Office for Nuclear Regulation

Safety of Lifting Operations

Sellafield Ltd Approach to Applying Crane Category Management

Project Assessment Report ONR-SDFW-PAR-19-027
Revision 0
10 May 2021

Published 08/21

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.

EXECUTIVE SUMMARY

Sellafield Limited Approach to Applying Crane Category Management

This report presents the findings of ONR's assessment of the design of the Sellafield Ltd Standard Crane (SLSC) and the generic safety case for out-of-cell building crane lifting operations.

Request for Regulatory Advice

Sellafield Ltd has requested ONR's regulatory advice and guidance to enable the deployment of the SLSC design and generic approach on future projects.

Sellafield Ltd will require several (up to 30) new out-of-cell building cranes to support its mission over the next decade.

Sellafield Ltd has established an approach known as 'category management' to ensure standardisation of key assets. Sellafield Ltd intends to apply this approach to out-of-cell building cranes. Sellafield Ltd has developed a generic 'high integrity' crane called the Sellafield Ltd Standard Crane (SLSC) which it considers is adequate for any high-hazard lifting application on the Sellafield site in the future. Sellafield Ltd also aims to standardise its safety cases for lifting operations and has developed a generic safety case for this purpose using the SLSC.

ONR's assessment of Sellafield Ltd's crane category management approach will ensure that future safety cases developed under this approach have the greatest chance of being adequate at the time of permissioning and deliver the desired standard of safety proportionate to the nature of the lifting operations. Sellafield Ltd has previously used a generic safety case approach for construction (mobile) cranes, giving operational experience of this type of approach.

Assessment and inspection work carried out by ONR in consideration of this request

Following initial consideration of the licensee's proposed approach and the potential for this to be applied to nuclear lifting operations, I judged it proportionate to obtain specialist inspector advice on the design of the SLS crane and generic safety case. I therefore sought advice from fault studies, conventional health and safety, mechanical engineering, and control and instrumentation specialist inspectors. Following an initial engagement with the licensee, the Human Factors specialist advised that human factors considerations are likely to be facility specific so it would not be proportionate to assess the generic case from a human factors perspective.

I judged it proportionate to consider the following aspects:

- Does the design of the SLSC meet legal requirements and relevant good practice for a crane used in nuclear lifting operations?
- Does the presentation of the licensee's generic safety case support the adoption and implementation into a facility's safety case in order to demonstrate risks are reduced so far as is reasonably practicable?
- Does the licensee's crane selection process result in a fit-for-purpose crane selection for each application?

Matters arising from ONR's work

The ONR inspectors identified several items of regulatory advice for Sellafield Ltd to consider as part of its future development of the SLSC and generic safety case.

Conclusions

Based on the evidence sampled, I conclude that:

- There are suitable safety measures to protect against overload and uncontrolled lower fault conditions on the SLSC.
- The mechanical structures, systems, and components have been designed to appropriate codes and standards to ensure the SLS crane has adequate strength for the proposed use.
- Detailed design of the control and instrumentation systems on the SLSC is incomplete. ONR has provided regulatory advice to enable Sellafield Ltd to address potential issues with the control system design.
- Sellafield Ltd has not yet demonstrated that conventional health and safety aspects have been adequately considered at the design stage. This is currently a shortfall which Sellafield Ltd needs to address as part of its future development work.

I conclude that once Sellafield Ltd has completed its future design and substantiation work, the SLSC is likely to meet legal requirements and relevant good practice for a crane used in nuclear lifting operations. This will be subject to further regulatory review to confirm this.

I conclude that Sellafield Ltd has undertaken a suitable fault identification and analysis process, and identified safety measures to ensure that both the likelihood and consequence of a fault leading to radiological release are reduced so far as is reasonably practicable for generic faults. I am satisfied that appropriate safety functions have been identified for the primary protective measures. I conclude that the generic safety case provides an adequate framework to identify and assess ‘facility-specific’ faults.

Sellafield Ltd’s generic safety case is judged to be inconsistent in the claims on ‘high confidence’ barriers and the approach to engineering substantiation for these. This is a shortfall which will need to be addressed by the licensee as part of its future design and substantiation work and facility specific implementation of the safety case.

Similarly, I consider that Sellafield Ltd’s approach to identification of nuclear safety measures for lifting operations should not restrict safety measure ‘designation’ to its ‘very high confidence’ barriers only. To meet ONR expectations under Licence Conditions 23 (operating rules) and 27 (safety mechanisms, devices and circuits), I consider the licensee should refine its approach to safety measure ‘designation’ taking into consideration risk and consequence for the particular facility/operation under consideration.

While I have identified shortfalls in Sellafield Ltd’s generic safety case approach, I am satisfied that these can be resolved as part of facility specific implementation and do not fundamentally undermine the generic safety case. I am also satisfied that opportunities to reduce risk through the crane design have not been foreclosed at this stage.

Overall, the presentation of Sellafield Ltd’s generic safety case for lifting operations using the SLSC, supports the adoption and implementation of this case into the safety cases of other facilities across the Sellafield site. I am satisfied that Sellafield Ltd has demonstrated that in doing this, risks will be reduced so far as is reasonably practicable.

I conclude that Sellafield Ltd's crane selection process adequately takes account of nuclear safety considerations. For nuclear lifting operations, the licensee will generally select the SLS crane. Where they propose to use a manufacturer's standard crane rather than the SLSC their own arrangements require this choice to be formally recorded and justified.

ONR's assessment as reported here does not preclude further regulatory assessment of Sellafield Ltd's crane selection for particular projects to support future permissioning decisions.

Recommendation

Recommendation: ONR to raise a regulatory issue for Sellafield Ltd to review and update its future work plan for the generic crane design and safety case, taking account of the regulatory advice in Appendix 1 to this report.

LIST OF ABBREVIATIONS

ALARP	As low as reasonably practicable
CCM	Crane Category Management
C&I	Control & Instrumentation
COTS	Commercial Off the Shelf
CT	Cross Travel
DSEAR	Dangerous Substances and Explosive Atmospheres Regulations 2002
EOTC	Electric Overhead Traveling Crane
LOLER	Lifting Operations and Lifting Equipment Regulations 1998
LT	Long Travel
ONR	Office for Nuclear Regulation
PLC	Programmable Logic Controller
RGP	Relevant Good Practice
SAA	Severe Accident Analysis
SAP	Safety Assessment Principle(s)
SFAIRP	So far as is reasonably practicable
SLSC	Sellafield Limited Standard Crane
SSC	Structure, System and Component(s)
STO	Safe Torque Off (variable speed drive function)
TAG	Technical Assessment Guide (ONR)
ULSS	Ultimate Limit Switch System
VSD	Variable Speed Drive

TABLE OF CONTENTS

Appendix

1 REQUEST FOR REGULATORY ADVICE

1. Sellafield Ltd has requested (Ref. 9) ONR's regulatory advice and guidance to enable the deployment of the Sellafield td Standard Crane (SLSC) design and generic approach on future projects.

2 BACKGROUND

2. Sellafield Ltd will require several (up to 30) new out-of-cell building cranes to support its mission over the next 10 years.

3. Sellafield Ltd has established an approach known as 'category management' to ensure standardisation of key assets. The licensee intends to apply this approach to out-cell building cranes. SL has developed a generic 'high integrity' crane called the Sellafield Standard crane (SLSC) which it considers is adequate for any high-hazard lifting application in the future. Sellafield Ltd also aims to standardise its safety cases for lifting operations and has developed a generic safety case for using the SLS crane.

4. ONR's assessment of the crane category management approach will ensure that future safety cases developed under this approach have the greatest chance of being adequate at the time of permissioning and deliver the desired standard of safety proportionate to the nature of the lifting operations. Sellafield Ltd has previously used a generic safety case approach for construction (mobile) cranes, giving operational experience of this type of approach for both ONR and Sellafield.

5. Sellafield Ltd has submitted two key documents to ONR (Ref. 9):

- RP/Des-Cap/PROJ/00037/B. Generic Integrated Safety Case for out-cell building crane lifting operations.
- RP/Des-Cap/PROJ/00039/B. The generic approach for out cell building crane lifting operations -what, why and how to implement it.

Sellafield Ltd Standard Crane (SLSC)

6. The SLSC design is an electric overhead travelling crane (EOTC), which is an evolution on the licensee's previous designs. Sellafield Ltd has specified a number of engineering features intended to reduce risk from fault conditions and equipment failures. These new features include:

- A hoist-drive motor-follower system (Motorsuiveur™ unit) to protect against over-speed and uncontrolled lowering faults, independent of the control system.
- A hoist-drive torque limiter to provide protection against overload and over-raise, independent of the control system and for some fault conditions, which is diverse to the electronic load-cell based overload protection system.
- An advanced Programmable Logic Control (PLC) system working in tandem with linear motion encoders to actively monitor the status of the crane during normal operation. In the event of an error being detected, the PLC system initiates a safe-stop command before any demand is placed on the protection systems.
- Principal control system motion limiting devices backed-up by hard-wired ultimate motion limiting devices which are independent of the control system.
- Hoist-drive by closed-loop direct torque control variable speed drive (VSD).

Generic Lifting Safety Case

7. Sellafield Ltd has developed a generic safety case approach for lifting operations using the SLSC.

8. Sellafield Ltd's primary hazard management strategy is to maintain the integrity of the load path and to ensure that the load remains attached, secure and controlled at all times. For lifting operations involving nuclear or chemotoxic inventories, the licensee's hazard management strategy includes maintaining containment and shielding of the hazardous inventory in the event of credible impacts through provision of designed packages and structures. Aspects such as ledged loads, suspended loads and recovery in relation to these hazards are considered within the licensee's approach as facility specific faults.

9. For lifting operations using the SLSC, Sellafied Ltd has provided a generic safety case covering crane design, operation, and maintenance. The approach includes guidance on how to develop this into a facility specific safety case, including consideration of the lifting philosophy, building design, fault tolerance and risk and any further reasonably practicable improvements.

10. Sellafield Ltd stated that a human factors review of its out-of-cell lifting operations arrangements is currently outstanding and will be completed prior to implementation of the first SLSC safety case. ONR will track this through regulatory oversight of Sellafield Ltd's future work plan.

3 ASSESSMENT AND INSPECTION WORK CARRIED OUT BY ONR IN CONSIDERATION OF THIS REQUEST

11. ONR's assessment was initiated via a preliminary meeting with the Sellafield Ltd project team (Ref. 10).

12. I judged it proportionate to obtain ONR specialist safety inspector advice from the following specialist areas:

- Fault studies (Ref. 15)
- Mechanical engineering (Ref. 11)
- Control and instrumentation (Ref. 12)
- Conventional health and safety (Ref. 14).

13. The ONR specialist inspectors considered the following aspects:

- Does the design of the SLSC meet legal requirements and relevant good practice for a crane used in nuclear lifting operations?

- Does the presentation of Sellafield Ltd's generic safety case support the adoption and implementation into a facility's safety case in order to demonstrate risks are reduced so far as is reasonably practicable?

- Does Sellafield Ltd's crane selection process result in a fit-for-purpose crane selection for each application?

4 MATTERS ARISING FROM ONR'S WORK

4.1 FAULT STUDIES

14. The fault studies assessment focussed on whether the licensee has undertaken suitable analysis to give confidence that the SLSC as designed, and once installed, will be able to operate safely and meet regulatory expectations.

15. The fault studies inspector sampled the licensee's safety case to inform their judgement as to whether the licensee has performed a comprehensive fault identification and analysis process, identified suitable and sufficient safety measures and appropriately classified these measures, and considered the defence in depth principles and the resilience of the facility to potential faults.

16. The fault studies specialist concludes that:

17. Sellafield Ltd has undertaken a suitable fault identification and analysis process in line with the expectations of ONR's Safety Assessment Principles (SAPs). Regulatory observations in relation to the identification of internal hazards and fire have been captured in Appendix 1 as regulatory advice to Sellafield Ltd.

18. Sellafield Ltd has identified safety measures to ensure that both the likelihood and consequence of a fault leading to radiological consequence are reduced to ALARP in line with ONR SAPs for generic faults. Appropriate safety functions have been identified for the primary protective measures. Regulatory observations have been captured in Appendix 1 as regulatory advice to Sellafield Ltd in relation to:

- Identification of conditions and limits to support key claims made in the safety case;
- The classification of equipment for defence in depth;
- Formal capture of independence claims;
- Identification of normal operations safety functions;
- Approach to evaluating numerical risk.

19. Sellafield Ltd has provided an adequate framework to identify and assess facility-specific faults but has not provided a conclusion on the risks associated with these faults. Such a judgement would need to be made upon consideration of the facility-specific safety analysis.

20. The safety case presents the analysis for fault conditions generic to the SLSC, regardless of operating facility. For fault conditions specific to the operating facility a framework has been provided to enable the fault conditions to be analysed in the facility-specific safety case. Based on the fault conditions sampled, the fault studies inspector concluded that the framework for considering facility specific faults is adequate.

21. Overall, the fault studies specialist inspector is satisfied that Sellafield Ltd has undertaken a suitable analysis of the generic aspects of the SLSC; this includes fault identification and analysis and identification of safety measures. Furthermore, Sellafield Ltd has provided an adequate framework to enable fault conditions to be analysed in the facility-specific case.

22. The fault studies inspector judges that solutions to their observations and recommendations can be developed by Sellafield Ltd to an adequate level to be incorporated into an adequate safety case.

4.2 MECHANICAL ENGINEERING

23. The mechanical engineering assessment considered the design of the SLSC and the suitability of protection measures against the generic faults identified within the safety case. The mechanical engineering inspector concluded that the standard crane specification incorporates suitable protection measures against the identified generic faults, so far as is reasonably practicable.

24. The inspector noted that Sellafield Ltd has identified a generic Examination, Inspection, Maintenance and Testing regime for the SLSC. The licensee plans to

develop a generic Technical Basis of Maintenance, which can be further developed on a per-facility basis. This is identified within Sellafield Ltd's future work plan and may be subject to further regulatory review to confirm the adequacy.

25. Sellafield Ltd has performed a gap analysis, concluding British Standard 2573 parts 1 and 2 are more conservative than the harmonised european standards (EN13001 and 15011 series) demonstrating that suitable codes and standards have been adopted for the design of the SLSC. The mechanical engineering inspector concluded that this provides a robust basis for Sellafield Ltd's crane procurement strategy for the next 15 years.

26. The mechanical engineering specialist inspector is content that Sellafield Ltd has identified relevant good practice and implemented relevant sources of learning from experience for crane lifting operations to support the development of the SLSC specification. The inspector advised that Sellafield Ltd should consider the requirement for periodic review of relevant good practice relating to the SLSC design.

27. The inspector identified three pieces of regulatory advice for Sellafield Ltd to consider prior to installation and commissioning of the first SLSC. This advice covers ONR expectations for development of the technical basis of maintenance, periodic review of relevant good practice and lifetime quality records. This advice is included in Appendix 1.

28. Overall, the mechanical engineering inspector is satisfied with the claims, arguments and evidence presented by Sellafield Ltd in the generic safety case and identified no significant shortfalls identified in the delivery of safety functions.

28.1 CONTROL AND INSTRUMENTATION

29. Due to the unavailability of a detailed Control & Instrumentation (C&I) design, the C&I inspector assessment was restricted to a consideration of the high-level descriptions of the claims arguments and evidence relating to the crane's protection against generic fault conditions. The C&I inspector was unable to conclusively judge the adequacy of C&I aspects of the crane's resilience to these fault conditions due to some key evidence being outstanding. Nevertheless, for a sample of generic fault conditions the C&I inspector explored whether the claimed deterministic resistance could be undermined by credible C&I failures, and whether protective barriers with C&I dependencies could be expected to achieve their claimed performance and independence.

30. The C&I inspector made several recommendations covering areas where Sellafield Ltd should produce further evidence to demonstrate that:

- The C&I systems support Sellafield Ltd's claim that the SLSC is deterministically safe under certain fault conditions.
- C&I systems provide defence-in depth against particular fault conditions where this is claimed by Sellafield Ltd.
- Supplementary protective barriers against particular generic fault conditions are independent from other barriers and the fault initiator, and that their design and substantiation can demonstrably support their performance claims.
- Sellafield Ltd has obtained the evidence necessary to demonstrate that it has verified/substantiated the deterministic capability of a motor follower protective barrier from a C&I perspective.

31. These recommendations are included in Appendix 1 as regulatory advice to Sellafield Ltd.

32. Some of the C&I inspector's recommendations highlight an inconsistency between Sellafield Ltd's proposal that C&I barriers of protection against generic fault conditions will not require formal designation, classification and substantiation. Also, that Sellafield Ltd's claim that 'high confidence' barriers, which include C&I barriers, have effectively been substantiated to the desired confidence levels required by any future project. This inconsistency is also reflected in the generic safety case presenting minimal evidence that C&I aspects of 'high confidence' barriers have been, or will be, substantiated to the corresponding standard of a safety function class 2 system under Sellafield Ltd's Nuclear Categorisation Scheme.

33. The inspector recognises that Sellafield Ltd has opportunities to improve the generic safety case and design prior to the first use of the SLSC and noted the following points:

- Sellafield Ltd's crane category management (CCM) arrangements demonstrate that the approach is intended to deliver cranes that meet legal requirements and established relevant good practice (RGP) for conventional lifting operations (e.g. compliance with harmonised standards and Sellafield Ltd's implementations), and that for the SLSC these will be supplemented by additional requirements to support nuclear lifting operations. The C&I inspector is content with the overall approach described within the licensee's arrangements.

- Sellafield Ltd recognises (via outstanding issues) the significance of some of the pending C&I evidence.

- Sellafield Ltd's proposals for future development of the CCM generic approach include a commitment to consider the advice and recommendations arising out of ONR's assessment and to engage with ONR as necessary.

34. Overall, the C&I inspector judged that Sellafield Ltd's arrangements can deliver cranes that meet legal requirements for conventional lifting operations. For nuclear/high hazard lifting operations, the licensee needs to provide further evidence to demonstrate that the C&I systems can fulfil their safety functions to the claimed level of confidence. The C&I specialist provided advice to Sellafield Ltd on ONR's expectations.

4.3 CONVENTIONAL HEALTH AND SAFETY

35. The Conventional Health and Safety (CHS) specialist inspector considered the adequacy of Sellafield Ltd's approach to compliance with the relevant health and safety legislation in relation to the design and operation of the SLSC.

36. The CHS specialist advised (Ref. 14) that Sellafield Ltd has not yet produced an adequate risk assessment to demonstrate that the crane design allows for effective and safe installation, operation, maintenance and decommissioning. Sellafield Ltd intends provide this information as part of its future development work (Ref. 13). In my judgment, this is unlikely to impact on the design of nuclear safety structures, systems and components (SSCs).

37. Regarding the Dangerous Substance and Explosive Atmospheres Regulations 2002 (DSEAR) it is foreseeable that cranes may be located in areas on the Sellafield site where an explosive atmosphere could or does occur and would be zoned under the regulations accordingly. The CHS specialist advised that the licensee should

generically assess this risk at the design stage to either confirm that the crane will not be used within an explosive atmosphere as defined, or it can be modified to ensure it is suitable to operate in such an area.

38. I have included these points as regulatory advice to SL in Appendix 1.

5 CONCLUSIONS

39. Based on the evidence sampled, I conclude that:

- There are suitable safety measures to protect against overload and uncontrolled lower fault conditions on the SLSC.
- The mechanical structures, systems, and components have been designed to appropriate codes and standards to ensure adequate strength for the proposed use.
- Detailed design of the control and instrumentation systems on the SLSC is incomplete. ONR has provided regulatory advice for Sellafield Ltd to address potential issues with the control system design.
- SL has not yet demonstrated that conventional health and safety aspects have been adequately considered at the design stage. This is currently a shortfall which Sellafield Ltd needs to address as part of its future development work.

40. I conclude that once Sellafield Ltd has completed its future detailed design and substantiation work, the SLSC is likely to meet legal requirements and relevant good practice for a crane used in nuclear lifting operations. This will be subject to further regulatory review to confirm this.

41. I conclude that Sellafield Ltd has undertaken a suitable fault identification and analysis process, and identified safety measures to ensure that both the likelihood and consequence of a fault leading to radiological release are reduced so far as is reasonably practicable for generic faults. I am satisfied that appropriate safety functions have been identified for the primary protective measures. I conclude that the generic safety case provides an adequate framework to identify and assess 'facility-specific' faults.

42. Sellafield Ltd's generic safety case is judged to be inconsistent in the claims on 'high confidence' barriers and the approach to engineering substantiation for these. This is a shortfall that Sellafield Ltd needs to address as part of its future design and substantiation work, and facility specific implementation of the safety case.

43. Similarly, I consider that Sellafield Ltd's approach to identification of nuclear safety measures for lifting operations should not restrict safety measure 'designation' to its 'very high confidence' barriers only. To meet ONR expectations under Licence Conditions 23 (operating rules) and 27 (Safety mechanisms, devices and circuits), I consider that Sellafield Ltd needs to refine its approach to safety measure 'designation' taking into consideration risk and consequence for the particular facility/operation under consideration.

44. While I have identified shortfalls in Sellafield Ltd's generic safety case approach, I am satisfied that these can be resolved as part of facility specific implementation and do not fundamentally undermine the generic safety case. I am also satisfied that opportunities to reduce risk through the crane design have not been foreclosed at this stage.

45. Overall, the presentation of Sellafield Ltd's generic safety case for lifting operations using the SLSC, supports the adoption and implementation of this case into the safety cases of other facilities across the Sellafield site. We are satisfied that Sellafield Ltd has demonstrated that in doing this, risks will be reduced so far as is reasonably practicable.

46. I conclude that Sellafield Ltd's crane selection process adequately takes account of nuclear safety considerations. For nuclear lifting operations, Sellafield Ltd will generally select the SLSC Standard crane. Where they proposes to use a manufacturer's standard crane rather than the SLSC Standard crane then their arrangements require this choice to be formally recorded and justified.

47. ONR's assessment as reported here does not preclude further regulatory assessment of Sellafield Ltd's crane selection for particular projects to support future permissioning decisions.

6 RECOMMENDATIONS

48. The project assessment report recommends:

Recommendation: ONR to raise a regulatory issue for Sellafield Ltd to review and update its future work plan (Ref. 13) for the generic crane design and safety case, taking account of the regulatory advice in Appendix 1.

7 REFERENCES

1. *ONR Guide – The Purpose and Use of Permissioning - NS-PER-GD-001 Revision X*. Month Year. http://www.onr.org.uk/operational/assessment/index.htm

2. *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition, Revision 1. January 2020. http://www.onr.org.uk/saps/saps2014.pdf.

3. ONR Technical Assessment Guides

   Guidance on Mechanics of Assessment NS-TAST-GD-096 Revision. ONR. April 2020

   Nuclear Lifting Operations NS-TAST-GD-056 Revision 7. ONR. October 2018

   External Hazards NS-TAST-GD-013 Revision 8. ONR. October 2018

   Internal Hazards NS-TAST-GD-014 Revision 6. ONR. November 2019

   The purpose, scope and content of nuclear safety cases NS-TAST-GD-051 Revision 6. ONR. December 2019
   http://www.onr.org.uk/operational/tech_asst_guides/index.htm

4. Relevant British, European and International Standards

   BS EN13001-1: 2015 – Cranes - General Design, General Principles and Requirements

   BS EN 13001-2: 2014 – Crane Safety. General Design and Load Actions.

   BS EN 13001-3-1:2012 – Cranes. General Design. Limit States and proof competence of steel structure

   BS 2573-1: Rules for the design of cranes. Specification for classification, stress calculations and design criteria for structures

   BS2573-2: Rules for the design of cranes. Specification for classification, stress calculations and design of mechanisms

   BS EN 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.

   BS EN ISO 12100 - Safety of machinery. General principles for design. Risk assessment and risk reduction.

   BS EN 60204-32 - Safety of machinery. Electrical equipment of machines - Requirements for hoisting machines.

   BS EN 15011 – Cranes – Bridge and gantry cranes.

   BS EN ISO 13849-1:2015 – Safety of machinery. Safety-related parts of control systems – General principles for design.

5. Relevant Legislation

   Lifting Operations and Lifting Equipment Regulations 1998

   Provision and Use of Work Equipment Regulations 1998

   Management of Health and Safety at Work Regulations 1999

Work at Height Regulations 2005

Manual Handling Operations Regulations 1992, as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002

Construction (Design and Management) Regulations 2015

Dangerous Substances and Explosive Atmospheres Regulations 2002

6. Sellafield Limited – S&RM Technical Manual – E2.10 – Specification of Safety Measures.

7. Sellafield Ltd. EG_ 1_2285_1_Issue 2. Design guide for the selection and use of variable speed drives, stepper motors and servo drives in Sellafield Ltd. Plants.

8. Sellafield Ltd, S&RM Technical Manual, D1.11 Guidance on the Production of Radiological and Criticality Fault Assessments Issue 1

9. SL submission of the generic safety case for the Sellafield Limited Standard Crane (SLSC) design (HPCP525) ONR/20/12694/01 dated 26 Aug 2020 (CM9 2020/259978)

10. ONR-SDFW-CR-19-404 - SL Crane Category Management – [redacted] – 21 August 2019 [CM: 2019/244376].

11. ONR-SDFW-AR-20-026 Mechanical Assessment of Sellafield Limited's Approach to Applying Crane Category Management - 01 December 2020 - CM9 2020/294163

12. ONR-SDFW-AR-20-018 Control and Instrumentation Assessment of the Generic Approach for Out-Cell Building Crane Lifting Operations - CM9 2020/239979

13. Future Development of the Generic Approach to Out-Cell Building Crane Lifting Operations Standard Crane (SLSC) design (HPCP525). (CM9 2020/259978)

14. Crane Category Management – ONR Conventional Safety Queries (CM9 2021/12352)

15. ONR-SDFW-AR-20-22 Fault Analysis Assessment of Sellafield Limited Approach to Applying Crane Category Management (CM9 2020/251252)

Appendix 1
Regulatory Advice to SL

Number	Advice to SL
C&I 01	With reference to the fault condition of "*crane skewing leading to derailment and crane collapse*", Sellafield Ltd should clearly articulate in the safety case why the deterministic resistance to crane skewing places no dependency on the SLSC control system. Sellafield Ltd should also consider how, in accordance with defence-in-depth principles, the SLSC control system could be used to prevent and/or indicate potentially damaging increases in skew loading.
C&I 02	With reference to the fault condition of "*locked load (during Long Travel/Cross Travel) leading to crane collapse*", Sellafield Ltd should consider how, in accordance with defence-in-depth principles, the SLSC control system could provide early indication/ prevention of the undesirable situation of the fault condition progressing such that it causes wheel slippage to occur and/or continue unrevealed. If this additional protection is already provided, then Sellafield Ltd should clearly articulate this in the safety case. Sellafield Ltd should also amend the safety case to clarify the basis for why ultimate deterministic protection via wheel slippage places no dependency on correct configuration/ operation of the Variable Speed Drives (VSDs).
C&I 03	Sellafield Ltd should provide ONR with the evidence it proposes to obtain for Outstanding Issue 2.a (Ref. 6), which is required to support the claim of independence between the Ultimate Limit Switch System (ULSSs) and the SLSC control system.
C&I 04	Noting the fault studies' recommendation to not restrict nuclear safety designation and safety function classification to 'very high confidence' deterministic barriers, the safety case should include suitable documented substantiation of C&I barriers that could potentially require a designation/classification, including those that are currently assigned as 'high confidence' barriers.
C&I 05	Sellafield Ltd should clarify/justify the extent of independence between barriers associated with the ULSSs and the emergency stop system, particularly in relation to whether their final switching elements are a potential common point of failure; noting that Sellafield Ltd has referred to both systems delivering a BS EN 60204 1 'stop category 0' function to stop motion by immediate removal of power from the machine actuators.
C&I 06	With reference to the fault condition of "*hoist over-lower*", Sellafield Ltd should ensure that a 'high confidence' claim for barrier 1 (i.e. the way in which crane operations are undertaken and refers to activating an emergency stop if necessary) can be supported by all aspects of the barrier, including the C&I implementation of the emergency stop function which should be designed and substantiated accordingly.
C&I 07	Sellafield Ltd should provide ONR with the evidence it proposes to obtain for Outstanding Issue 2.c (Ref. 6), which is required to provide a very high degree of confidence that the Long Travel/Cross Travel (LT/CT) end-stops and buffers can withstand the worst credible VSD over-speed condition and thereby deterministically prevent crane over-travel. In particular, and noting that the LT/CT axes do not have

	independent (of the SLSC control system) over-speed protection, Sellafield Ltd should justify the selection and acceptability of 160% over-speed as a worst case scenario and clarify the arrangements for addressing potential inadequacy of the end stop withstand capability calculations as a generic case for all flask handling installations across the Sellafield site.
C&I 08	Sellafield Ltd should consider whether applications of the SLSC could potentially require the LT/CT axes to have independent (of the SLSC control system) over-speed protection, which should consider the wider effects of over-speed/acceleration on load swing, control, stability, etc. and not just implications for end-stop protection capability. This should consider the adequacy of any over-speed protection within the PLC/VSD motion control system, including its integrity and whether it can terminate an over-speed fault independently of the initiator; noting also that Sellafield Ltd's arrangements (E2.10 and ES_1_2285_1) restrict claims on complex/ programmable electronic devices to ≤ 0.5 failure per annum unless a "smart instrument assessment" has been performed. (The level of confidence in this over-speed protection should also influence Sellafield Ltd's judgement on the adequacy of the end-stops' 160% over-speed rating in a combined over-travel/ over-speed fault situation – i.e. C&I 07)
C&I 09	Sellafield Ltd should provide ONR with the evidence it proposes to obtain for Outstanding Issue 2.b (Ref. 6) to support the argument that the motor follower system provides deterministically safe protection against an uncontrolled lower fault condition (i.e. demonstrate to a very high degree of confidence that the system has no credible unrevealed dangerous failure modes which could prevent delivery of the safety function). From a C&I perspective, this should provide objective evidence (i.e. including empirical/design data) to support the argument that the deterministic safety capability cannot be undermined by a servo drive misconfiguration or malfunction (including from any interface with the wider SLSC control system) and should also clarify the significance of the supply voltage value in this regard.
C&I 10	With reference to the fault condition of "*hoist uncontrolled lower*", Sellafield Ltd should address the potential inconsistency between the 'high confidence' claim for the load path (barrier 2) and its reliance on the VSD's control of the service brake (i.e. co-ordinates brake application with motor torque) and consider the adequacy of overall protection in light of any resulting changes; noting that Sellafield Ltd's arrangements (E2.10 and ES_1_2285_1) restrict claims on complex/ programmable electronic devices to ≥ 0.5 failure per annum unless a "smart instrument assessment" has been performed. The VSD brake control also makes a further contribution to load path integrity through its use in the control interlock that protects against torque limiter slippage failure, which will also need to be considered.
C&I 11	As the SLSC advanced control systems utilises complex motion control technology (e.g. PLC/VSD motion control), Sellafield Ltd should evaluate the adequacy of the technological means of maintaining standstill (e.g. BS EN 60204 32 stop categories) when an operator might not be fully attending to the crane.
C&I 12	Noting that the ULSS barriers for the generic fault conditions are 'high confidence' barriers that utilise a VSD Safe Torque Off (STO) module to stop motion independently of the SLSC control system, then on the

	basis that the safety case states that generic SSCs with very high confidence and high confidence claims have "*effectively been substantiated to the highest confidence levels that could be required by any project in future*", and Sellafield Ltd's arrangements (E2.10 and ES_1_2285_1) restrict claims on complex/ programmable electronic devices to ≤ 0.5 failure per annum unless a "smart instrument assessment" has been performed, Sellafield Ltd should resolve the inconsistency in its proposal to not undertake further substantiation work on the VSD STO module by providing an adequate nuclear safety substantiation or revising and justifying its claims accordingly.
ME 01	Prior to commissioning the first SLSC, Sellafield Ltd should produce an adequate generic Technical Basis of Maintenance for nuclear lifting arrangements; demonstrating the licensee has adequate oversight of Examination, Inspection, Maintenance and Testing activities.
ME 02	Prior to commissioning the first SLSC, Sellafield Ltd should demonstrate it has adequate arrangements for periodically reviewing relevant good practice and legal requirements relating to the SLSC design.
ME 03	Prior to installation of the first SLSC, Sellafield Ltd should produce the required life-time records and confirm they are adequate for equipment qualification and quality assurance purposes.
CHS 01	Prior to installation of the first SLSC, Sellafield Ltd should carry out a risk assessment to meet the requirements of Regulation 3 (1) of the Management of Health and Safety at Work Regulations 1999. The risk assessment should demonstrate that the crane design allows for effective and safe installation, operation, maintenance and decommissioning. This risk assessment should also cover the requirements of other relevant regulations: • Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) • Provision and Use of Work Equipment Regulations 1998 • Management of Health and Safety at Work Regulations 1999 • Work at Height Regulations 2005 • Manual Handling Operations Regulations 1992, as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002 • Construction (Design and Management) Regulations 2015 • Dangerous Substances and Explosive Atmospheres Regulations 2002
CHS 02	Regarding the Dangerous Substance and Explosive Atmospheres Regulations 2002 (DSEAR) it is foreseeable that cranes may be located in areas on the Sellafield site where an explosive atmosphere could or does occur and would be zoned under the regulations accordingly. Sellafield Ltd should generically assess this risk at the design stage to either confirm that the crane will not be used within an explosive atmosphere as defined or can be modified to ensure it is suitable to operate in such an area.

FS 01	Sellafield Ltd's arrangements should include a prompt for facility-specific consideration of accidents associated with failure of design basis provisions for out-cell building crane lifting operations, to establish whether there may be potential for consequences exceeding severe accident criteria. Explanatory Note: ONR's expectations for Severe Accident Analysis are proportionate to the hazard and will depend on the facility, the lift and the potential consequences. This recommendation is made to include a prompt within the generic approach to ensure that out-cell building crane operations are considered by Sellafield Ltd's severe accident management arrangements when appropriate.
FS 02	Sellafield Ltd should include a fire initiated on the SLSC within the generic integrated safety case and demonstrate the features of the SLSC that protect against fire.
FS 03	In order to underpin and provide clarity to the claims on load path integrity and inform examination, maintenance and testing expectations, Sellafield Ltd should define which structures, systems and components make up the crane load path under the defined normal operating conditions and fault conditions (including those conditions where a deterministic claim is made; for example locked load during long/cross travel).
FS 04	Where claims made in the generic safety case rely on an assumed condition or limit being met, these should be considered for formal identification as conditions/limits in the safety case. While conditions and limits are likely to be plant-specific, the SLSC safety case should be clear in its expectations for derivation of both operational/administrative and engineering conditions and limits when applied to a specific facility.
FS 05	Sellafield Ltd's approach to identification of nuclear safety measures for lifting operations should not restrict safety measure 'designation' to its 'very high confidence' barriers only. The generic approach should facilitate the consideration of defence in depth for nuclear lifts, and evaluation of the number and adequacy of safety measures in a graded manner taking into consideration risk and consequence for the particular facility/operation under consideration to give an overall balanced design and operating philosophy. In evaluating safety measures for defence in depth, consideration should also be given to single point vulnerabilities in the identified protection (for example, errors in setup/maintenance of equipment)
FS 06	Sellafield Ltd should consider the divergence between their guidance on barrier analysis outlined in S&RM Technical Manual D1.11 and the barrier analysis approach applied in the generic integrated safety case for out-cell crane operations.
FS 07	Sellafield Ltd should formally capture key claims around independence of the over-raise limit from the control system (detection, decision making and termination) within the safety function design requirements for the system.
FS 08	Sellafield Ltd should include guidance to minimise by design and assess the impact of internal hazards and fire arising within the facility

	for the development of the lifting strategy and facility-specific crane case.
FS 09	Sellafield Ltd should clearly articulate within the generic integrated safety case or supporting guidance how safety functions for normal operations are incorporated and how the approach complies with their arrangements for identifying normal safety functions, particularly where a “high confidence” or greater claim is placed upon that function.
FS 10	Sellafield Ltd should provide guidance to outline how numerical risk should be evaluated when applying the crane category management approach to a specific facility, for both generic and facility specific hazards/risks. This should include discussion of the significance of extant reliability data within the context of application to the SLSC .
FS 11	When assessing facility-specific Safety Cases implementing the SLSC , ONR should consider the totality of the facility-specific lifting case, including the facility design, lifting attachments, loads and operational practices, when considering the demonstration that risks from faults associated with the SLSC are ALARP. A graded approach to identification of appropriate safety measures reflecting the principles of defence in depth is expected. Explanatory Note: This is a matter which ONR inspectors may consider as part of future permissioning activities. It is shared with Sellafield Ltd for guidance on ONR expectations.
FS 12	ONR should consider the closure statements against Outstanding Issue 2 of the generic integrated safety case to confirm that the basis of ONR’s assessment for the SLSC remains valid. Explanatory Note: This is a matter which ONR inspectors may consider as part of future permissioning activities. It is shared with Sellafield Ltd for guidance on ONR expectations.