

KUALA LUMPUR UNIVERSITY
OF SCIENCE AND TECHNOLOGY
吉隆坡科技大学

CSC 2303-REQUIREMENTS ENGINEERING
SEPTEMPER 2026

Nuclear Power Plant Group Project

NAME	**1: Mohamed Elsadig** **2: Ismail Abdirisaq Abdiqani** **3: Bin Ahmed Mohamed**
MATRIC NO.	**1:** **2:** **3:**
DATE	**14/08/2026**

A. Stakeholder Identification

A nuclear power plant has many stakeholders because the plant is connected to safety, electricity production, maintenance, and government regulations. Some stakeholders work directly with the plant, while others are mainly concerned about its effects and safety.

1. Plant Operators

Plant operators are direct users of the system. They are mainly concerned with operating the plant safely and knowing what is happening inside the plant. They monitor the plant systems and respond to alarms and unusual situations. They need information such as temperature, pressure, reactor status, equipment status, and alarms. Their influence is High because they use the system during normal operation and may need it during an emergency.

Possible requirements:

- The system should show important information in real time.
- Alarms should be clear and easy to notice.
- Operators should be able to see abnormal conditions quickly.

2. Plant Management

Management is responsible for the overall operation of the plant. Their main interests are safety, production, costs, and the general performance of the plant. They need reports about production, maintenance, safety incidents, and system performance. Their influence is High because they make and approve important decisions.

Possible requirements:

- The system should provide performance reports.
- Management should be able to access important safety information.
- Major incidents should be recorded.

3. Nuclear Regulatory Authority

The regulatory authority checks whether the nuclear power plant follows safety regulations and legal requirements. Its main interest is nuclear safety and protecting people and the environment. It may need access to safety reports, inspection results, incident records, and other relevant information. This stakeholder has Very High influence because the plant has to follow its regulations.

Possible requirements:

- Safety records should be accurate.
- The system should keep records needed for inspections.
- Incidents should be properly recorded and reported.

4. Maintenance Engineers

Maintenance engineers work with the equipment and systems in the plant. They are interested in keeping equipment reliable and finding problems early. They inspect equipment, perform repairs, and carry out planned maintenance. They need equipment status, fault information, maintenance history, and maintenance schedules. Their influence is Medium to High.

Possible requirements:

- The system should keep maintenance history.
- Equipment faults should be shown to maintenance staff.
- The system should give maintenance alerts when needed.

5. Safety Engineers

Safety engineers are mainly concerned with reducing risks and preventing accidents. They check safety systems, study possible hazards, and help improve safety procedures. They need information about alarms, safety systems, abnormal conditions, and previous incidents. Their influence is High because safety requirements are important for the whole project.

Possible requirements:

- The system should identify abnormal conditions.
- Safety alarms should work reliably.
- Safety-related events should be recorded.

6. Emergency Response Team

This team becomes especially important when there is an emergency at the plant. Their main concern is getting the correct information quickly so they can respond properly. They may need information about the location of the problem, affected equipment, plant status, alarms, and emergency procedures. Their influence is High during emergency situations.

Possible requirements:

- Emergency alarms should be provided quickly.
- Important plant information should be available during an emergency.
- The system should support emergency procedures.

7. Local Community

People living around the plant are also stakeholders. They are not users of the technical system, but a serious problem at the plant could affect them. Their main interests are public safety, environmental protection, and receiving correct information during a serious incident. Their influence is Medium. They do not control the technical system, but their concerns about safety should still be considered.

Possible requirements:

- Emergency information should be communicated clearly.
- Public safety information should be available when necessary.
- Environmental information should be properly recorded.

8. IT and System Administrators

IT administrators are responsible for the computer systems, networks, user accounts, and other technical parts of the system. They are concerned about cybersecurity, system availability, data protection, and system performance. They need information about system errors, access records, network problems, and security events. Their influence is Medium to High because they maintain the technical infrastructure.

Possible requirements:

- Users should only access information they are authorized to use.
- Important activities should be recorded in system logs.
- Important data should be backed up.
- Unauthorized access should be prevented.

Stakeholder-Interest Matrix

The stakeholders can be classified according to their influence and interest in the project.

Stakeholder	Influence	Interest
Plant Operators	High	High
Plant Management	High	High
Nuclear Regulatory Authority	Very High	High
Maintenance Engineers	Medium-High	High
Safety Engineers	High	High
Emergency Response Team	High	High
Local Community	Medium	High
IT/System Administrators	Medium-High	High

	High Interest	Low Interest
High Influence	Regulatory Authority, Plant Management, Plant Operators, Safety Engineers, Emergency Response Team	—
Medium Influence	Maintenance Engineers, IT Administrators, Local Community	—
Low Influence	—	—

Most of the stakeholders have high interest because the project is related to nuclear safety. The regulatory authority has the highest influence because the plant must follow its regulations. Plant management and operators also have a strong influence because they are directly involved in plant operation.

B. Requirements Elicitation Techniques

Requirements elicitation is the process of collecting information from stakeholders to understand what the system needs to do. ISO/IEC/IEEE 29148:2018 describes requirements elicitation as part of requirements engineering and includes systematic techniques for identifying and documenting user needs (ISO/IEC/IEEE, 2018).

1. Interviews

Interviews are useful when the requirements engineer needs detailed information from a specific stakeholder.

Purpose: To understand the stakeholder's work, problems, and requirements through direct questions.

Suitable stakeholders: Plant operators, maintenance engineers, safety engineers, managers, and IT administrators.

Advantages:

- Detailed information can be collected.
- The interviewer can ask another question when an answer is unclear.
- Stakeholders can explain their problems in their own words.

Limitations:

- Interviews can take a lot of time.
- Different stakeholders may give different opinions.
- The interviewer can misunderstand an answer.

Expected outputs: Stakeholder needs, possible requirements, problems, and points that need further discussion.

2. Questionnaires

Questionnaires are useful when the project team wants answers from a larger number of people. Purpose: To

collect similar information from many stakeholders using the same questions.

Suitable stakeholders: Operators, technicians, maintenance staff, and other employees. Advantages:

- Many people can be reached.
- Answers are easier to compare.
- It can save time when there are many stakeholders.

Limitations:

- Answers may not give enough detail.
- Some people may skip questions.
- It is not easy to ask follow-up questions.

Expected outputs: Common problems, user needs, opinions, and priorities.

3. Workshops

A workshop is a meeting where several stakeholders discuss the system together.

Purpose: To discuss requirements and reach a common understanding between different stakeholders.

Suitable stakeholders: Management, operators, engineers, safety staff, IT staff, and the requirements team.

Advantages:

- Different opinions can be discussed at the same time.
- Conflicts can be noticed early.
- Several requirements can be discussed in one session.

Limitations:

- It may be difficult to find a suitable time for everyone.
- Some participants may dominate the discussion.
- The meeting can take longer if there are disagreements.

Expected outputs: Agreed requirements, stakeholder concerns, priorities, and conflicts.

4. Observation

Observation means watching users while they perform their normal work. For example, the requirements team could observe how operators monitor plant systems.

Purpose: To understand the real work process and how users interact with existing systems. Suitable

stakeholders: Plant operators, maintenance engineers, and technical staff.

Advantages:

- It shows how the work is actually performed.
- It can find problems that users forget to mention.
- It helps the analyst understand the working environment.

Limitations:

- It can take time.
- People may change their behavior when they know they are being observed.
- Some activities cannot be observed freely because of safety restrictions.

Expected outputs: Work procedures, user activities, system interactions, and possible requirements.

5. Document Analysis

Document analysis means studying existing documents related to the plant. These could include safety procedures, regulations, maintenance records, system manuals, and previous requirements.

Purpose: To find existing requirements, rules, procedures, and technical restrictions.

Suitable stakeholders: Regulatory authority, safety engineers, management, IT administrators, and requirements engineers.

Advantages:

- Existing information can be collected.
- It helps identify important regulations.
- Documents can be compared with information collected from stakeholders.

Limitations:

- Some documents may be outdated.
- Technical documents can be difficult to understand.
- Some stakeholder needs may not be written in the documents.

Expected outputs: Regulatory requirements, safety rules, existing system requirements, procedures, and technical constraints.

C. Best Elicitation Approach

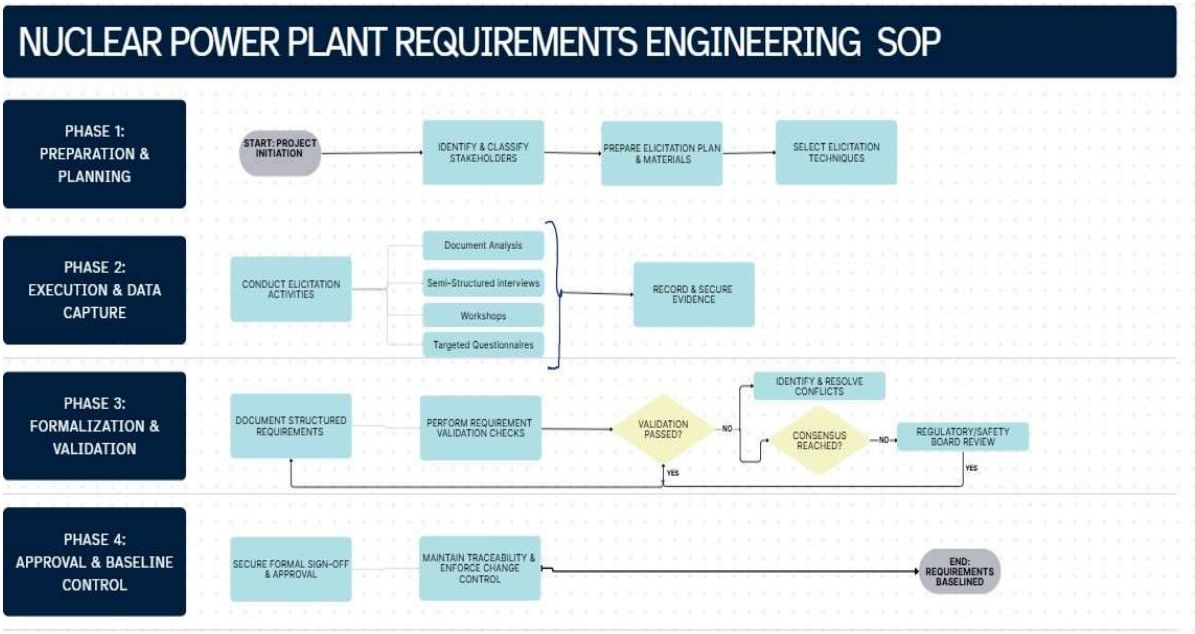
For a safety-critical project like the Republic of the Congo's proposed nuclear power plant, relying on a single elicitation technique creates dangerous blind spots. Our team recommends a hybrid elicitation strategy combining Document Analysis, Semi-Structured Interviews, Workshops, and Targeted Questionnaires. This tailored combination ensures technical rigor, broad engagement, and safety compliance while keeping the process structured and efficient.

Justification of the Selected Strategy

- **Completeness:** Relying on memory or informal chats is risky in nuclear projects. Document Analysis anchors the requirements in established international safety standards, national energy policies, and regulatory guidelines so foundational safety constraints are not overlooked.
- **Accuracy:** Semi-Structured Interviews allow requirements engineers to sit down one-on-one with domain specialists like Plant Operators, Safety Engineers, and Maintenance Engineers. This format gives engineers the flexibility to ask follow-up questions, clarify complex operational routines, and double-check specific alarm thresholds.
- **Stakeholder Coverage:** The hybrid approach engages all levels of authority and operation. Regulators and legal bodies are covered through document analysis. Specialized technical experts are reached via direct interviews. Management and department heads collaborate in workshops. General plant employees and technicians provide broad feedback through structured questionnaires.
- **Safety:** Prioritizing regulatory documentation and safety engineer interviews early establishes strict safety constraints before operational or financial requirements are negotiated. Safety is treated as a mandatory non-negotiable baseline rather than an afterthought.
- **Cost Efficiency:** Running individual interviews for every employee would drain time and resources. Using Questionnaires to gather input from larger staff groups saves substantial person-hours, allowing high-cost interview and workshop slots to focus on critical operational modules.
- **Time Management:** Workshops bring key decision-makers into a single room to discuss operational procedures together. Negotiating requirements in real time eliminates endless email chains and drastically speeds up consensus building.
- **Traceability:** Outputs from these specific techniques, such as interview transcripts, signed workshop summary notes, and annotated regulatory excerpts provide a clear paper trail connecting final requirements to raw stakeholder input.
- **Confidentiality:** Systems involving IT Administrators, network architecture, and nuclear safety protocols require strict discretion. Interviews and Document Analysis allow engineers to discuss cybersecurity controls and sensitive technical setups in secure settings rather than open group forums.

D. Standard Operating Procedure (SOP) for Requirements Collection

The following Standard Operating Procedure (SOP) outlines the step-by-step workflow for identifying, capturing, validating, and managing requirements throughout the project lifecycle.



Step-by-Step SOP Implementation

1. Define Project Scope and Objectives: Establish clear project boundaries, focusing strictly on system monitoring, emergency procedures, regulatory compliance, and software/system requirements engineering rather than nuclear reactor design. Define primary quality goals: system reliability, safety compliance, and operational traceability.

2. Identify and Classify Stakeholders: Map all direct and indirect stakeholders into the Stakeholder-Interest Matrix (e.g., Regulatory Authority, Plant Operators, Safety Engineers, IT Administrators, Local Community). Identify their specific influence levels and information needs.

3. Prepare Elicitation Plan and Materials: Develop custom elicitation toolkits, including interview question guides for safety engineers, workshop agendas for cross-functional teams, questionnaire forms for operators, and non-disclosure agreements (NDAs). Assign clear roles within the requirements team (lead interviewer, scribe, workshop facilitator).

4. Select Elicitation Techniques: Match each stakeholder group with the most appropriate technique based on safety impact and confidentiality needs. Assign document analysis to regulatory standards, interviews to safety and IT engineers, workshops to plant management, and questionnaires to maintenance technicians.

5. Conduct Elicitation Activities: Carry out planned interviews, workshops, survey distributions, and document reviews while maintaining ethical standards, non-coercive

communication, and cultural respect for local communities.

6. **Record and Secure Evidence:** Systematically store all raw data gathered during sessions. Maintain signed interview transcripts, workshop decision logs, survey spreadsheets, and annotated regulatory references. Apply access controls and encryption to confidential cybersecurity and plant infrastructure logs.
7. **Document Structured Requirements:** Translate unstructured notes and meeting minutes into standard, clear requirement statements. Use explicit language avoiding vague terms like "fast", "user-friendly", or "adequate".
8. **Classify and Review Requirements:** Group the draft requirements into distinct categories: Functional, Non-Functional, Safety, Regulatory, Environmental, or Operational. Share these initial structured drafts back with originating stakeholders to verify intended meaning.
9. **Perform Requirement Validation:** Evaluate every drafted requirement against formal quality criteria: correctness, completeness, consistency, technical feasibility, unambiguity, testability/verifiability, traceability, and safety compliance.
10. **Resolve Stakeholder Conflicts:** Identify overlapping or conflicting requirements across departments (e.g., Plant Operators needing immediate remote access versus IT Administrators enforcing network isolation). Convene trade-off resolution meetings to negotiate compromises, prioritizing mandatory safety regulations above operational convenience.
11. **Obtain Formal Approval:** Present the validated, conflict-free requirements specification package to project leads, Plant Management, and Safety Directors for formal sign-off. Archive signed approval certificates to establish the official requirements baseline.
12. **Maintain Traceability and Change Control:** Log all approved requirements into a Requirements Traceability Matrix (RTM) linking each item to its originating stakeholder and source document. Enforce a formal Change Control Board (CCB) procedure: any post-baseline modification request must undergo impact analysis, safety verification, and formal sign-off before being introduced.

E. Requirement Validation

Validation is the step that decides whether the requirements collected during elicitation are good enough to become the official baseline of the project. Verification asks whether the system was built correctly, while validation asks whether we wrote down the right requirements in the first place. For a nuclear power plant this difference matters, because a requirement that is wrong or open to interpretation will be designed, built and tested exactly as written, and the mistake will only be discovered when the plant is in operation.

In our plan, no requirement enters the baseline until it has passed the procedure described below. The procedure is carried out by the requirements team together with the stakeholder who gave the requirement, and for safety and regulatory items also with a reviewer who was not involved in writing it.

Validation Procedure

1. **Step 1: Entry check.** The requirements team confirms that the draft requirement has an ID, a category, a named source stakeholder and a piece of supporting evidence such as an interview record or a regulatory document. A requirement without a traceable source is sent back before any review time is spent on it.
2. **Step 2: Criteria check.** Each requirement is examined one at a time against the eight criteria listed in the next section. The reviewer writes the result for every criterion, so the record shows not only that the requirement passed, but also what was checked.
3. **Step 3: Stakeholder read-back.** The written requirement is read back to the stakeholder who originally raised it. The stakeholder confirms that the final wording still carries the meaning they intended, because a requirement can be perfectly clear and still say the wrong thing.
4. **Step 4: Independent review.** Safety, security and regulatory requirements are reviewed by a safety engineer who did not write them, and the licensing items are checked against the position of the Nuclear Regulatory Authority. This removes the risk of a team approving its own interpretation of a regulation.
5. **Step 5: Conflict handling.** Any contradiction found during the review is sent to the conflict procedure and is not left open in the document.
6. **Step 6: Approval and baseline.** A requirement that passes all checks is signed by the project lead and the Safety Director, added to the requirements baseline and entered in the Requirements Traceability Matrix. From that moment it can only be modified through the Change Control Board.

Validation Criteria

The table below defines the eight checks applied to every requirement, the question the reviewer answers, the method used, and the record that the check produces.

Check	What it means	How it is checked	Record produced
Correctness	The requirement states what the stakeholder or the regulation actually asks for.	Read-back with the source stakeholder, and comparison with the cited regulation or standard.	Signed read-back form

Completeness	Nothing important is missing, including the behaviour in start-up, normal operation, shutdown, maintenance and emergency conditions.	Walkthrough against an operating-mode checklist, and review of the open TBD list.	Walkthrough minutes, closed TBD list
Consistency	The requirement does not contradict another requirement or a term used elsewhere in the specification.	Cross-reference of every requirement that touches the same function, plus a check of the project glossary.	Cross-reference sheet, conflict log entry
Feasibility	The requirement can be achieved with the available technology, budget, schedule and staff skills.	Feasibility review with the design engineers and, where needed, the equipment supplier.	Feasibility note
Unambiguity	The sentence can only be understood in one way and contains no vague words such as fast, reliable or user-friendly.	Vague-word scan, then two reviewers explain the requirement separately and their explanations are compared.	Language review sheet
Verifiability / Testability	There is a practical way to prove later that the delivered system meets the requirement.	A verification method (test, inspection, analysis or demonstration) and a measurable acceptance criterion are assigned, and a draft test case is written.	Draft test case
Traceability	The requirement can be followed backwards to a stakeholder need and forwards to design and testing.	The RTM is updated when the requirement is approved, with the source record and the verification reference.	RTM row
Safety	The effect of the requirement on the safety functions of the plant is known and correctly classified.	Independent review by a safety engineer against the hazard list and the applicable IAEA and national safety requirements.	Safety review sign-off

Identifying, Discussing, Documenting and Resolving Conflicts

With this number of stakeholders, conflicting requirements are expected. The purpose of the procedure is not to avoid conflicts but to bring them to the surface early, because a conflict that is hidden in the specification becomes a design fault later.

Identification. Conflicts are found in three ways. The consistency check finds requirements that describe the same function in different ways. Workshops expose disagreements directly,

because two departments describe the same process in front of each other. The read-back sessions reveal the rest, when a stakeholder sees a requirement raised by another group and objects to it.

Discussion. The requirements engineer arranges a short trade-off meeting with the affected parties only. Each side is asked to explain the need behind its requirement instead of repeating the requirement, because most conflicts come from two valid needs and not from one side being wrong. The possible options are then compared in terms of safety impact, regulatory impact, cost and schedule.

Documentation. Every conflict is entered in the conflict log with an identifier, the requirements involved, the parties, the options considered, the option chosen, the reason for the choice, the approver and the date. Nothing is closed by a verbal agreement, and a conflict that is still open is reported to project management instead of being left in the document.

Resolution. Decisions follow a fixed order of priority: first mandatory nuclear safety and regulatory obligations, then environmental and public protection obligations, then operational and technical needs, and last cost and convenience. If the parties cannot agree, the conflict goes to the Change Control Board, and where the licence is affected the decision of the Nuclear Regulatory Authority is final.

Three examples from the conflict log are shown below.

ID	Conflict	Parties	Resolution and reason
CL -01	Operators asked for access to live plant data from outside the site during an incident, while IT required full isolation of the control network.	Plant Operators, IT and System Administrators	A one-way data feed to a read-only reporting server outside the control network was agreed. The need was visibility, not control, so no command path was created. Approved by the Safety Director.
CL -02	Management asked to reduce the number of redundant monitoring servers to lower cost, while safety engineers required redundancy for the availability target.	Plant Management, Safety Engineers	Redundancy was kept. Safety and availability obligations rank above cost in the priority order, and the reduction would have broken NFR-04.
CL -03	The local community asked for detailed public information during an incident, while security requirements restrict the release of plant technical data.	Local Community, Nuclear Regulatory Authority	The public alert gives location, risk level and required action, but no technical plant detail. The wording was agreed with the regulator so that the community is informed without creating a security risk.

F. Ethical Techniques and Behaviour

Requirements engineering in this project is not only a technical activity. The team will speak to plant employees who may fear for their jobs, to residents who did not choose to live near a nuclear plant, and to officials who control sensitive information. The practices below follow the ACM and IEEE codes of ethics and are written as behaviour the team will apply in the field.

Informed Participation

Every participant is told before the session who the team is, what the session is for, how their answers will be recorded and stored, who will read them, and how long the records will be kept. Participation is voluntary, and a participant may refuse a question or withdraw at any point without giving a reason. Consent is signed before the session begins, and a separate consent is taken for audio recording.

Honesty and Transparency

The team presents the purpose and the limits of the project honestly, including the fact that the requirements team does not decide whether the plant will be built. Stakeholders are told how much influence their input really has, so a community concern that will be forwarded to the regulator is described in exactly that way rather than answered with a promise the team cannot keep. Findings are also shared back with participants in plain language after the analysis.

Confidentiality

Interview records, questionnaire responses and workshop notes are stored with access control, and only the members of the requirements team need access to the raw material. When employees describe weaknesses in current safety practice, their statements are reported without identifying the individual, because an employee who is identified will not speak openly a second time. Personal data from community participants is anonymised in the report.

Avoiding Conflicts of Interest

Before elicitation starts, each team member declares any relationship with a bidding supplier, a contractor, a political body or a stakeholder organisation. A member with such a relationship does not run the sessions that involve that party and does not write or approve the related requirements. The declarations are kept in the project file, so the independence of the process can be shown later if it is questioned.

Respect for Local Communities and Culture

The sessions with communities near the proposed site are arranged at times and places that suit the residents, and not only the project team. They are conducted in French and in the local language with a qualified interpreter, and the materials use plain language instead of technical vocabulary. Local leaders are consulted on the format before the sessions are arranged, and community concerns are recorded as requirements input rather than treated as opposition to be managed.

Non-Coercive Communication

The team does not use technical authority, seniority or the presence of managers to push a stakeholder towards a particular answer. Questions are asked in a neutral form, so the team asks how the alarm response works today instead of asking whether the current alarm response is acceptable. When the subject is safety practice, employees are interviewed without their supervisor in the room, so that they can describe what actually happens rather than what is written in the procedure.

Accurate Recording of Stakeholder Views

Stakeholder views are recorded as they were given, including views that are inconvenient for the project. Notes are written during the session and confirmed with the participant before the session ends, and a second team member acts as scribe in workshops so that the record does not depend on one person's memory. Where a statement is an opinion or an assumption, it is marked as such and is not converted into a firm requirement. The team never invents or completes an answer that was not given.

Responsible Handling of Sensitive Information

Plant layout details, cybersecurity controls, emergency response timings and supplier prices are treated as restricted material. They are stored encrypted, shared only with people who need them for their work, and discussed in individual interviews rather than in open workshops. Any extract intended for the public report is reviewed with the plant security officer and the regulator before it is released.

Professional Accountability

Each team member remains responsible for the requirements they wrote, and the sign-off records show who wrote, reviewed and approved every item. Where the team does not have the specialist nuclear knowledge needed for a requirement, it states the limitation and asks for a qualified expert instead of writing an assumption into a safety requirement. Fabricating a stakeholder answer, hiding a known conflict, editing records after a session or approving a safety requirement without the independent review are treated as misconduct, and any requirement affected by them is removed from the baseline and collected again.

G. Sample Requirements and Evidence

The statements below are examples of the output that the elicitation activities would produce. They cover functional, non-functional, safety, regulatory, environmental and operational categories. Two of them are then taken through the validation criteria of Section E, and the traceability matrix at the end links every requirement back to the stakeholder need behind it.

Sample Requirements

ID	Type	Requirement statement	Source stakeholder	Technique
SR-01	Safety (functional)	The monitoring system shall send an automatic reactor shutdown signal within 2 seconds of detecting that the neutron flux has passed the licensed trip setpoint.	Safety Engineers, Nuclear Regulatory Authority	Interviews , Document analysis

FR-02	Functional	The system shall display the coolant temperature, pressure and flow rate in the main control room, refreshed at least once every second, and shall show the time of the last successful update beside each value.	Plant Operators	Interviews
FR-03	Functional	The system shall record every safety-related event and every operator action in a log that cannot be edited, and shall allow the log to be exported for inspection.	Safety Engineers, Nuclear Regulatory Authority	Interviews , Document analysis
NFR -04	Non-functional (availability)	The plant monitoring system shall reach an availability of at least 99.99% per calendar year, excluding maintenance windows agreed in advance with plant management.	Plant Management, Plant Operators	Workshops
NFR -05	Non-functional (security)	The plant control network shall have no routable connection to any public network. Data may leave the control network only through a one-way link to the reporting server, and no external system shall be able to send a command into the control network.	IT and System Administrators, Safety Engineers	Interviews
ENV -06	Environmental	The system shall notify the Nuclear Regulatory Authority and the responsible environmental agency within 15 minutes of any measured radiological release above the authorised limit, and shall store the notification with a timestamp.	Nuclear Regulatory Authority, Local Community	Document analysis, Questionnaires
OPS -07	Operational	The system shall start the public alert procedure for communities within a radius of 10 km within 5 minutes of the declaration of a site emergency, using at least two independent alert channels.	Emergency Response Team, Local Community	Workshops, Interviews

Validation of Two Sample Requirements

SR-01 and NFR-04 were chosen because the first is a safety-critical functional requirement and the second is a measurable non-functional requirement, so between them they show how the eight criteria are applied in practice.

Requirement SR-01, automatic shutdown signal on high neutron flux.

Check	How it was validated	Result
Correctness	Read back to the safety engineers who raised it and compared with the licensed trip setpoint in the regulator's design safety documentation.	Passed, setpoint reference added to the requirement
Completeness	A walkthrough confirmed that the behaviour is defined for normal operation, start-up and post-trip conditions. The behaviour on sensor failure was missing.	Passed after adding SR-01a for sensor failure
Consistency	Compared with FR-02 and NFR-05. The shutdown path does not depend on the reporting link, so no contradiction exists.	Passed
Feasibility	Confirmed with the design engineers that a response within 2 seconds is achievable with the proposed instrumentation.	Passed
Unambiguity	The first draft said the system shall shut down quickly. The vague word was replaced by the 2 second limit and the defined trip setpoint.	Passed after rewriting
Verifiability	Verification method: test. Acceptance criterion: in ten simulated over-flux injections the shutdown signal is issued in less than 2 seconds every time.	Passed, test case TC-SR-01 written
Traceability	Linked back to interview record INT-03 and the regulatory clause, and forward to the reactor protection system design and TC-SR-01.	Passed, recorded in the RTM
Safety	Reviewed by a safety engineer who did not write the requirement and classified as safety-critical.	Passed, signed on the safety review sheet

Requirement NFR-04, monitoring system availability of at least 99.99%.

Check	How it was validated	Result
Correctness	Confirmed with plant management in the workshop that the figure applies to the monitoring system and not to plant generation availability.	Passed, wording clarified
Completeness	Checked whether the measurement period and the exclusions are stated. The exclusion for agreed maintenance was missing in the first draft.	Passed after adding the maintenance exclusion
Consistency	Compared with the maintenance requirements. The agreed maintenance windows are excluded explicitly, so there is no contradiction.	Passed
Feasibility	Reviewed with the design team. The target allows about 53 minutes of unplanned downtime per year and needs redundant servers and power supply, which fit inside the budget.	Passed with redundancy included
Unambiguity	The phrase high availability taken from the workshop notes	Passed after rewriting

	was replaced by a numeric target with a stated measurement period.	
Verifiability	Verification method: analysis and operational measurement. Acceptance criterion: recorded unplanned downtime over twelve months does not exceed 53 minutes.	Passed, test case TC-NFR-04 written
Traceability	Linked back to workshop record WS-02 and forward to the redundancy design and TC-NFR-04.	Passed, recorded in the RTM
Safety	Classified as safety-related, because losing the monitoring system reduces the ability of the operators to detect an abnormal condition.	Passed, signed on the safety review sheet

Requirements Traceability Matrix

The matrix connects each requirement to the stakeholder need that produced it, to the evidence collected during elicitation, and to the design element and verification activity that will prove it. It is updated whenever a requirement is approved or changed, so the project can always show where a requirement came from and how it will be tested.

Req ID	Stakeholder need	Source evidence	Design element	Verification	Status
SR-01	The reactor must shut down automatically before an unsafe power level is reached (Safety Engineers, Regulatory Authority)	INT-03 interview transcript, regulatory design clause	Reactor protection system logic	TC-SR-01 (test)	Approved
FR-02	Operators need live plant readings they can trust while monitoring the plant (Plant Operators)	INT-05 transcript, control room mock-up review PR-01	Control room display module	TC-FR-02 (demonstration)	Approved
FR-03	Safety events and operator actions must be available for later inspection (Safety Engineers, Regulatory Authority)	INT-06 transcript, annotated regulation DOC-02	Event logging and archive module	TC-FR-03 (inspection)	Approved
NFR -04	Management needs a monitoring system dependable enough to base decisions on (Plant Management)	WS-02 workshop decision log	Redundant server and power design	TC-NFR-04 (analysis)	Approved

NFR-05	The control network must not be reachable from outside the plant (IT and System Administrators)	INT-08 transcript, conflict log CL-01	Network isolation and one-way data link	TC-NFR-05 (inspection and test)	Approved
ENV-06	The authorities must learn quickly about any release above the limit (Regulatory Authority, Local Community)	Annotated environmental regulation DOC-05, questionnaire summary Q-02	Automatic notification service	TC-ENV-06 (test)	Under review
OPS-07	Residents must be warned in time to follow the emergency plan (Local Community, Emergency Response Team)	WS-04 workshop log, conflict log CL-03	Public alert interface	TC-OPS-07 (demonstration)	Under review

Conclusion

These three sections close the requirements process described earlier in the report. The validation procedure makes sure that what was collected is correct, clear, feasible and testable before it is frozen as a baseline. The ethical practices protect the quality of the input itself, because requirements taken from people who were rushed, pressured or misinformed are not reliable however carefully they are reviewed afterwards. The sample requirements and the traceability matrix show the result: a specification in which every statement can be explained, traced to the stakeholder who needed it, and proven in the finished system.

References

Association for Computing Machinery. (2018). ACM code of ethics and professional conduct. ACM. https://www.acm.org/code-of-ethics

Institute of Electrical and Electronics Engineers. (2020). IEEE code of ethics. IEEE. https://www.ieee.org/about/corporate/governance/p7-8.html

International Atomic Energy Agency. (2016). Safety of nuclear power plants: Design (Specific Safety Requirements No. SSR-2/1, Rev. 1). IAEA. https://www.iaea.org/publications

ISO/IEC/IEEE. (2018). ISO/IEC/IEEE 29148:2018: Systems and software engineering – Life cycle processes – Requirements engineering. International Organization for Standardization. https://www.iso.org/standard/72089.html

Sommerville, I. (2016). Software engineering (10th ed.). Pearson Education.

U.S. Nuclear Regulatory Commission. (2026). Regulations and guidance. https://www.nrc.gov/reactors/operator-licensing/regs-guides

International Atomic Energy Agency. (2025). Stakeholder engagement in new nuclear power programmes. IAEA. https://www.iaea.org/

ISO/IEC/IEEE. (2018). ISO/IEC/IEEE 29148:2018: Systems and software engineering — Life cycle processes — Requirements engineering. International Organization for Standardization. https://www.iso.org/standard/72089.html

U.S. Nuclear Regulatory Commission. (2026). Regulations and guidance. https://www.nrc.gov/reactors/operator-licensing/regs-guides

U.S. Nuclear Regulatory Commission. (2026). Regulations and standard review plan concerning radiation protection for new reactors. https://www.nrc.gov/reactors/new-reactors/how-we-regulate/oversight/rad-protection/reg