Safety Case Considerations for the Use of Robots in Nuclear Decommissioning

Howard Chapman, John-Patrick Richardson, Colin Fairbairn, Darren Potter, Stephen Shackleford and Jon Nolan

Decommissioning activities in the nuclear industry can often require personnel to undertake tasks manipulating plant, equipment and deploying tools in close proximity to contaminated materials.

The predominant risk associated with such work is exposure to radiological dose uptake from direct radiation, internal dose due to inhalation, or from wounds. There is an aspiration within the nuclear industry to remove the need for operators to undertake manual decommissioning activities by using ‘robotic systems’ which offer the benefit of overall risk reduction safer, sooner and cheaper.

A vital part of the UK Nuclear Decommissioning Authority (NDA) mission is to help drive innovation to address the wide-ranging complex challenges across their sites and businesses. The NDA’s ‘Grand Challenges’ for technical innovation aims to remotely decommission gloveboxes by 2025 and provide a 50% reduction in decommissioning activities carried out by humans in hazardous environments by 2030 [1].

It is known that:

“nuclear sites with their background in radiological substances and hazards have created the need for extensive safety measures involving the requirement for high integrity instrumentation and control measures for protection to stringent nuclear standards” [2].

This paper examines the underpinning Regulations, Standards and Technical Assessment Guides necessary for the deployment of ‘robotic systems’ to remove the need for operators to undertake manual nuclear decommissioning activities. It also investigates the information currently available to produce a safety case, together with commentary on work being undertaken by the UK National Nuclear Laboratory (NNL) who are currently reviewing technology and proof of concept trials to help future development in this area.

Introduction

The civil nuclear industry worldwide is regulated to ensure that activities related to nuclear energy and ionising radiation are conducted in a manner which adequately protects people, property and the environment.

In the UK, the Office for Nuclear Regulation (ONR) is the agency responsible for the licensing and regulation of nuclear installations, and the legal framework for the nuclear industry is based around the Health and Safety at Work Act (HSWA) [3], the Energy Act [4] and the Nuclear Installations Act (NIA) [5].

A fundamental requirement cited in the legislation is that risks be reduced to As Low As Reasonably Practicable (ALARP). This principle provides a requirement to implement proportionate measures to reduce risk where doing so is reasonable. The ALARP principle is applied by adhering to established good practice, or in cases where this is unavailable, it is applied to demonstrate that measures have been implemented up to the point where the cost of additional risk reduction is disproportionate to the benefit gained [6].

The aspiration to use robots in the nuclear industry requires hazards to be safely managed and the risks demonstrated to be ALARP. This paper investigates how this might be achieved to ensure all potential hazards are identified and prevented, with key safety measures recognised, implemented and maintained in an appropriate and pragmatic manner, benefitting from experience gained from wider industry.

Outside of the nuclear industry industrial robots are found increasingly in the workplace where it is widely acknowledged that robot movements can have the potential to cause humans physical harm and damage to other equipment. Deployment of robots in the nuclear industry also raises further concern that impact events may have the potential to result in loss of containment of nuclear material, and cause damage to nuclear safety significant equipment and instrumentation.

Operators and equipment must therefore be protected against the robot. The strict segregation of man and robot has previously been employed in wider industry as a
Key Hazard Management Strategy (HMS) to protect workers. The robot remained enclosed in a controlled area while it performed its tasks. In the present day, thanks to a new generation of robots and technologies segregation may no longer be necessary if the potential for collision is not perceived as being hazardous [7].

Assessment of Hazards

Robot Systems Regulation and Legal Requirements

The European Union (EU) formulates general safety objectives via a large number of directives, (circa 30 active directives currently available). However, only a small selection of directives are relevant to a typical machine builder and the safety objectives are more precisely specified through standards [7].

The standards have no direct legal status on their own until they are referenced in domestic laws and regulations. In practice, manufacturers of robotic Commercial Off-the-Shelf (COTS) equipment use the “Conformité Européenne” (CE) mark to document the fact that all relevant European directives have been applied and appropriate conformity to all assessment procedures achieved [7].

Based on the European Parliament and Council of the European Union Machinery Directive 2006/42/EC [8], a robot system is considered to be partly completed machinery. This means that robot systems require CE marking. The person placing the machine into a specific application is known as the ‘integrator’ and must perform the conformity assessment procedure to conclude a Declaration of Conformity [7].


Two standards from the ISO 10218 “Safety of Industrial Robots” Part 1 [12]: “Robots” and Part 2 [13]: “Robot systems and integration” are listed under the Machinery Directive 2006/42/EC [8] to specify detailed safety requirements. ISO 10218-1 is solely concerned with the actual robot system, whilst in contrast to this, ISO 10218-2 expands to the entire robot application [7].

In practice, the standards above have proved to be insufficient in their own right when it comes to safely implementing an actual Human and Robot Collaboration (HRC). Protective measures for HRC are therefore currently identified through ISO/TS15066 [14] in order to help production technicians and safety experts in the development of safe shared workspaces and the risk assessment process. This describes four types of collaboration reproduced below [7] as protection principles to ensure human safety is guaranteed at all times during collaborative operation [7], as shown in Figure 1:

1: Safety-Rated Monitored Stop

Here, the human only has access to the robot once stopped and the robot system must not start up again automatically and unexpectedly.

2: Hand Guiding

In this case the human only has access to a stationary robot. The hand guiding of the robot system can only be enabled by manually operating an enabling device.

3: Speed and Separation Monitoring

With this method, the distance between human and robot is permanently monitored by a sensor. The robot system moves with correspondingly safely reduced speed. The closer the human gets to the robot, the slower the robot becomes. If the distance is too short, a safety stop is triggered.

Safety is guaranteed in the first three methods by maintaining the distance between human and robot, to avoid collision. When implementing one of these three methods, no special HRC robots are necessary. Standard industrial robots can be used that are equipped with corresponding safety packages for speed monitoring, or workspace monitoring by the manufacturer.

4: Power and Force Limiting

In contrast to methods one to three, contact between human and robot is possible under certain circumstances, whereas in the case of method four, the manufacturer of the application must guarantee that the collision between human and robot is not hazardous. The manufacturer of the application confirms this with a signature on the declaration of conformity.

Risk Assessment

To ensure robot safety, manufacturers and users normally apply a three-stage risk assessment approach detailed in ISO 12100 reproduced below [9] as follows:

- Inherent safe design measures (hazard elimination);
- Safeguarding and complementary protective measures (fixed guards, movable guards with interlocks, safety devices); and
- Information for use (safe working practices for the use of the machinery, warning of residual risks, recommended Personal Protective Equipment (PPE)). Residual risk is then managed by the user.

The performance requirement of safety measures is set out in ISO 10218, which also mentions compliance with Safety Integrity Levels (SILs) which comes from vol-

![Fig. 1. Overview of Robot Systems Regulation and Standards.](image)
Assessment of Radiological Hazards

Radiological safety assessments follow a rigorous process and are required as part of Nuclear Installations Site Licence Conditions.

The fundamental requirement in any nuclear decommissioning safety case involving robot systems will be to demonstrate that hazards presenting radiological exposure; loss of containment of nuclear material; and damage to nuclear safety significant equipment and instrumentation can all be safely managed, and also that the identified risks are deemed ALARP.

A clear link of how the assessment will be implemented is known as the ‘Golden Thread’. This can be achieved through a Claims Arguments Evidence (CAE) approach, as illustrated in Figure 3. From a robotic CAE perspective, there is a top-level claim requirement to ensure all robot systems can be safely managed and the risks are ALARP. This is supported by a series of sub-claims listed below:

- All robot system hazards can be identified, and potential hazards understood.
- All robot system hazards can be adequately prevented or managed, by determining the unmitigated consequences such that appropriate safety measures can be identified and the risks can be shown to be ALARP.
- All key operational and engineering measures can be identified, implemented and maintained.

The foundation of a HMS in a nuclear robot system safety case will be based upon a standard hierarchical approach to safety. This starts with elimination of the hazard wherever possible, followed by substitution to replace the hazard, isolation of people from the hazard, administrative control, with reliance upon PPE being the weakest and therefore least favourable HMS as shown in Figure 4. It is argued that in the context of nuclear robot systems which operate remotely, the use of PPE is not necessarily relevant unless it relates to the need for human intervention, for example during repair or maintenance work.

The approach for developing a robot system safety case is summarised as:

- Identification of hazards;
- Assessment of hazards and identification of suitable safety measures;
- Substantiation of safety measures; and
- Implementation of safety measures.

A structured and systematic examination of robot systems will be undertaken using Hazard and Operability (HAZOP) studies to identify potential problems that may represent risks to personnel, or equipment, or prevent efficient operation.

Hazards are then assessed, and safety measures are identified in the safety case. The HMS developed for the robot system will be used to identify safety measures which are proportional to hazard severity, demonstrate there is sufficient strength in depth, and that the risk is ALARP.

The individual hazards identified by HAZ-OP will be presented in the form of a number of fault sequences. Each fault sequence starts with an initiating event that could
lead to unwanted consequences and place a demand on a set of safety measures. The assessment of the fault sequence included failure of some or all of these safety measures. Radiological safety assessments specify the Engineering and/or Operational Safety Measures that need to be in place to minimise the risks to acceptable levels, i.e. ALARP and ensure the adequacy of safety. The concept of defence in depth is fundamental to radiological safety to prevent accidents and if prevention fails, to limit potential consequences. For significant faults Design Basis Analysis (DBA) requires the designation of a passive safety measure, such as an enclosure wall, or two key independent safety measures, such as high integrity Control, Electrical and Instrumentation Equipment (CE&I)) with predefined action on failure and substitution arrangements. Alternatively, it is possible in some instances for Operational Safety Measures to be claimed, which must be carried out to prevent possible harm /dose uptake.

For lesser significant faults, DBA requires the designation of one safety measure, which can either be passive, or an item of CE&I equipment that does not need to have any predefined action on outage or substitution arrangements. Alternatively, it is possible in some instances for Operational Safety Measures, about operator actions, or plant conditions to be claimed which support the safety case. The various engineering safety measures in the safety case are uniquely identified as a Structure, System, or Component (SSC), and the safety function and performance requirement of each is recorded in an Engineering Schedule and substantiated against their required Safety Function, Performance Requirement and PFD. The operational safety measures and compliance arrangements are defined within a Clearance Certificate.

However a fault sequence is initiated, it is also important to identify the involvement of any Programmable Electronic Systems (PES) in protection/mitigation as the system may not be capable of substantiation, ultimately requiring a different safety measure to be defined. PES contain both hardware and software. Software is different from hardwired systems in that it has a greater potential for a number of systematic failures (as opposed to random failures) which may remain unrevealed for many years. Knowledge of the failure of a PES is usually only identified when the system fails in operation, because they employ hierarchical coding and identification of sequential coding errors are usually difficult.

Where the PES controls a process, the liability to initiate fault sequences must be recognised in the safety assessment, and an ‘initiator type’ safety function defined. Where a PES initiates a fault sequence, no credit may be claimed for protection by the same PES in the same fault sequence. Therefore, dependency upon PES for protection/mitigation should be minimised wherever possible.

PES should be distinguished from SMART Instruments – although the latter include some software (sometimes referred to as ‘firmware’), they are arguably very little different from the hardwired (‘dumb’) instruments.

Unlike a PES, SMART instrument software can be simulated, run inactively or actively with real-time communication between execution and operation limit. SMART instrument software may only be altered using configured operator parameters, allowing the opportunity to remove any potential coding error identified and for multiple level recovery. Hence SMART instrumentation is not prone to the same level of systematic failure.

There is currently little specific data for PES/SMART reliability available for the purposes of making a nuclear decommissioning safety case. This results in some frequency estimates (for comparison with criteria) that are over-estimated in comparison to reality, but this drawback is not as significant as using reliability figures that cannot easily be justified.

Any risk reduction benefit claimed for PES/SMART is currently generally limited. For example, a PES would normally be claimed within a possible PFD range of unity to 1 in 30.

For nuclear decommissioning purposes, substantiation of PES and SMART systems is achieved through interpretation of the relationship between PFD and SIL requirements contained in IEC 61508 [16].

Assessment of Robot Systems for Decommissioning Activities

There appears to be an understanding in wider industry that stringent standards for nuclear decommissioning places a requirement for CE&I safety measures to be substantiated to SIL 3, or even SIL 4 to meet the designation of high integrity protection systems. The dilemma in the nuclear industry is often a choice of placing reliance upon a single but complex safety measure, versus multiple layers of safety measures. Complex systems typically demand significant effort, and therefore cost more to substantiate and maintain, compared with systems involving multiple layers.

For the majority of nuclear decommissioning cases the integrity level designated to each individual hardwired ‘dumb’ CE&I layer of protection is usually no more than SIL 1 in practice, which provides a PFD of 1 in 100 and a risk reduction of 100 for each layer. Only in rare cases have claims been made on SIL 2 CE&I safety protection systems. It is argued that the substantiation process would prove far too onerous to achieve SIL 3, or SIL 4 level of integrity.

One common mis-understanding appears to be in the interpretation of safety integrity claims made upon multiple layer protection systems. An example multiple layer protection system arbitrarily consisting of 3 layers of protection is used to exemplify the mis-understanding. Architectures with 3 layers of CE&I protection are not the same as a SIL 3 system and should be substantiated as a series of 3 x SIL 1 separate systems. It is argued that the safety integrity level of such circumstances should default to the lowest common denominator, i.e. SIL 1, or possibly SIL 1 + 1 in rare circumstances.

A robot system recently deployed by NNL at its Preston Laboratory included the use of a robot controlled 5kW laser which enabled selective, semi-autonomous controlled laser cutting for disassembly in confined spaces [20]. This capability consisted of a KUKA KR series robot which operated in an enclosure with a SIL 1 rated hardwired door interlock system, which disal-
Fig. 5. Future Deployment of Robot Systems for Decommissioning Activities Operated within a Virtual Enclosure.

allowed laser activation and robotic movement if anyone attempted to access the enclosure during usage.

Multiple safety systems focused on limiting the robot’s movement to a controlled safe working area. This provided additional laser firing safety inputs, reducing the amount of human intervention required in order to reduce rig downtime. The KUKA robot included physical hard-stops installed in each robot joint which helped reduce potential damage to the enclosure, as well as limiting its working area.

Based on the methods described earlier for HRC, the NNL robot system safety case at Preston Laboratory ultimately relied primarily upon claims on ‘dumb’ hardwired door interlock systems and physical end stops, rather than claims on robot SMART systems.

It is recognised that future deployment of robot systems for decommissioning activities may not benefit from physical enclosures, and will require hazard management strategies moving towards methods described previously under HRC 3 or HRC 4 to prevent potential collisions.

NNL are currently reviewing available industry-wide SMART technology together with proof of concept non-active commissioning trials, to support the necessary substantiation to achieve a SIL 1 rating for individual layers within a diverse multi layer protection system. It is argued that such an approach could prove useful to create virtual enclosures (as shown in Figure 5), allowing HRC 3 or HRC 4 for nuclear decommissioning.

Historically most of the ISO standards defined for robot systems have been developed singularly for the automotive industry with the opportunity for human intervention for teach and repeat. Future deployment of SMART robot systems for decommissioning activities enable the opportunity for the review and monitoring of sequences with constant communication to the robot prior, during and after the execution of operations.

Path Forwards

This paper has examined the underpinning Regulations, Standards and Technical Assessment Guides necessary for the deployment of 'robotic systems' to remove the need for operators to undertake manual nuclear decommissioning activities. It is NNL’s view that consideration of the approach taken for the robot systems outside of traditional industrial settings, for example their use in medical applications, may have useful applicability for safety in harsh nuclear decommissioning environments and HRC 3 or HRC 4 interaction.

NNL believes the adoption of HRC 3 or HRC 4 methods for decommissioning purposes will require a change in the way the nuclear industry views the reliability of SMART protective layers. This will be achieved by striking a balance between risk versus the benefits gained from using robot systems. A challenge to the current position of high risk and low confidence in SMART protective layers will offer the potential for decommissioning risk reduction safer, sooner and cheaper.

The forthcoming NNL review of wider industry SMART instrument applications will make reference to any guidance currently in the process of being established by the International Atomic Energy Agency (IAEA), due for publication later in 2020. It is expected that the IAEA guidance will provide a common technical basis of how to design, select and evaluate candidate SMART devices for their safe use in nuclear safety systems, including instrumentation and control, electrical, mechanical and other areas [21].

NNL aims to improve on the current position by establishing a higher degree of confidence in SMART protection systems, which can provide a safety function to prevent impact causing harm to humans and equipment resulting in loss of containment of nuclear material. This will be supported by a safety performance requirement to operate within specified distances within a virtual enclosure to ensure the risk of generating a hazardous collision between robot, human and equipment is reduced to ALARP.

The intention is to ensure the science becomes a robust, safe and efficient engineered solution for nuclear industry decommissioning activities and achieve UK NDA’s ‘Grand Challenges’.

References

Robots in nuclear decommissioning

38


VGB POWERTECH as printed edition, monthly published, 11 issues a year

Annual edition as CD or DVD with all issues from 1990 to 2019: Profound knowledge about electricity and heat generation and storage.

Order now at www.vgb.org/shop
Benefit from the image of our journal, in which only technical papers reviewed by experts are published.

Reprints are produced individually according to your requests and with the same contents as the original paper.

Your CI can be transferred into the paper, or you will get a copy of the original layout from our journal.

Please do not hesitate to contact us!
Mr Gregor Scharpey | phone: +49 201 8128-200 | E-mail: mark@vgb.org