



ONR GUIDE			
CRITICALITY WARNING SYSTEMS			
Document Type:	Nuclear Safety Technical Assessment Guide		
Unique Document ID and Revision No:	NS-TAST-GD-018 Revision 8		
Date Issued:	June 2019	Review Date:	Oct 2023
Approved by:	Gareth Thomas	Professional Lead	
Record Reference:	CM9 Folder 1.1.3.978. (2020/281104)		
Revision commentary:	Rev 7: Routine update Rev 8: Updated Review Period		

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE AND SCOPE	2
3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION	2
4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS.....	4
5. GENERAL ADVICE TO ASSESSORS	5
6. FEATURES OF A CID SYSTEM	7
7. ALTERNATIVE MEASURES TO CID SYSTEMS.....	10
8. FEATURES OF A CID OMISSION CASE	10
9. REFERENCES	15

© Office for Nuclear Regulation, 2019

If you wish to reuse this information visit www.onr.org.uk/copyright for details.

Published 06/19

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

1. INTRODUCTION

- 1.1 ONR has established its Safety Assessment Principles (SAPs) which apply to the assessment by ONR specialist inspectors of safety cases for nuclear facilities that may be operated by potential licensees, existing licensees, or other duty-holders. The principles presented in the SAPs are supported by a suite of guides to further assist ONR's inspectors in their technical assessment work in support of making regulatory judgements and decisions. This technical assessment guide is one of these guides.

2. PURPOSE AND SCOPE

- 2.1 This document provides guidance to ONR inspectors on the assessment of licensees' arrangements for the installation or omission of Criticality Warning Systems (CWS) as described in outline in ONR's Safety Assessment Principles Paragraph 594 [1].
- 2.2 Note that CWS is a general term used in this document to cover all the various types of system that can be used to provide warning that a criticality incident has occurred. The term "Criticality Incident Detection (CID) system" is used to refer to a specific type of system involving multiple detectors and coincidence voting to provide a low frequency of false alarms.
- 2.3 This Technical Assessment Guide (TAG) contains guidance to advise and inform ONR inspectors in the exercise of their professional regulatory judgement. As with all guidance, inspectors should use their judgement and discretion in the depth and scope to which they employ this guidance.

3. RELATIONSHIP TO LICENCE AND OTHER RELEVANT LEGISLATION

- 3.1 The Licence Conditions are listed in full in [2]. For Ionising Radiations Regulations 2017 (IRR17), see [3].

LC11: Emergency Arrangements

- 3.2 The provision of a CWS would normally form part of the licensee's emergency arrangements for warning and evacuation of employees. Emergency exercises should be held to test these arrangements periodically.

LC15: Periodic Review

- 3.3 The adequacy of the safety case, including arrangements for CWS, should be reviewed against the current operating conditions (which include, for example, changes in the scope and nature of fissile material movements, or alterations to the building structure), and those foreseen for the next period of operation (usually 10 years), and take into account anticipated conditions over the lifetime of the facility.

LC19: Construction or Installation of New Plant

- 3.4 The design of a new facility should be considered at an early stage in order to assess the need for a CWS. The licensee should demonstrate that an installed CWS would detect the minimum incident of concern in all areas of the facility in which a criticality incident is foreseeable.

LC 20: Modification to Design of Plant Under Construction

- 3.5 Such modifications should be assessed to ensure that they do not impact adversely on the need for a CWS within the facility (e.g., by changing the sizes of vessels or specification of materials). Modifications could also impact on the ability of a CWS to detect an incident, e.g., by creating additional shielding or distance between the potential site of a criticality and the CWS detectors.

LC 21: Commissioning

- 3.6 Inactive and, where appropriate, active commissioning tests should be carried out to ensure, for example, that the design criteria for the CWS have been met. The training of staff in their response to the alarm should also be tested during commissioning.

LC 22: Modification or Experiment on Existing Plant

- 3.7 Such modifications should be assessed to ensure that they do not impact adversely on the need for a CWS within the facility (e.g., by changing the sizes of vessels or specification of materials). Modifications could also impact on the ability of a CWS to detect an incident, e.g., by creating additional shielding or distance between the potential site of a criticality and the CWS detectors.

LC23: Operating Rules

- 3.8 This licence condition refers to the need for an adequate safety case. Where fissile material may be present, the default should always be that a CWS should be installed unless omission can be justified. Safety documentation would normally comprise the case for omission of a CWS or the technical details justifying the number and spacing of the installed detectors.

LC27: Safety Mechanisms, Devices and Circuits

- 3.9 CWS do not normally provide any direct fault sequence termination function. CWS should normally be classified as safety-related equipment rather than safety mechanisms. However, if a CWS is linked to an active accident termination system then this may increase its safety classification to a safety mechanism.

LC28: Examination, Inspection, Maintenance and Testing

- 3.10 It is expected that a CWS would form part of the licensee's site-wide arrangements under this licence condition. An appropriate Examination, Investigation, Maintenance and Testing (EIMT) regime is required in order to achieve the necessary level of reliability.

IRR17 Regulation 8: Radiation Risk Assessments

- 3.11 The licensee should carry out a risk assessment in order to identify the measures required to restrict the exposures of workers and the public to ionising radiation. Such measures could include the provision of a CWS to mitigate the consequences of a criticality incident.

IRR17 Regulation 9: Restriction of Exposure

- 3.12 The restriction of exposure to ionising radiation should, wherever reasonably practicable, be achieved by engineering controls and design features. Attention should first be given to the provision of systems to reduce the frequency of a criticality incident to an acceptably low level. However, a CWS may also be provided to mitigate the consequences of a criticality incident.

IRR17 Regulation 11: Maintenance and Examination of Engineering Controls etc. and Personal Protective Equipment

- 3.13 The licensee should put in place adequate maintenance and examination arrangements to ensure that an installed CWS is working correctly and achieving an appropriate level of reliability.

IRR17 Regulation 13: Contingency Plans

- 3.14 Whenever a radiation accident is reasonably foreseeable, the licensee should prepare contingency plans to restrict the exposure to ionising radiation of all those who may be affected. The provision of a CWS may be one part of a contingency plan for criticality incidents.

4. RELATIONSHIP TO SAPS, WENRA REFERENCE LEVELS AND IAEA SAFETY STANDARDS

SAPs Addressed

- 4.1 It should be noted that the SAPs form a complete document and should be taken as a whole. It is not appropriate to base an assessment on a few selected principles, possibly taken out of context, without considering all other relevant principles. Indeed, many of the principles are relevant to CWS and ONR assessors should constantly bear this in mind. Hence, in order to carry out a comprehensive assessment, it will generally be necessary to refer to several other TAGs in addition to this one. This section reproduces the only paragraph in the SAPs that refers explicitly to CWS:

“594. Adequate warning systems (not necessarily a Criticality Incident Detection (CID) system) should be provided wherever fissile material is present, unless an assessment shows that no criticality excursion could give any individual a whole body dose exceeding the annual whole body dose limit, or that the predicted frequency is acceptably low. An estimate of the criticality consequences should inform the need for the installation of the warning system. Where appropriate, a criticality warning system may have an additional function and be linked to safety systems design to achieve the safe termination of the criticality incident (e.g. it may initiate boron injection) or trigger an alarm.”

Discussion of SAPs

- 4.2 From Paragraph 594 it can be seen that two possible approaches can be adopted in making a CWS omission case; one based on the dose consequences of a criticality incident and one based on the frequency of a criticality incident.
- 4.3 The annual whole-body dose limit is currently 20 mSv [3] and the dose criterion in SAPs Paragraph 594 has been chosen to align with this value. A CWS omission argument may be made on the basis that no individual would receive a dose in excess of this value as a result of the maximum foreseeable incident.
- 4.4 It should be noted that different dose criteria have been adopted by licensees for making consequence-based CWS omission arguments, e.g., 100 mSv and 500 mGy. The licensee should justify the dose criterion if it is greater than 20 mSv.
- 4.5 For frequency-based CWS omission cases, in order to judge whether the frequency of criticality is acceptably low, the current approach, which we support, is to use the criterion developed by Aspinall and Daniels in the 1960s [4]. Namely, all criticality controls should be assumed to have failed and a judgement made as to whether criticality would then be reasonably expected in the natural order of events. If criticality would be reasonably expected then a CWS should be provided. This criterion is discussed in detail in Section 8. ONR inspectors should consider complementary approaches on a case-by-case basis.
- 4.6 In the unlikely event of a criticality incident, it is important to be able to terminate the incident as quickly as possible. This is particularly true for liquid systems where an

incident could continue for several hours in the absence of any intervention, e.g., Tokai Mura in Japan in 1999. Hence, the provision of systems to terminate a criticality incident should be considered. These could include a means to inject a neutron poison such as boron or gadolinium, isolation valves to stop the inflow of fissile solutions, and drains to allow fissile solutions to be removed to geometrically favourable vessels. Clearly, all of these systems would need to be operated remotely.

WENRA Reference Levels, IAEA Safety Standards and Other Safety Standards

- 4.7 There are no WENRA reference levels referring explicitly to CWS.
- 4.8 The IAEA has developed criticality safety guidance in Ref. [5], which contains advice on CWS.
- 4.9 There are standards applicable to CWS from the British Standards Organisation (BSO), International Standards Organisation (ISO) and International Electrotechnical Commission (IEC). See Refs. [6, 7, 8, 9, 10, 11] for further details.
- 4.10 The Safety Directors' Forum has published a good practice guide to Criticality Detection [12].

5. GENERAL ADVICE TO ASSESSORS

Introduction

- 5.1 Licensees should carry out criticality safety assessments for operations involving significant quantities of fissile material. Licensees should also consider the need for a CWS to mitigate the consequences of a criticality incident in cases where the omission criteria outlined in Paragraph 594 of the SAPs are not satisfied. Part of ONR's specialist assessment function is the assessment of the adequacy of cases which describe the details of an installed CWS or justify the omission of a CWS.
- 5.2 The UK Nuclear Industry's Safety Directors' Forum has produced guidance on criticality detection [12] which may be of use to inspectors.

ALARP Considerations

- 5.3 The fundamental requirement in terms of risk reduction is the ALARP principle, which states that risks should be reduced to a level that is as low as reasonably practicable. This applies to all risks, including that from a criticality incident.
- 5.4 Although a CWS does not reduce the frequency of a criticality incident, it can reduce the consequences (and hence the risk) by triggering a rapid evacuation of the facility. Hence, a CWS should generally be installed unless the licensee can make an acceptable omission case. As discussed later, the decision on whether to install a CWS may, in general, be based on both quantitative and qualitative factors, although primary consideration should be given to the qualitative factors. Moreover, an holistic approach should be adopted and consideration given to all of the relevant factors in reaching a balanced decision on whether a CWS is required.
- 5.5 In other words, it is no use reducing the risk from criticality to a very low level if this is more than offset by a large increase in another component of the risk. Rather, an holistic approach should be taken to ensure that the total risk is reduced to a level that is ALARP.

Hierarchy of Protection

- 5.6 It should be noted that the provision of safety measures, both engineered and managerial, to reduce the frequency of a criticality incident should be considered before the provision of measures to mitigate the consequences, e.g., CWS.
- 5.7 It is necessary to make an adequate criticality safety case to demonstrate that the frequency of criticality will be acceptably low. This is consistent with the hierarchy of protective measures specified in the SAPs, which states that, for any hazard, the first consideration should be to attempt to eliminate (or reduce the frequency of) the hazard.
- 5.8 The criticality safety case should be produced on an iterative basis alongside a CWS omission case and should include all safety measures required to reduce the frequency of a criticality incident to an acceptably low level.
- 5.9 Licensees should then consider whether it is appropriate to provide a CWS (and/or other measures such as additional shielding) to mitigate the consequences of a criticality incident, or instead consider whether it appropriate that a CWS can be omitted.
- 5.10 In other words, it is not acceptable to simply provide a CWS to mitigate the consequences of a criticality incident in preference to engineered (or administrative) measures to reduce the frequency of an incident.
- 5.11 Emphasis should be placed on the criticality assessment to provide measures to reduce the frequency of a criticality before mitigating consequences, e.g., via a CWS. However, it should be noted that in most circumstances a CWS is provided to mitigate against the unforeseen risk rather than the foreseen risk identified in the safety assessment.

Purpose of a CWS

- 5.12 The purpose of installing a CWS is primarily to limit the exposure, and hence the risk, to individuals by providing an alarm to initiate prompt evacuation in the event of a criticality incident. With some systems, further fission spikes may occur some seconds or minutes after the initial spike, and prompt evacuation will prevent exposure from these further spikes.

ONR Position on Installation or Omission of CWS

- 5.13 ONR assessors should keep in mind that our starting point is that CWS should always be installed in areas where fissile materials are stored, processed, handled, etc., unless omission can be justified. It is up to the licensee to justify reasons for not putting in such a system.
- 5.14 Hence, with regard to CWS, licensees have two options:
- i) install a CWS and demonstrate that the design and operation are appropriate; or
 - ii) produce a CWS omission case that is acceptable to ONR.
- 5.15 The licensee has to justify the omission (rather than inclusion) of such systems. In many instances, this requirement can be complied with using simple deterministic arguments to demonstrate that a criticality incident is not foreseeable, e.g., for a facility such as a laboratory that only handles a small fraction of the minimum critical mass. Alternatively, the licensee may base a CWS omission argument on the fact that the consequences of a criticality incident would be acceptably low, due to the presence of massive shielding or occupancy restrictions.

Shielding Considerations in CWS Omission Cases

- 5.16 If the dose to the operator is limited by shielding then this might form the basis of an acceptable CWS omission case. However, care should be taken in assessing the safety case to ensure that a justifiably bounding case in terms of fission yield, neutron/gamma fluxes and shield attenuation have been identified. Changes in shielding arrangements may prompt a review of the CWS omission case if appropriate.

Occupancy Considerations in CWS Omission Cases

- 5.17 There will be examples of areas where occupancy is restricted due to high radiation levels, e.g., shielded cells. This could form the basis of an acceptable CWS omission case. However, ONR will be less willing to accept arguments based on limited occupancy where the only restrictions on occupancy are due to administrative controls.

6. FEATURES OF A CID SYSTEM

Introduction

- 6.1 Many of the CWS currently in operation in the UK are actually CID systems, incorporating multiple detectors and a coincidence voting system to provide high reliability against false alarms. This section describes the features ONR would expect to see in CID systems.

Facility Coverage

- 6.2 Licensees should aim to show that all possible locations in which a criticality incident is foreseeable are covered by a CID system. However, ONR assessors may need to take into account the likely distribution of fissile material and worker occupancy in judging the adequacy of the facility coverage.

Control and Instrumentation

- 6.3 Although the probability of a criticality incident may be very low, it is important that the CID system operates correctly if it is called upon. The licensee should demonstrate that adequate EIMT arrangements are in place to maintain an appropriate level of reliability. In addition, adequate redundancy, segregation and high engineering quality must be demonstrated.
- 6.4 Detailed guidance on the characteristics required of safety systems and safety-related instrumentation is given in Refs. [13, 14]. Guidance on performance and testing requirements for CID systems is given in Ref. [10].

Minimum Incident of Concern

- 6.5 The total yield from a criticality incident can vary over a significant range and is difficult to predict. A CID system should be able to detect the minimum size incident of concern. Following Ref. [15], this is currently taken to be:

for close working (< 0.5 m) operations:

10^{14} fissions over a period of between 1 ms and 0.5 s for fast systems; or
 10^{14} fissions over a period of between 1 ms and 60 s for slow systems; and

for non-close working (> 0.5 m) operations:

10^{15} fissions over a period of between 1 ms and 5 s for fast systems; or
 10^{15} fissions over a period of between 1 ms and 60 s for slow systems.

- 6.6 In cases where an incident size of 10^{15} fissions would not be detectable, e.g., due to the presence of massive bulk shielding, the minimum size incident of concern may be taken to be that which would give the most highly exposed individual an unacceptable whole-body dose. If the maximum foreseeable incident would not give the most highly exposed individual an unacceptable whole-body dose, this may form the basis of a CID omission case.
- 6.7 In general, dry metallic systems give rise to fast incidents and solution systems give rise to slow incidents. The licensee should provide a full justification for the choice of incident type as fast or slow.
- 6.8 In general, the smaller the incident, the more difficult it is to detect. ONR assessors should seek assurance that the CID system is capable of detecting the minimum size incident of concern in all areas of the plant in which it is foreseeable that a criticality incident could occur.

Source Modelling

- 6.9 In many cases, licensees might choose to model a criticality incident as a point source. ONR assessors should bear in mind that this may lead to an overestimate of the doses to the CID detectors in cases where an incident would occur in a significant volume, e.g., for liquid systems, since self-shielding effects are not modelled.
- 6.10 The licensee should provide justification for the values chosen for the following parameters as applicable:
- i) Incident yield, i.e. number of fissions;
 - ii) Number of neutrons emitted per fission;
 - iii) Neutron energy spectrum from fission;
 - iv) Number of prompt gamma rays emitted per fission; and
 - v) Gamma-ray energy spectrum from fission.

Detector Characteristics

- 6.11 In principle, the detectors in a CID system could be either neutron or gamma detectors. However, in practice, most systems tend to use gamma detectors. In general, for shielded systems, the gamma doses received by the detectors could have four components:
- i) Prompt gamma rays from fission;
 - ii) Secondary gamma rays produced by the interaction of neutrons in materials;
 - iii) Gamma rays from the decay of fission products; and
 - iv) Gamma rays from the decay of activation products.
- 6.12 It is acceptable to consider all four components (noting that the doses due to activation gamma rays are generally negligible) but caution should be exercised to ensure that the doses to the detectors are not overestimated. For example, in contrast to shielding assessments, the densities and thicknesses of the shielding materials should be assumed to have their maximum values.
- 6.13 ONR assessors need to be satisfied that the engineered system is fit for purpose. This includes the need for the system to have a high reliability against spurious trips (e.g., many CID systems contain 3 separate rings of detectors and operate on a 2-out-of-3 coincidence voting system to reduce the frequency of false alarms).
- 6.14 One of the key issues which should be addressed in the safety case is the number and siting of detectors. It is sometimes the case, for example, that detector heads are not

grouped together in sets of 3 at plant locations. Rather, individual heads from each ring may be distributed throughout the facility. As a minimum, licensees should demonstrate that 2 detectors from different rings would trigger in a criticality incident.

- 6.15 CID control cabinets contain sensitive electronic components which can be damaged by ionising radiation. Consideration should be given to the location of the CID cabinet to ensure that it remains functional during and after a criticality incident. It may be appropriate to provide shielding for the CID cabinet.

Alarm Characteristics

- 6.16 Licensees' safety cases should specify requirements for the audibility of the alarm such that it is sufficient and fit for purpose in all relevant areas of the facility. This may need to include areas where audibility is restricted due to the need for workers to wear PPE or high levels of background noise.
- 6.17 Details of the detector response should be guided by Ref. [15].
- 6.18 The benefit of a CID system derives from the speed with which evacuation occurs. Hence, the alarm should be distinct from all other alarms used in the facility and should be instantly recognisable by the workforce.

Criticality Emergency Planning

- 6.19 Public Health England, PHE¹, has provided general guidance on the protection of on-site personnel in the event of a radiation accident [16]. This guidance applies to all types of sites, including nuclear sites. PHE points out that a radiation accident may give rise to both deterministic health effects and stochastic health effects. (Note that, in general, off-site personnel are unlikely to receive doses high enough to result in deterministic effects as a result of a criticality incident).
- 6.20 The PHE guidance states that the purpose of prior measures for on-site personnel for radiation accidents should be to avoid deterministic effects and to reduce the probability of stochastic effects so far as is reasonably practicable (in line with the ALARP principle). Priority should be given to the avoidance of deterministic effects.
- 6.21 A criticality incident is one type of radiation accident that could give rise to very high doses, resulting in deterministic effects to on-site personnel. One factor which can contribute to reducing the doses from a criticality incident is the provision of a CID system, which would initiate a prompt evacuation in the event of a criticality accident.
- 6.22 The whole-body dose targets for the avoidance of deterministic effects recommended by PHE are: 1 Gy for low LET (linear energy transfer) radiation, which includes gamma rays and X-rays; and 0.5 Gy for neutrons. These targets are set below the current best estimates of the true thresholds in order to provide confidence that deterministic effects will be avoided.
- 6.23 Following on from Ref. [16], PHE has provided further advice on the protection of on-site personnel in the event of a radiation accident [17]. PHE states that all countermeasures with the potential for avoiding deterministic effects should be considered to be justified unless strong arguments to the contrary can be presented.
- 6.24 Arguments that could be used to justify not implementing a particular countermeasure could be based on excessive costs (e.g., time, money or trouble) associated with the countermeasure or the very low probability of a radiation accident occurring.

¹ Formerly the *Health Protection Agency* (HPA) and before that the *National Radiological Protection Board* (NRPB).

- 6.25 PHE guidance also states that the following countermeasures should always be included (see Table 8 in Ref. [17]):
- i) Provision of suitable detectors, alarms and warning signs;
 - ii) Training of staff in the meaning of the alarms and warning signs;
 - iii) Provision of clearly signed routes to aid evacuation; and
 - iv) Training and rehearsals to ensure that staff members are familiar with the procedures to follow in the event of a radiation accident.
- 6.26 Hence, in cases where an acceptable CWS omission argument cannot be made, ONR would expect all the countermeasures listed above to be implemented.
- 6.27 In such cases, the licensee should also identify an appropriate dose contour for evacuation. As mentioned earlier, since the threshold for deterministic effects is generally assumed to occur at a whole-body dose of around 500 mGy, ONR would expect licensees to adopt a dose criterion no higher than this value for identification of the dose contour for evacuation.
- 6.28 With regard to evacuation contours, practices within industry vary with some contours being constrained to lie within the building boundary using shielding. Other contours extend to areas within the licensed site boundary. ONR assessors should challenge licensees in cases where contours extend beyond the licensed site boundary.
- 6.29 A further topic is the consideration given by the licensee to the actions to be taken in the event of coincident alarms. For example, it should be considered what the emergency procedures require if the on-site release alarm (requiring sheltering in the plant) were to activate concurrently with a criticality alarm (requiring evacuation from the plant).

7. ALTERNATIVE MEASURES TO CID SYSTEMS

- 7.1 Section 6 presents ONR's understanding of the characteristics of a CID system. In particular, a 2-out-of-3 coincidence voting system is often used to reduce the frequency of false alarms and achieve a high level of reliability.
- 7.2 There are many examples in the UK nuclear industry where such systems have been installed. However, there are also cases where alternative, e.g., less expensive, measures to a CID system are sufficient and the installation of a full CID system is not justified.
- 7.3 For example, for some short-term activities where the risk of criticality is only present for a short time, a CWS consisting of a number of portable gamma (or possibly neutron) monitors may provide a suitably reliable alarm function. In these cases, the CWS may only need to provide coverage for that part of the facility local to the operations involving fissile material. Such situations may arise during one-off or decommissioning activities.

8. FEATURES OF A CID OMISSION CASE

Introduction

- 8.1 This section discusses the types of arguments that licensees may use to justify the omission of a CID system. Similar arguments may also be used to justify the omission of other types of CWS.

Current Position

8.2 In the UK, CID omission cases for facilities handling fissile material are generally based on one of the following two criteria:

Criterion 1: A CID system is not required where an assessment shows that the maximum dose to the most exposed individual from a maximum foreseeable criticality incident (outside a nuclear reactor) would not exceed the maximum acceptable emergency dose; or

Criterion 2: A CID system should be provided at all places where fissile material may be used or stored, unless it is confidently judged that in the event of the failure of any or all of those criticality controls which rely on human agency or on mechanical or electrical devices, criticality would not reasonably be expected having regard to the nature of the particular operations and facility concerned.

8.3 Criterion 1 has been used to make CID omission cases for fuel storage ponds, in cases where assessments show that the significant depth of water would provide sufficient shielding to reduce the doses from a maximum foreseeable criticality incident to below the maximum acceptable emergency dose.

8.4 Criterion 2 dates from the work of Aspinall and Daniels in the 1960s [4] and has been reiterated in the more recent work of Delafield and Clifton in the 1980s [15]. Many CID omission cases have been based on the use of this criterion.

8.5 The following justification for considering the failure of all criticality controls is presented in Ref. [4]:

“It is common for an investigation, whether into a criticality control infringement, or a glove box failure, or a conventional industrial accident, to reveal a combination of failures and circumstances leading to the accident such that, had they been postulated before the incident, they would likely have been dismissed as incredible.”

8.6 The following additional guidance is provided in Ref. [4] on how the phrase “reasonably expected” should be interpreted:

“However, having countenanced the failure of all operational controls, consideration ought then to be directed to the consequences which may be expected in the natural or reasonably foreseeable order of events from freeing the materials from all such artificial controls; i.e. without importing further high improbabilities by way of deliberate and difficult manipulations of the materials into ingenious but unnatural forms and shapes of extra reactivity; or the intrusion of materials unlikely to be present; or of abnormal accumulations of materials well beyond those which could be expected in the natural order of events or within a period in which the control failure is bound to be revealed.”

8.7 To summarise, the criticality safety case should cater for all reasonably foreseeable faults, whereas a CID system is provided to cater for the unforeseeable. It is the last line of defence, designed to work when everything else has failed. An illustration of this concept is presented in Ref. [18].

Quantitative vs Qualitative Arguments

- 8.8 In making a CID omission case, both qualitative and quantitative factors may be considered. The qualitative factors constitute what can be described as Relevant Good Practice (RGP), whereas the quantitative factors might take the form of a Cost Benefit Analysis (CBA), which may be informed by a Probabilistic Safety Assessment (PSA). Detailed guidance on CBA is given in Refs. [5, 19].
- 8.9 It must be stressed that the primary consideration should be the qualitative factors (RGP), since PSA is generally subject to significant uncertainties, which is partly due to the fact that PSA considers foreseen rather than unforeseen events, unlike a CWS omission case. In some cases, quantitative factors (e.g., CBA) may be used to support an omission case. However, it is recognised that there will be cases where a CBA suggests that a CID system is not required but this is modified by considerations of RGP.

Relevant Good Practice

- 8.10 There are many cases in which it is very difficult to obtain an estimate of the frequency of a criticality incident and hence reliance must be placed on qualitative considerations alone to decide whether a CID system should be installed.
- 8.11 For example, consider the case of a large tank containing fissile-bearing sludge where significantly more than the minimum critical mass of the fissile material is present. Under normal circumstances, criticality safety may be ensured because of the presence of neutron absorbers and the dilution of the fissile material by the other materials present.
- 8.12 In order for a criticality incident to occur, a significant fraction of the fissile material would need to congregate into an optimally moderated unfavourable geometry with significant reflection. It is intuitively obvious that the probability of this situation occurring is low but it would be very difficult to obtain a numerical estimate of this probability.
- 8.13 In such cases, it is recommended that the nature of the facility and its operations should be considered. In particular, it is appropriate to consider three different categories of facility:

Category A: High risk facilities, or facilities with a high susceptibility to criticality accidents occurring from unforeseen circumstances, where there can be no doubt about the requirement to install a CID system (e.g., in areas of large fissile inventory, high U-235 enrichments, high Pu-239 contents, many process operations, high worker occupancy, multiple safety mechanisms/protection systems).;

Category B: Areas where a safety hazard has been identified and capital expenditure has to be balanced against potential risk. Omission cases are unlikely to be acceptable if there is high occupancy, a large fissile inventory, operator control, etc., are involved in the process; and

Category C: Low risk facilities, or facilities with a low susceptibility to criticality accidents occurring from unforeseen circumstances, where there is no doubt that installation of a CID system would be an inappropriate, unreasonable and unnecessary burden on industry. We would expect a strong

omission case in areas of high occupancy.

- 8.14 The decision on whether to install a CID system should be relatively straightforward for Category A and Category C facilities, i.e. Category A will usually require a CID system whereas Category C will usually not. However, for Category B facilities more effort may be required to convince ONR assessors; Ref. [20] provides advice that assessors might find useful.
- 8.15 In these cases, the ONR assessor should consider what has been done in similar facilities in the past. For example, if a CID system has generally been installed in a particular type of facility in the past, then it would be reasonable to expect that this practice should be continued in the future for facilities of this type unless a very robust omission case can be made.
- 8.16 An exception to this may occur for an old facility where no attempt was made to produce a CID omission case. In some such cases, it may be possible to make a CID omission case for a new facility even though a similar existing facility may have an installed CID system.

Acts of Sabotage

- 8.17 In some cases, a deliberate act of sabotage would be required to form a critical system, e.g., the deliberate malicious introduction of excess fissile material. Such circumstances are essentially a security matter rather than a safety issue and are considered to be outside the scope of a CID omission case.
- 8.18 Hence, if the only credible route to criticality would involve the deliberate malicious introduction of excess fissile material, then a satisfactory CID omission case can be made relatively simply.

Fast Criticality Incidents

- 8.19 It has been argued in the past that, where a criticality incident would be fast, e.g., for a dry metallic system, a CID system would provide no benefit and could be omitted, since it would not prevent lethal doses being received by nearby workers.
- 8.20 However, Ref. [4] points out that, in such cases, a CID system will still provide some benefit since the doses from decaying fission products to other workers situated further away will be reduced. In such cases, rapid evacuation may make the difference between these workers receiving lethal and non-lethal doses. Moreover, the doses to other workers who may otherwise subsequently enter the area would be reduced if the area was evacuated and re-entry restricted.
- 8.21 In addition, in many facilities it would be difficult to be sure of the type of criticality that might occur because of the range of activities that are undertaken. Ref. [21] shows that most of the criticality incidents that have occurred to date were not terminated after the initial burst of radiation but consisted of repeated bursts of radiation, and so rapid evacuation will usually be a very effective mitigation measure even for nearby workers. Hence, it is not considered to be acceptable to base a CID omission case simply on the fact that a criticality incident would be fast.

Arguments for Removal of a CID System

- 8.22 Arguments for the removal of a CID system should be supported by an adequate omission case. For example, it may be possible to justify deactivating or removing the CID system from a facility in which the inventory of fissile material is being significantly reduced, e.g., due to a change in the nature of operations or as a result of decommissioning activities. In such cases, a point will come where the risk of a

criticality incident has been reduced to a sufficiently low level such that a CID system is no longer required.

- 8.23 In general, the frequency of false alarms will increase as a CID system ages, although this can be minimised by careful maintenance and care. The licensee may argue that a point has been reached where the risk of personal injury associated with relatively frequent evacuations due to false alarms outweighs the risk from a criticality incident and hence that the CID system should be deactivated or removed. In such cases, in order to make an acceptable omission case, the licensee will need to demonstrate that all reasonably practicable steps have been taken to keep the frequency of false alarms to a minimum.

Other Approaches to CID Omission Cases

- 8.24 In assessing the possible requirement for a CID system, it is appropriate to take an holistic approach and to consider all the potential benefits and harms when deciding whether such a system should be provided.
- 8.25 For example, there may be a risk of the spread of radioactive contamination and personal injury during a rapid evacuation from a contaminated area in which workers are required to wear PPE such as ventilated suits. In addition, there will generally be radiological risks associated with periodic testing of the CID detectors using radioactive sources, and conventional risks associated with the installation and maintenance of the CID detectors.
- 8.26 Although the Aspinall and Daniels criterion [4] described in Section 8 is commonly used, the above factors may also be taken into consideration in coming to a balanced decision on whether a CID system is required.
- 8.27 In other words, as mentioned earlier, it is no use reducing the risk from criticality to a very low level if this is more than offset by a large increase in another component of the risk. Rather, an holistic approach should be taken to ensure that the total risk is reduced to a level that is ALARP.

9. REFERENCES

- [1] *Safety Assessment Principles for Nuclear Facilities*. 2014, Rev 0.
- [2] *Licence condition handbook*. Office for Nuclear Regulation. February 2017.
<https://www.onr.org.uk/documents/licence-condition-handbook.pdf>.
- [3] *The Ionising Radiations Regulations 2017*.
- [4] *Review of UKAEA Criticality Detection and Alarm Systems, Part 1: Provision and Design Principles*, AHSB(S) R 92K, J Aspinall and J T Daniels, 1965.
- [5] *Criticality Safety in the Handling of Fissile Material*, IAEA safety Standards Series No. SSG-27, 2014.
- [6] *BS ISO 1709:2018, Fissile materials, Principles in criticality safety in storing, handling and processing*.
- [7] *BS ISO 27467:2009, ISO 27467:2009(E), Nuclear Criticality Safety — Analysis Of A Postulated Criticality Accident*.
- [8] *BS ISO 11320:2011, Nuclear Criticality Safety — Emergency Preparedness And Response*.
- [9] *BS ISO 16117, Nuclear Criticality Safety - Estimation Of The Number Of Fissions Of A Postulated Criticality Accident*.
- [10] *ISO 7753:1987, Nuclear Energy – Performance and Testing Requirements for Criticality Detection and Alarm Systems*.
- [11] *IEC 60860-1987, Warning Equipment for Criticality Accidents*.
- [12] *Nuclear Industry Safety Directors' Forum, The UK Nuclear Industry Good Practice Guide to Criticality Detection at UK Nuclear Licenced Sites, October 2017*.
- [13] *NS-TAST-GD-003, Revision 8, Safety Systems, December 2018*.
- [14] *NS-TAST-GD-031, Revision 5, Safety Related Systems & Instrumentation, September 2018*.
- [15] *Design Criteria and Principles for Criticality Detection and Alarm Systems, SRD R 309, H J Delafield and J J Clifton, October 1984*.
- [16] *Protection of On-Site Personnel in the Event of a Radiation Accident, Documents of the NRPB, Volume 16, No 1, 2005*.
- [17] *Further Guidance on the Protection of On-Site Personnel in the Event of a Radiation Accident, RPD-EA-9-2007, September 2007*.
- [18] *“Oh No It Isn’t!”, “Oh Yes It Is!”, The Omission of Criticality Incident Detection Systems in the UK, P R Thorne, R L Bowden and J Venner, Proceedings of ICNC 2003*.
- [19] *NS-TAST-GD-005, Revision 9, Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), March 2018*.
- [20] *Process Criticality Accident Likelihoods, Consequences, And Emergency Planning, T P McLaughlin, International Conference on Nuclear Criticality Safety, 1991, Los Alamos report: LA-UR- 91-2325, DE91 016030*.
- [21] *A Review of Criticality Accidents 2000 Revision, LA-13638, T P McLaughlin et al, Los Alamos National laboratory*.