CS-001

Therac-25: A Structural Authority Gate Analysis

Realis Institute Case Study 001

Version 1.0 | Realis Institute

realisinstitute.com

Therac-25: A Structural Authority Gate Analysis

Realis Institute Case Study 001 | Version 1.0

Purpose

This case study applies Structural Authority Gate (SAG) classification to the Therac-25 radiation therapy accidents between 1985 and 1987. The analysis demonstrates how SAG exposes a structural failure that conventional safety analyses leave in the background: the absence of instantiated authority governing software safety throughout the operational system.

The Therac-25 is a canonical case in safety engineering, software engineering, and computer ethics. Technical failure modes are well documented. Cultural and organizational contributors have received extensive analysis. What is insufficiently articulated is the authority structure, more precisely, the absence of one, that permitted harm to recur through multiple incidents, institutions, and regulatory interactions.

This document serves as a diagnostic application of SAG.

Background (Minimal)

The Therac-25 was a computer-controlled radiation therapy machine manufactured by Atomic Energy of Canada Limited. Between June 1985 and January 1987, the system produced six known radiation overdoses at medical facilities in the United States and Canada. At least three patients died as a direct result. Others sustained severe injuries including radiation burns, paralysis, and amputation.

Documented technical causes included software race conditions, inadequate error handling, and removal of hardware safety interlocks present in earlier models. These causes appear in the Leveson and Turner IEEE paper and subsequent analyses.

This case study examines authority structure.

The Authority Question

Who held authority to halt use of the Therac-25 after the first overdose?

The historical record provides no clear answer. The absence reflects lack of instantiated authority rather than missing documentation.

The SAG decisive test asks:

> *Could a single accountable person be named without contradicting the surrounding facts?*

Applied to the Therac-25 system within its institutional context, including manufacturer, hospitals, and regulators, the answer at every critical juncture was Indeterminate or Absent.

SAG Classification of Key Decision Points

1. Kennestone Regional Oncology Center (June 1985)

What happened	A patient received a massive radiation overdose during treatment and reported a burning sensation. The hospital physicist contacted AECL to ask whether an overdose was possible. AECL responded that overdose could not occur.
Authority language in the record	Hospital staff held responsibility for patient care but lacked authority over software safety. AECL asserted that overdose was impossible and did not claim accountability for investigation outcomes. The FDA was not notified. Reporting requirements applied only to manufacturers.
SAG classification	Who held accountability for determining whether the software had malfunctioned? No explicit designation existed. The hospital had clinical responsibility. AECL manufactured the system. Neither party asserted accountable authority over the investigation outcome.
Classification	**Indeterminate**
Basis	Authority over software incident investigation diffused across institutions. The hospital lacked standing to compel investigation. AECL denied malfunction. Regulatory involvement did not occur. No singular accountable person existed.

2. Hamilton, Ontario (July 1985)

What happened	A patient received an overdose. The machine displayed error messages while indicating no dose delivered. The operator proceeded multiple times before the system suspended treatment. AECL and Canada's Radiation Protection Bureau were notified. AECL suspected a microswitch failure but could not reproduce the fault.
Authority language in the record	AECL quality assurance management testified that modifications improved safety by several orders of magnitude. The CRPB issued directives requesting hardware interlocks and software changes. AECL partially complied by reducing retry counts rather than implementing full suspension mechanisms.

SAG classification	Who held accountability for ensuring compliance with CRPB software safety directives? The CRPB issued requirements. AECL partially complied. No enforcement structure assigned singular accountability.
Classification	**Indeterminate**
Basis	Regulatory authority existed. The record identifies no accountable individual responsible for enforcement. Partial compliance persisted until subsequent incidents changed enforcement priorities.

3. East Texas Cancer Center (March to April 1986)

What happened	Two patients received massive overdoses within three weeks. The first died five months later. The second died three weeks after the incident. Hospital physicist Fritz Hager reproduced the failure by entering data at high speed, identifying a software race condition.
Authority language in the record	After the first incident, AECL engineers reported inability to reproduce the error and suggested electrical causes. The hospital physicist conducted an independent investigation and notified AECL. After the second incident, AECL acknowledged the software defect following demonstration.
SAG classification	Who possessed authority to determine whether the system could continue operating between the two incidents? The hospital physicist identified risk without authority. AECL denied malfunction. Authority to keep the system out of service did not instantiate.
Classification	**Indeterminate**
Basis	Authority to halt operation diffused among institutions. The system returned to service, resulting in a second fatality.

4. FDA and AECL Corrective Action Process (1986 to 1987)

What happened	The FDA declared the Therac-25 defective and required a Corrective Action Plan. AECL submitted multiple revisions. The process extended over two years.

Authority language in the record	The FDA declared defect, demanded corrective action, and required user renotification. AECL issued operational advisories that did not describe hazards or defects. FDA internal memoranda documented absence of software specifications, testing plans, and quality assurance controls.
SAG classification	Where did accountable authority for software safety reside at AECL? The software had been written by a single programmer who left the company in 1986. Subsequent proceedings failed to identify a responsible owner or steward.
Classification	**Absent**
Basis	Software safety authority never instantiated. Departure of the programmer left no accountable steward for patient-critical code.

5. Yakima Valley Memorial Hospital (January 1987)

What happened	A patient received an overdose caused by a different software defect. AECL had developed fixes after earlier incidents but had not installed them.
Authority language in the record	AECL quality assurance management stated that fixes had been planned but not installed. The FDA recommended shutdown of all Therac-25 units until permanent modifications occurred.
SAG classification	Who held accountability for deployment of known software safety fixes? AECL possessed the fixes. Installation had not occurred. No party held accountability for deployment timing.
Classification	**Absent; later Present by regulatory action**
Basis	The system continued operating despite known defects and available fixes. Authority over deployment timing diffused among manufacturer, hospitals, and regulators. Decisive authority appeared only when the FDA recommended shutdown of all Therac-25 units.

What SAG Reveals

Standard analyses identify software defects, testing failures, error messaging problems, and organizational weaknesses. These findings explain technical failure.

Continued operation requires a separate explanation.

SAG exposes the structural condition that permitted recurring harm.

At no point did a single accountable person hold authority over software safety.

Hospitals bore responsibility without authority. The manufacturer denied failure modes. Regulators acted reactively without singular enforcement accountability.

When authority is Absent, refusal cannot occur. Standing to suspend operation pending designation of accountability did not exist.

Implications

What conditions would explicit authority have changed?

If SAG had informed response after the first incident:

Kennestone, June 1985: Classification Absent would have triggered refusal and suspension pending designation of accountable authority for investigation.

Hamilton, July 1985: Classification Indeterminate or Absent would have required designation or refusal.

East Texas, March 1986: Return to service would not occur without explicit accountability for investigation outcomes.

Yakima, January 1987: Operation would not proceed with known uninstalled fixes absent accountable deployment authority.

SAG does not prevent software defects. The framework prevents operation when accountability for safety does not exist.

Conclusion

The Therac-25 is commonly taught as a failure of software engineering, testing, and safety culture. Each category applies.

The case also represents a failure of authority structure.

Harm persisted because authority over software safety never instantiated at the manufacturer, at the hospitals, or within regulatory oversight. Responsibility appeared everywhere. Authority appeared nowhere.

SAG classification would have exposed this condition at the first incident. The appropriate response would have been refusal or designation request, forcing a single unanswered

question:

> *Who is accountable for this?*

That question never received an answer. The Therac-25 demonstrates the consequence.

Sources

Leveson, N.G. and Turner, C.S. An Investigation of the Therac-25 Accidents. IEEE Computer, 26(7), 1993.

FDA correspondence and internal memoranda, 1986 to 1987, as documented in Leveson and Turner.

Canadian Radiation Protection Bureau correspondence, 1985 to 1987, as documented in Leveson and Turner.

Deposition testimony from AECL quality assurance personnel, as documented in Leveson and Turner.

This case study applies SAG classification to historical events and assigns no blame or legal judgment.

Notes on Preparation

Some case studies were developed with the assistance of AI tools used for drafting, synthesis, and internal review. Analytic judgment, classification, and publication decisions are governed by Realis Institute.