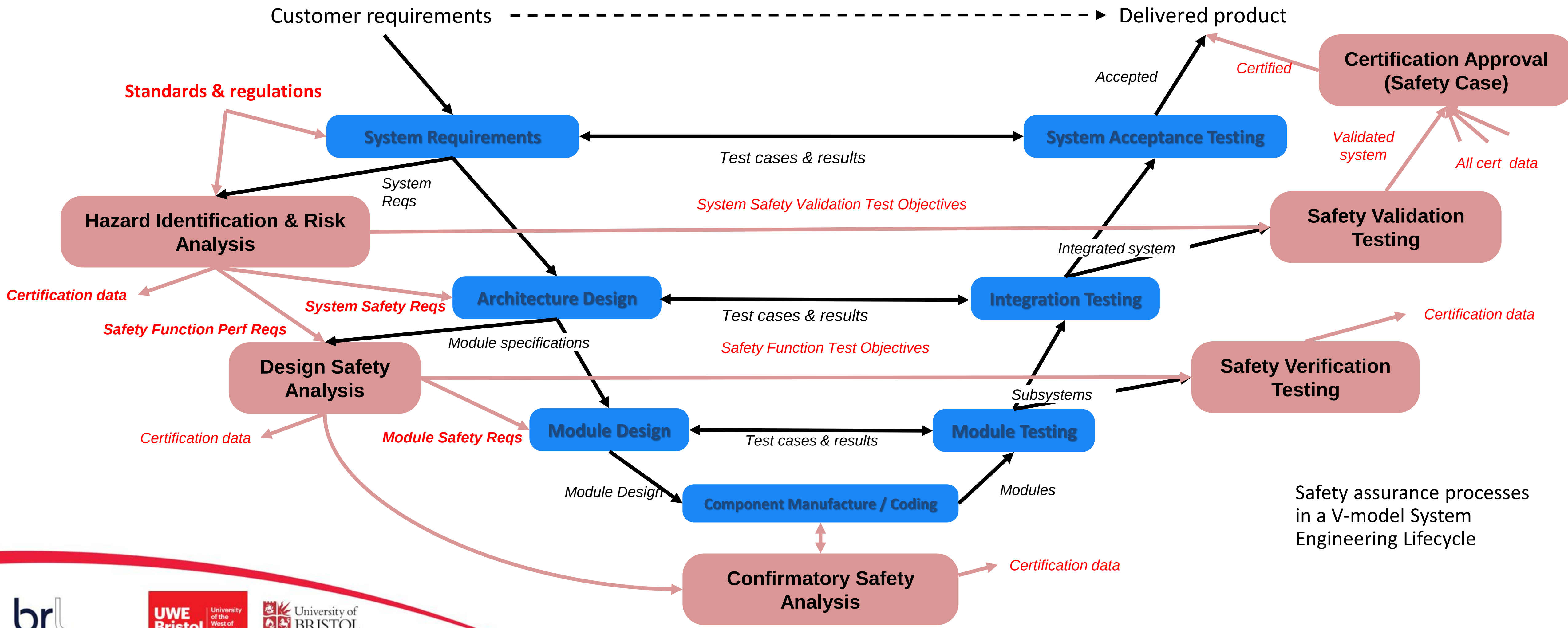
No specific safety standards for robotics in construction (either from ISO/TC 195 Construction machinery or ISO/TC 299 Robotics)

So, what guidance from elsewhere…?

- **Robot Design**
  - ISO 10218-1: Safety requirements for industrial robots – Robots
  - ISO 10218-2: Safety requirements for industrial robots – Robot systems and integration
  - ISO TS 15066 Collaborative robots (see later)
  - ISO 13482: Safety requirements for mobile service robots ('scaled up' to construction applications…)
  - Also: UL 3100, Outline of Investigation for Automated Mobile Platforms (AMPs)
UL 4600: Standard for Safety for the Evaluation of Autonomous Products
UK Safety Critical Systems Club: SCSC-153A/B Safety Assurance Objectives for Autonomous Systems
IEEE 7001 Transparency of AI Systems
- **Robot deployment – suggest to use existing workplace safety guidance & standards, but with methods updated for RAS**
  - Revised methods tailored to robotics (e.g. Environmental Survey Hazard Analysis, see following slides)
  - Validation of robot operational safety against standards by simulation of construction sites using digital twins

System safety engineering perspectives

- ***System safety engineering*** is the name given to the methods and processes aimed at achieving safety assurance
- Safety engineering processes are often defined as an extension to system development lifecycles:



Safety assurance processes in a V-model System Engineering Lifecycle

Functional safety assurance of RAS – the challenges

• The Curse of Dimensionality

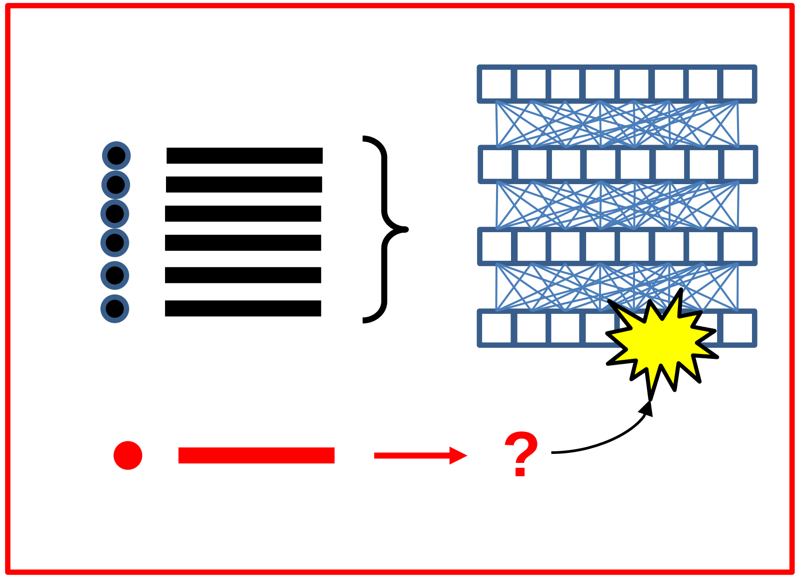
Photo: Ken from Concord CC BY-SA 2.0

vs.

Non-autonomy: Local dynamics **Autonomy: Situated dynamics**

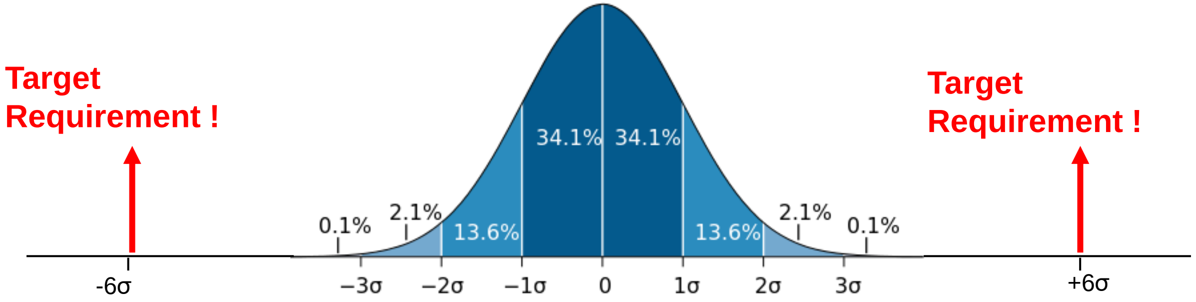
- Situated behaviour highly dimensional
- Full test coverage of state space not feasible

• The Problem of Induction



- ML is an *inductive process* (generalization)
- Inductive inference is unsound
- Missing data or counterexamples can invalidate the models generated by ML algorithms

• The Rare Event Problem



- Typical probability requirements for acceptable safety are <u>extremely demanding</u> (90% success rate is *hopelessly inadequate!*)
- Amount of testing required is not feasible; designers must have prior belief that design is correct without need for testing

System safety engineering perspectives

- Safety engineering is as much about designing the environment as the system itself

1980s

Docklands Light Railway – driverless operation from conventional (non-ML/AI) computer technology

Photo: Julian Herzog CC BY 4.0

Airbus A320-211 – Digital Fly-By-Wire control and modern flight management systems (non-ML/AI) – essentially pilotless while wheels are off ground

2010s

Autonomous Pod – driverless operation, but more advanced technologies required (e.g. ML/AI)

Artificially prepared/constrained environment

- Interactions are eliminated by design; "intelligent" behaviour not required
- Hence, simpler technology will suffice
- Systematic safety analysis is (just about) feasible

Environment much less constrained

- Many more features to interact with; many interactions are not eliminated by design; more complex behaviour required from the system to maintain safety (avoid accidents)
- More advanced system technology required, to achieve intelligent behaviour (i.e. ML/AI)
- Very much harder to show that safety analysis is complete

System safety engineering perspectives (2)

- Bounded vs. unbounded domains:

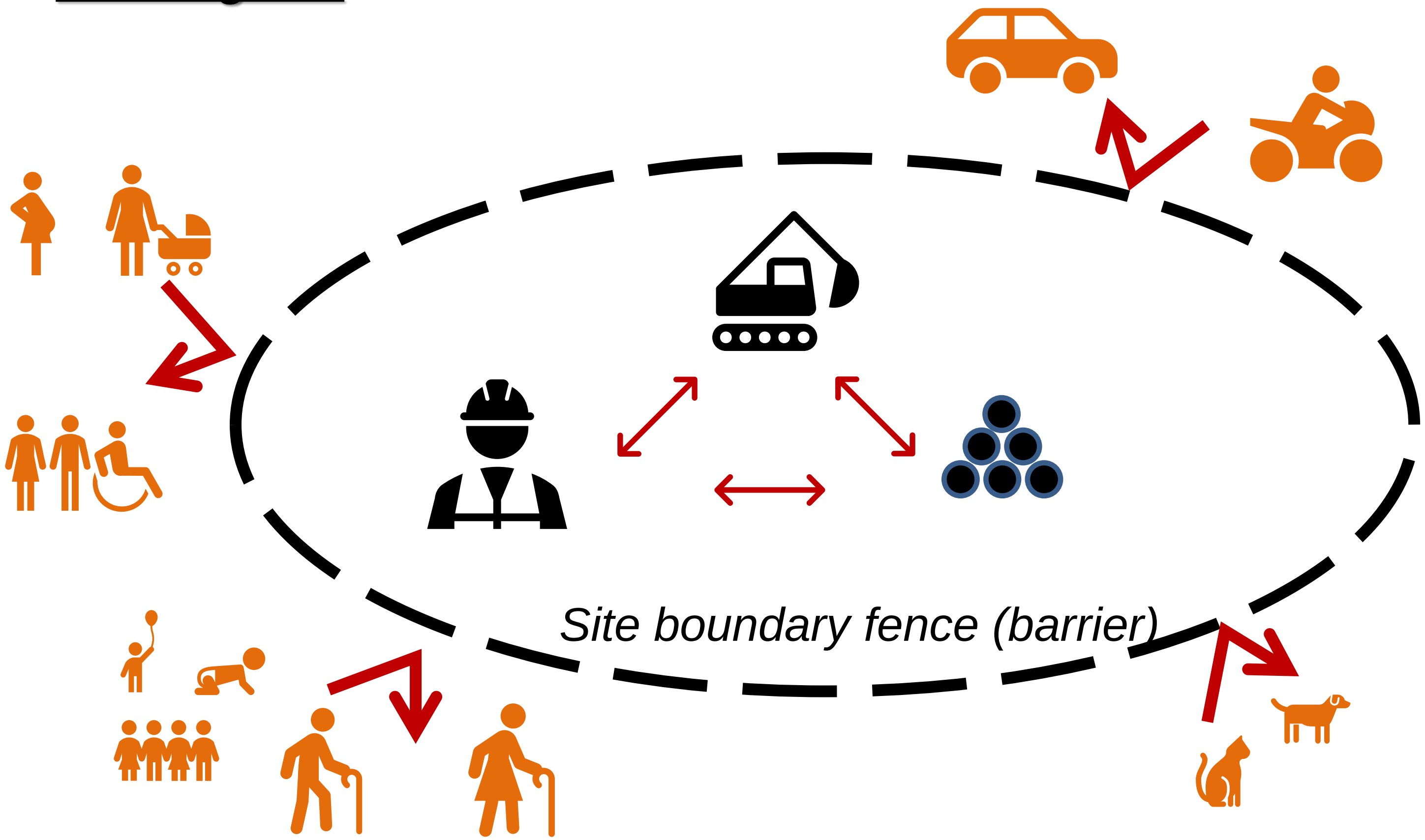
Manufacturing Robots in closed domain (workcells)

"Tesla Robot Dance" by jurvetson is licensed under CC BY 2.0

Collaborative manufacturing robot in open domain

"Rethink Robotics — Brooks and Baxter" by jurvetson is licensed under CC BY 2.0

Building Site



- Boundaries reduce the number of interactions required of a system

Hazard and Risk Assessment for RAS
Environmental Survey Hazard Analysis

- New (2014) method of functional hazard & risk assessment aimed at RAS problems

- Basic philosophy:
  - Traditional methods (e.g. HAZOP, FHA) aimed at identifying the hazards of *mission-related* system failures
  - BUT: autonomous systems must interact with the environment in ways ***not necessarily related to its mission***
  - SO: risk assessment must consider how RAS interact with everything in an environment, i.e. survey the environment and consider the risks of anything that is found there
  - Traditional methods do not assist well with this approach *(not impossible, just unhelpful)*

Environmental Survey Hazard Analysis

- Some references: [Harper et al 2014] , [Harper 2020], [Harper, Caleb-Solly 2021]

Example: a robot waiter on a café terrace

ESHA Procedure (approx.)

1. Survey the environment, looking for ***all*** possible features (intended ***and unintended***) that might require an interaction
2. For each feature identify the interactions necessary ***either*** for general survival ***or*** performance of intended mission.
3. Identify harmful events associated with the features, the safety interactions necessary to avoid them, and the system design features necessary to perform the safety functions.

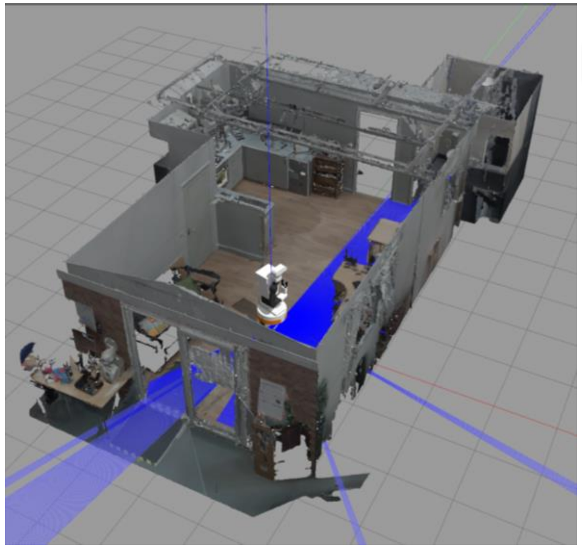
ESHA Guide-words (original version) (Dogramadzi & Harper et al, 2014)

- The environment itself (the background) [terrain areas/regions]
  - ➢ Surfaces, features
  - ➢ Ambient Conditions (e.g. light levels, temperature, pressure, acoustic noise, atmosphere quality, EMI/RFI)

- Objects situated within the environment
  - Motion:
    - ➢ Things that don't move (Obstacles)
    - ➢ Things that move without purposeful behaviour (Simple Moving Objects)
    - ➢ Things that move purposefully (Agents)
      - ❑ Biological (Living) Agents
        - ▪ Sentient Agents (Human, generally speaking)
        - ▪ Non-sentient Agents (Animals, generally speaking)
      - ❑ Non-biological Agents
        - ▪ Unintelligent Systems (which perform only mission tasks)
        - ▪ Intelligent Systems (which perform both mission and non-mission tasks)
  - Shape:
    - ➢ Objects detected by sensors as a single point (0-D)
    - ➢ Objects detected by sensors as a linear shape (1-D)
    - ➢ Objects detected by sensors as a surface-like shape (2-D)
    - ➢ Objects detected by sensors as having volume (3-D)

Safety validation of robot applications by simulation using digital twins

- Current line of research at BRL; originally for driverless vehicles; now adapting it for robots
- Example below: healthcare assistive robots
  - Exposing target users to untested healthcare robots (esp. during ML phases) is ethically questionable
  - So, test in simulation first, to get preliminary evidence / confidence in safety, before real world testing takes place



Simulated environments (digital twins)

Physical test environment (e.g. Lab house)

Real world

Assertion-checking simulators – a toolset for safety validation

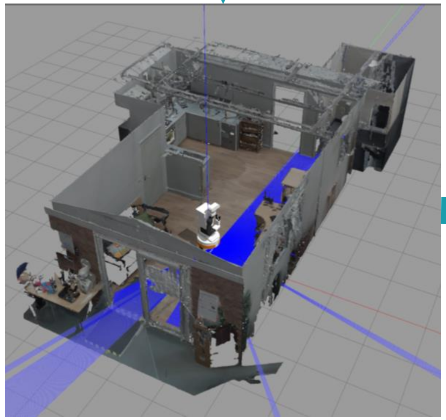
- **Simulation-based testing** with **situation coverage** [1] is an essential tool for safety validation of autonomous systems, as high state space coverage from physical testing is not practicable.
- **Assertion checking** is an effective method of evaluating the situated behaviour of RAS, both in simulation and runtime [2].

TEST CASE GENERATOR

Achieve high levels of **scenario coverage**

ASSERTIONS CATALOGUE

Library of SQL query scripts checking the data stream against **rules derived from safety standards**



Simulation (e.g. Gazebo)

Data stream capture (DBMS)

QUERY

Assertion checking engine (DBMS query tool)

GUI / Analytics

1. Alexander R Hawkins H & Rae D (2015), *Situation coverage - a coverage criterion for testing autonomous robots*, Univ. of York Technical Report YCS_2015_496
2. Harper C, Chance G, Ghobrial A et al. (2022), *Safety Validation of Autonomous Vehicles using Assertion Checking*, https://doi.org/10.48550/arXiv.2111.04611 (submitted to IEEE Trans. ITS)

Industrial robotics safety standards: ISO 10218-1/2

- ISO 10218-1: Safety requirements for robots:
  - Requirements for hazard/risk assessment of design
  - Basic safety philosophy: if problem occurs, stop! (still valid for construction apps?)
  - Operational modes:
    - *Automatic, Manual reduced speed (< 250 mm/s), Manual high speed (> 250 mm/s)*
    - *Automatically stop if safety condition detected or if changing between modes*
    - *Requirements for HMIs (pendants, remote controls)*
    - *Speed and separation monitoring, singularity protection*
  - Establishment of safety spaces/zones based on reachable space around robot: axis-limiting
  - Guidance on information for use, warning signs, etc.

- ISO 10218-2: Safety requirements for robot systems and integration:
  - Installation design, commissioning
  - Collaborative operation (see also TS 15066)

- *Suggestion/recommendation for current practice in Construction*: review these standards as guidance and adapt them to construction projects on a case-by-case basis

Safety requirements for collaborative robots in construction

- Collaborative operation guidelines originally in TS 15066 but also now in ISO 10218 -1/2 (2011 and later)
- Collaborative Operational modes:
  - **Safety-rated monitored stop**: robot stops when person enters robot's workspace/reachable space
  - **Speed and separation monitoring**: robot speed is a function of separation distance to personc, approaches zero (stopped) as person reaches the robot
  - **Power and force limiting**: robot power/force is limited if person comes into (intended or unintended) contact; must design for transient contact and quasi-static contact scenarios (from risk assessment); TS 15066 contains quantitative data on allowable contact forces
  - **Hand guiding**: user manipulates robot to teach it a particular action sequence (task) which it then repeats automatically on subsequent runs; safety rated monitored speed and stop functions are required, and power/force limiting is recommended

- Construction robotics may require other collaborative modes – discussion?

Conclusions

- Currently no specific standards for safety requirements in construction robotics

    - ***Is it time for such a standard to be created?***

- My recommendation:
    - Standards exist for industrial robotics and mobile service robotics
    - Some guidance exists for design of ML/AI technology in safety-related applications

    - Use guidance from other sectors and construct a project-specific safety case for use of robotics
        - Do an Environmental Survey Hazard Analysis (or equivalent), not older methods
        - Validate robotic equipment safety in simulation during initial phases of project