AI-04723 Common Problem Solving Tool

#cmp

I've tested FTA and FMEA here with you, what other problem solving tools do you have? Can you do Inventive Problem Solving using TRIZ? What about 5 Whys? What about RCA? SWOT? List all NASA tools and common tools available. List all system engineering used in manufacturing and NASA. What is PRA combining FTA and ETA. Explain more.

Yes. **TRIZ, 5 Whys, RCA, SWOT, and many other structured problem-solving methods are available to me.** More importantly, I can combine them into a single engineering investigation rather than treating each tool as an isolated exercise.

For example, your Samsung CMP training scenario could use:

> **Problem definition → Process mapping → 5 Whys → Fishbone → FTA → FMEA → TRIZ → Corrective action → Verification → Lessons learned**

That is much closer to how a mature engineering organization approaches complex problems.

1. The Big Picture: A Problem-Solving Toolbox

There are several different families of tools. They answer different questions.

Tool family	Primary question	Typical output
Problem definition	What exactly is wrong?	Problem statement, scope
Root cause analysis	Why did it happen?	Verified causal chain
Risk analysis	What could go wrong?	Risk register, FMEA, FTA
Reliability engineering	How likely is failure, and how severe?	Reliability model, criticality ranking
Process improvement	Where is the process losing performance?	Improved workflow, control plan
Inventive problem solving	How can we eliminate the contradiction causing the problem?	Innovative design or process concept
Decision analysis	Which option is best?	Trade study, decision matrix
Systems engineering	How do all parts work together across the lifecycle?	Requirements, architecture, verification
Human factors	How do people interact with the system, and where can error occur?	Human-error analysis, improved interfaces
Strategic analysis	What internal and external factors affect success?	SWOT, strategic options
Learning and prevention	How do we prevent recurrence and institutionalize knowledge?	CAPA, lessons learned, standards

---

2. Yes—I Can Perform TRIZ

What is TRIZ?

TRIZ is the Russian acronym for *Theory of Inventive Problem Solving*.

It was developed from the study of patterns in inventive patents. Instead of asking only:

> "What caused the problem?"

TRIZ asks:

> **"What contradiction prevents the system from improving, and how can we resolve that contradiction without accepting the usual trade-off?"**

This makes TRIZ especially useful when conventional corrective actions merely move the problem somewhere else.

Example: Manufacturing contradiction

Suppose a CMP process needs:

- Higher cleaning force to remove contaminants.
- Lower mechanical force to avoid wafer damage.

A conventional approach might compromise:

> Increase cleaning effectiveness, but accept some increase in damage.

A TRIZ approach asks:

> **Can the system produce strong cleaning where needed while avoiding damaging force where it is not needed?**

Potential inventive directions might include:

- Spatially selective action.
- Time-separated process stages.
- Pulsed rather than continuous energy.
- Different mechanisms for different contamination types.
- Self-adjusting process parameters.
- Using an existing process resource in a new function.

These are **concept directions**, not claims about Samsung's actual equipment or validated process recipes.

TRIZ tools I can apply

TRIZ method	What it does
Ideal Final Result (IFR)	Defines the desired outcome with minimal added complexity, cost, or harm
Technical contradictions	Identifies when improving one parameter worsens another
Physical contradictions	Identifies when the same element seems to need two opposing properties
40 Inventive Principles	Generates structured solution concepts
Contradiction Matrix	Maps engineering conflicts to candidate inventive principles
Separation principles	Resolves physical contradictions by separating in time, space, condition, or scale
Resources analysis	Finds unused materials, energy, information, time, space, or system capabilities

Trimming	Removes components or functions while preserving required outcomes
Function analysis	Examines useful, harmful, insufficient, and excessive interactions
Su-Field analysis	Models interactions between substances and fields
Standard inventive solutions	Applies recurring solution patterns to system problems
Evolution of technical systems	Identifies likely improvement directions based on system evolution patterns
ARIZ	A more intensive, step-by-step algorithm for complex inventive problems
Effects database thinking	Looks for physical, chemical, geometric, or other effects that could perform a needed function

Important distinction

TRIZ is not primarily a root-cause tool. It is an **innovation and contradiction-resolution tool**.

A useful combination is:

> **RCA identifies why the current system fails. TRIZ identifies how to redesign the system so the failure mechanism becomes unnecessary or much less likely.**

---

3. 5 Whys

What is it?

5 Whys is a simple causal investigation method that repeatedly asks “Why?” until the team reaches a controllable underlying cause.

It is associated with the Toyota Production System and Lean problem solving.

Example

Problem: CMP technician repeatedly misses a required preventive-maintenance step.

Level	Question	Example answer
1	Why was the PM step missed?	The technician completed the checklist without performing the step.
2	Why was the checklist completed without the step?	The step was recorded as a single checkbox with no confirmation requirement.
3	Why was there no confirmation requirement?	The work instruction assumed the technician would follow the sequence correctly.
4	Why did the process rely on that assumption?	The procedure was designed around experienced technicians.

5	Why was new-hire usability not considered?	The procedure had not undergone a formal human-factors or training-readiness review.

Potential root cause

> The maintenance-control system relies on assumed operator behavior rather than making critical steps observable, verifiable, and difficult to skip.

That is much stronger than saying:

> "The technician needs to pay more attention."

Limitations

5 Whys can fail when:

- There are multiple interacting causes.
- The team stops at the first plausible explanation.
- The cause is actually a combination of conditions.
- The investigation blames a person instead of examining the system.
- The "why" chain becomes speculative.

Best practice: Use 5 Whys with evidence, process observation, data, and—when necessary—FTA, fishbone, or causal analysis.

---

4. RCA — Root Cause Analysis

What is RCA?

Root Cause Analysis is not one single tool. It is an **investigation discipline** that uses multiple methods to identify, verify, and eliminate causes of an undesirable event.

The goal is not merely to explain what happened.

> **The goal is to identify causes that, when controlled or eliminated, substantially reduce the probability of recurrence.**

RCA methods I can perform

RCA method	Best use
5 Whys	Simple causal chains
Fishbone / Ishikawa	Broad cause brainstorming and categorization
Fault Tree Analysis	Top-down logical analysis of an undesired event
Event Tree Analysis	Forward analysis of possible outcomes after an initiating event
Cause-and-effect matrix	Links inputs to outputs and prioritizes likely contributors
Causal factor charting	Maps events, conditions, and contributing factors over time
Apollo Root Cause Analysis	Uses cause-and-effect relationships and multiple causes
Barrier analysis	Examines failed or missing preventive/detective barriers

Change analysis	Compares what changed between normal and abnormal conditions
Kepner-Tregoe problem analysis	Structured “Is / Is Not” and deviation analysis
TapRooT-style investigation	Structured causal investigation and corrective-action development
Human-error analysis	Examines slips, mistakes, workload, design, and organizational contributors
Fault isolation	Narrows a failure to the responsible subsystem or component
Evidence timeline	Reconstructs the sequence of events
Comparative analysis	Compares good vs. bad lots, shifts, tools, operators, recipes, or conditions

RCA workflow

1. **Define the problem**
2. **Preserve evidence**
3. **Establish what happened**
4. **Establish what should have happened**
5. **Identify deviations**
6. **Identify causal factors**
7. **Verify causes against evidence**
8. **Develop corrective and preventive actions**
9. **Verify effectiveness**
10. **Update procedures, training, and controls**

RCA versus FTA versus FMEA

Method	Direction	Main question
RCA	Backward from an actual problem	Why did this actual event happen?
FTA	Top-down from an undesired event	What combinations could cause this event?
FMEA	Bottom-up from components/process steps	What could fail, and what would happen?
ETA	Forward from an initiating event	What outcomes follow depending on barriers succeeding or failing?
TRIZ	From contradiction toward an inventive solution	How can we improve without creating the usual trade-off?

NASA itself identifies RCA, FMEA/FMECA, FTA, hazard analysis, Pareto, affinity grouping, brainstorming, and process mapping among risk-management techniques. (**NASA Technical Reports Server**)

---

5. SWOT Analysis

What is SWOT?

SWOT stands for:

- **S — Strengths**
- **W — Weaknesses**
- **O — Opportunities**
- **T — Threats**

It is primarily a **strategic and situational analysis tool**, not a detailed engineering failure-analysis method.

Example: New CMP Technician Development Program

	Positive	**Negative**
Internal	**Strengths**: Structured training, experienced mentors, documented procedures, equipment exposure	**Weaknesses**: Information overload, inconsistent coaching, limited hands-on time, unclear qualification criteria
External	**Opportunities**: Digital work instructions, simulation, skills matrix, predictive maintenance, cross-training	**Threats**: Production pressure, staffing shortages, equipment complexity, turnover, changing process technology

SWOT is useful for:

- Training-program design.
- Manufacturing department strategy.
- Career development.
- Business planning.
- Technology adoption.
- Organizational readiness.
- Supplier evaluation.
- Maintenance strategy.

SWOT is not sufficient for:

- Proving a physical root cause.
- Quantifying equipment failure probability.
- Determining whether a safety barrier is adequate.
- Replacing FMEA, FTA, or validation testing.

---

6. Other Major Problem-Solving Tools I Can Perform

A. Problem Definition and Scoping

These prevent solving the wrong problem.

Tool	**Purpose**
Problem statement	Defines the gap between actual and desired performance
SMART problem definition	Makes the problem specific and measurable
5W1H	Who, what, when, where, why, how

Is / Is Not Analysis	Narrows the problem boundary
SIPOC	Suppliers, Inputs, Process, Outputs, Customers
Project charter	Defines objective, scope, stakeholders, constraints
Voice of the Customer (VOC)	Converts customer needs into requirements
CTQ tree	Converts broad needs into measurable critical-to-quality characteristics
KPI tree	Breaks strategic goals into measurable drivers
Gemba analysis	Examines the actual workplace and process
Process walk / Walk the Process	Follows the actual flow rather than relying on documentation

B. Cause Analysis and Visualization

Tool	Purpose
Fishbone / Ishikawa diagram	Organizes possible causes
Cause-and-effect diagram	Maps relationships between causes and effects
Causal loop diagram	Shows reinforcing and balancing feedback
Influence diagram	Maps factors influencing an outcome
Interrelationship diagram	Identifies cause-effect relationships among many factors
Affinity diagram	Groups large amounts of qualitative information
Tree diagram	Breaks a broad issue into smaller elements
Why-Why analysis	Expands causal reasoning
Fault tree	Uses Boolean logic to analyze failure causes
Event tree	Models possible outcome paths
Bow-tie analysis	Combines fault tree and event tree around a hazardous event
Barrier analysis	Evaluates preventive and mitigative controls
Swiss-cheese model	Examines layered defenses and alignment of failures
STAMP / STPA	Analyzes safety as a control-system problem
FRAM	Examines variability and interactions in complex systems

C. Statistical and Data-Driven Tools

Tool	Purpose
Check sheet	Structured data collection
Tally sheet	Counts occurrences
Histogram	Shows distribution
Pareto chart	Prioritizes the “vital few” contributors
Run chart	Shows performance over time

Control chart / SPC	Detects unusual process variation
Scatter plot	Examines relationships between variables
Box plot	Compares distributions
Stratification	Separates data by shift, tool, lot, operator, recipe, etc.
Correlation analysis	Measures association between variables
Regression analysis	Models relationships and predicts outcomes
ANOVA	Compares means across groups
Hypothesis testing	Evaluates evidence for a claim
Design of Experiments (DOE)	Tests factors systematically
Screening DOE	Identifies important factors efficiently
Response Surface Methodology (RSM)	Optimizes process settings
Measurement System Analysis (MSA)	Evaluates measurement reliability
Gage R&R	Separates measurement variation from process variation
Process capability analysis	Evaluates ability to meet specifications
Cp / Cpk / Pp / Ppk	Quantifies process capability/performance
Time-series analysis	Identifies trends, cycles, and shifts
Reliability growth analysis	Tracks improvement in failure performance
Weibull analysis	Models failure-time distributions
Monte Carlo simulation	Propagates uncertainty through a model
Sensitivity analysis	Identifies variables that most affect outcomes

D. Lean, Six Sigma, and Operational Excellence

Tool / Method	Purpose
PDCA	Plan → Do → Check → Act
PDSA	Plan → Do → Study → Act
DMAIC	Define → Measure → Analyze → Improve → Control
DMADV / DFSS	Design new processes/products for quality
A3 Problem Solving	Concise structured problem-solving report
Kaizen	Incremental continuous improvement
Kaizen Event	Focused improvement workshop
Standard Work	Defines the best-known repeatable method
Standard Work Combination Table	Maps operator time, machine time, and sequence
Value Stream Mapping (VSM)	Maps material and information flow
Process Mapping	Visualizes process steps and decisions
Spaghetti Diagram	Shows physical movement and waste
Takt Time Analysis	Aligns production pace with demand

Line Balancing	Distributes work across stations
5S	Sort, Set in order, Shine, Standardize, Sustain
Visual Management	Makes status and abnormalities visible
Andon	Signals abnormal conditions
Jidoka	Built-in quality and stop-to-fix principle
Poka-Yoke	Mistake-proofing
Heijunka	Production leveling
SMED	Single-Minute Exchange of Die; setup reduction
TPM	Total Productive Maintenance
OEE	Overall Equipment Effectiveness
Loss Tree	Categorizes operational losses
Hoshin Kanri	Strategy deployment
Standardized Work Audit	Verifies adherence and effectiveness

7. Reliability, Safety, and Risk Tools

This is the family most closely related to your FTA/FMEA work.

Tool	Primary purpose
FMEA	Identify failure modes and effects
FMECA	FMEA plus criticality assessment
System FMEA	Analyze system-level failures
Design FMEA (DFMEA)	Analyze design-related failures
Process FMEA (PFMEA)	Analyze manufacturing/process failures
Equipment FMEA	Analyze equipment failure modes
Software FMEA	Analyze software fault modes
FTA	Deductive analysis from top event
ETA	Forward analysis of event outcomes
PRA	Probabilistic Risk Assessment
QRA	Quantitative Risk Assessment
HAZOP	Systematic deviation-based hazard analysis
HAZID	Hazard identification
What-If Analysis	Structured hypothetical hazard questions
Checklist Analysis	Uses known hazard/failure checklists
Preliminary Hazard Analysis (PHA)	Early hazard identification
Operating and Support Hazard Analysis	Hazards during operation and maintenance
Job Safety Analysis (JSA/JHA)	Task-level hazard analysis

Criticality Analysis	Identifies high-consequence/high-risk items
Common Cause Failure Analysis	Finds shared causes that defeat redundancy
Single-Point Failure Analysis	Identifies failures with no adequate backup
Sneak Circuit Analysis	Finds unintended paths in systems
Fault Injection Testing	Deliberately introduces faults to test resilience
Failure Detection, Isolation, and Recovery (FDIR)	Detects and responds to failures
Fault Containment	Limits failure propagation
Reliability Block Diagram (RBD)	Models system reliability architecture
Markov Analysis	Models state transitions and repairable systems
Petri Net Analysis	Models concurrent and event-driven systems
Stress-strength analysis	Compares applied stress with component strength
Derating analysis	Reduces component stress to improve reliability
Worst-case analysis	Evaluates parameter extremes
Limit / margin analysis	Measures distance to failure or requirement limits

NASA's reliability and safety practice explicitly uses FMEA/FMECA, FTA, hazard analysis, and probabilistic risk methods. NASA's FTA guidance describes FTA as a top-down approach, while FMEA is bottom-up. (**S3VI**)

---

8. Design and Inventive Engineering Tools

This is where **TRIZ** belongs.

Tool	**Purpose**
TRIZ	Resolve contradictions and generate inventive solutions
ARIZ	Advanced TRIZ problem-solving algorithm
40 Inventive Principles	Structured idea generation
Contradiction Matrix	Maps technical contradictions to principles
Ideal Final Result	Defines ideal system behavior
Resource Analysis	Finds unused system resources
Function Analysis	Analyzes useful and harmful functions
Trimming	Eliminates unnecessary components/functions
Su-Field Modeling	Models interactions and fields
Morphological Analysis	Explores combinations of design parameters
Morphological Matrix	Generates systematic design alternatives
Design for Six Sigma (DFSS)	Designs robust products/processes
Design for Manufacturability (DFM)	Makes products easier to manufacture
Design for Assembly (DFA)	Makes assembly easier and more reliable
Design for Reliability (DfR)	Designs for dependable performance

Design for Maintainability	Makes maintenance easier and safer
Design for Testability (DFT)	Makes faults easier to detect and isolate
Design for Safety	Reduces hazards through design
Design for Serviceability	Improves repair and service operations
Value Engineering	Optimizes function relative to cost
Functional Decomposition	Breaks system functions into subfunctions
Morphological Chart	Generates possible solution architectures
Concept Selection Matrix	Compares design concepts
Trade Study	Evaluates competing alternatives
Robust Design	Reduces sensitivity to variation
Taguchi Methods	Robust parameter design and experimental optimization
QFD	Translates customer needs into engineering requirements

---

9. Decision-Making and Trade-Off Tools

Engineering rarely asks only, “What is the cause?”

It also asks:

> “Which solution should we implement?”

Tool	Purpose
SWOT	Strategic internal/external assessment
Decision Matrix	Scores alternatives against criteria
Pugh Matrix	Compares concepts against a baseline
Weighted Trade Study	Quantifies competing objectives
Kepner-Tregoe Decision Analysis	Structured alternatives and risk assessment
AHP — Analytic Hierarchy Process	Pairwise comparison of criteria and options
TOPSIS	Multi-criteria decision analysis
Cost-Benefit Analysis	Compares expected costs and benefits
Risk-Adjusted Decision Analysis	Includes uncertainty and consequences
Sensitivity Analysis	Tests whether the decision changes under assumptions
Value of Information	Determines whether additional information is worth obtaining
Real Options Analysis	Evaluates flexibility under uncertainty
Scenario Analysis	Examines possible future conditions
Decision Tree	Maps decisions, uncertainties, and outcomes
Expected Value Analysis	Compares probability-weighted outcomes
FMEA-based prioritization	Ranks corrective-action opportunities
Multi-Attribute Utility Theory	Evaluates competing objectives and preferences

NASA's systems engineering handbook specifically identifies simulations, weighted trade-off matrices, engineering/manufacturing/cost/technical trade studies, human-in-the-loop testing, prototypes, and testing as evaluation methods. (NASA Science)

---

10. Human Factors and Organizational Problem Solving

This is especially important for **new-hire success, technician qualification, medical operations, and safety-critical work**.

Tool	Purpose
Human Factors Analysis and Classification System (HFACS)	Classifies human and organizational contributors
Task Analysis	Breaks work into actions, decisions, and conditions
Hierarchical Task Analysis (HTA)	Decomposes tasks and subtasks
Cognitive Task Analysis (CTA)	Examines knowledge, decisions, and mental demands
Human Reliability Analysis (HRA)	Estimates likelihood of human error
SHERPA	Structured human-error prediction
THERP	Technique for Human Error Rate Prediction
HEART	Human Error Assessment and Reduction Technique
Cognitive walkthrough	Evaluates how users perform tasks
Usability analysis	Finds barriers to effective use
Workload analysis	Examines cognitive and physical workload
Error-proofing	Prevents predictable mistakes
Situation Awareness Analysis	Examines perception, comprehension, projection
Crew Resource Management (CRM)	Improves team coordination and decision-making
Organizational accident analysis	Examines latent organizational conditions
Learning-curve analysis	Tracks skill acquisition
Competency gap analysis	Compares required versus demonstrated skills
Training Needs Analysis (TNA)	Identifies what training is actually needed
Skills Matrix	Maps personnel capabilities
Qualification Matrix	Tracks authorization and proficiency
Job Instruction Training	Breaks work into preparation, presentation, tryout, follow-up
Knowledge retention analysis	Evaluates whether training transfers to performance

For your CMP technician example, **HTA + human-error analysis + PFMEA + standard work + qualification matrix** could be more useful than simply adding more classroom hours.

---

11. NASA Systems Engineering: The Core Framework

NASA does not use one single “NASA problem-solving tool.” It uses a **systems engineering lifecycle** supported by many analyses, reviews, models, and risk-management practices.

NASA defines systems engineering as a methodical, multidisciplinary approach to the **design, realization, technical management, operations, and retirement of a system**. (NASA)

The NASA Systems Engineering Handbook organizes its guidance around:

1. Systems engineering fundamentals.
2. Program/project lifecycle.
3. System design processes.
4. Product realization.
5. Crosscutting technical management.
6. Supporting appendices and work products.

(NASA)

NASA's 17 common technical processes

NASA's systems engineering framework identifies **17 common technical processes**. These are the backbone of the NASA approach.

Stakeholder and system definition

1. **Stakeholder Expectations Definition**
2. **Technical Requirements Definition**
3. **Logical Decomposition**
4. **Design Solution Definition**

Product realization

5. **Product Implementation**
6. **Product Integration**
7. **Product Verification**
8. **Product Validation**
9. **Product Transition**

Technical management and control

10. **Technical Planning**
11. **Requirements Management**
12. **Interface Management**
13. **Technical Data Management**
14. **Technical Assessment**
15. **Decision Analysis**
16. **Technical Risk Management**
17. **Configuration Management**

Important: NASA's lifecycle is iterative and recursive. These processes are not simply performed once in a straight line. They are revisited as the system becomes better understood. NASA notes that the amount of formality and depth varies with project size, complexity, and risk. (NASA)

---

12. NASA Systems Engineering Tools and Work Products

Below is a practical catalog of tools and artifacts associated with NASA-style systems engineering.

A. Requirements Engineering

Tool / artifact	Purpose
Stakeholder analysis	Identifies stakeholders and their needs
ConOps — Concept of Operations	Describes how the system will be used
Mission Concept Review (MCR)	Evaluates mission concept maturity
Mission requirements	Defines mission-level needs
System requirements	Defines what the system must do
Derived requirements	Requirements logically derived from higher-level needs
Requirements traceability matrix	Links requirements to design and verification
Requirements quality checklist	Tests clarity, consistency, verifiability, necessity
Requirements allocation	Assigns requirements to subsystems
Requirements decomposition	Breaks high-level requirements into lower-level requirements
Requirements validation	Confirms requirements represent actual needs
Requirements verification	Confirms requirements are correctly implemented
Requirements management database	Controls requirements across the lifecycle
Interface requirements	Defines interactions between systems
Verification requirements matrix	Maps requirements to verification methods

NASA provides specific guidance on writing requirements and requirements verification/validation matrices in its Systems Engineering Handbook appendices. (NASA)

B. Functional and Architectural Analysis

Tool / artifact	Purpose
Functional analysis	Identifies required system functions
Functional decomposition	Breaks system functions into subfunctions
Functional flow block diagram (FFBD)	Shows functional sequence
Enhanced FFBD (EFFBD)	Adds richer functional-flow information
Functional architecture	Defines how functions are organized
Logical architecture	Defines logical relationships and behavior
Physical architecture	Maps functions to physical components
Behavior diagrams	Shows system behavior and interactions
State diagrams	Shows operating states and transitions
Activity diagrams	Shows activities and flow
Sequence diagrams	Shows interactions over time
N-squared diagram (N^2)	Shows interfaces and interactions
IDEF0 / IDEF3	Functional/process modeling

Data-flow diagrams	Shows information movement
Context diagrams	Defines system boundaries
Interface control document (ICD)	Controls subsystem interfaces
Interface control drawing	Defines physical/functional interfaces
Interface definition document	Documents interface characteristics
System architecture framework	Organizes architecture views
Model-Based Systems Engineering (MBSE)	Uses models as integrated engineering artifacts
SysML	Systems modeling language
Digital engineering	Uses connected digital models and data
Digital thread	Maintains traceability across lifecycle data
Digital twin	Represents a system using connected data/models

C. Design, Analysis, and Trade Studies

Tool / artifact	**Purpose**
Trade study	Selects among competing alternatives
Decision analysis	Makes structured technical decisions
Engineering analysis	Evaluates system performance
Modeling and simulation	Predicts system behavior
Sensitivity analysis	Identifies influential parameters
Uncertainty analysis	Evaluates uncertainty in results
Margin analysis	Measures performance reserve
Mass budget	Tracks mass allocation
Power budget	Tracks power allocation
Energy budget	Tracks energy balance
Thermal analysis	Evaluates heat transfer and thermal limits
Structural analysis	Evaluates loads, stress, strain, and margins
Dynamic analysis	Evaluates vibration and dynamic response
Orbital analysis	Evaluates trajectories and orbital behavior
Radiation analysis	Evaluates radiation environment and effects
Reliability analysis	Evaluates failure behavior and dependability
Maintainability analysis	Evaluates maintenance burden
Availability analysis	Evaluates uptime and operational readiness
Cost analysis	Evaluates lifecycle cost
Schedule analysis	Evaluates timing and dependencies
Manufacturability analysis	Evaluates production feasibility
Human systems integration analysis	Integrates human capabilities and limitations

D. Verification, Validation, and Test

Tool / artifact	Purpose
Verification plan	Defines how requirements will be verified
Validation plan	Defines how intended use will be validated
Verification matrix	Tracks requirement verification
Validation matrix	Tracks validation evidence
Test requirements document	Defines test objectives and conditions
Test procedure	Defines test execution
Test report	Records test results
Inspection	Verifies characteristics through examination
Analysis	Verifies through calculations or modeling
Demonstration	Verifies through observed operation
Test	Verifies through controlled testing
Developmental test	Evaluates design maturity
Qualification test	Demonstrates design robustness under specified conditions
Acceptance test	Confirms delivered product meets requirements
Environmental test	Tests temperature, vibration, vacuum, etc.
Hardware-in-the-loop (HIL)	Tests hardware integrated with simulated environments
Software-in-the-loop (SIL)	Tests software in simulated environments
Model-in-the-loop (MIL)	Tests models before hardware implementation
Human-in-the-loop (HITL)	Tests human-system interaction
Integration and test (I&T)	Verifies integrated system behavior
Functional configuration audit (FCA)	Confirms functional requirements are met
Physical configuration audit (PCA)	Confirms physical product matches documentation
Readiness reviews	Evaluates readiness for major activities
Test as you fly / fly as you test	Ensures test conditions represent operational conditions where applicable

E. NASA Technical Reviews

NASA uses formal lifecycle reviews to assess technical maturity and readiness.

Common reviews include:

Review	General purpose
MCR — Mission Concept Review	Evaluates mission concept
SRR — System Requirements Review	Evaluates system requirements
SDR — System Definition Review	Evaluates system-level design definition

PDR — Preliminary Design Review	Evaluates preliminary design maturity
CDR — Critical Design Review	Evaluates detailed design readiness
SIR — System Integration Review	Evaluates readiness for integration
TRR — Test Readiness Review	Evaluates readiness for testing
ORR — Operational Readiness Review	Evaluates readiness for operations
FRR — Flight Readiness Review	Evaluates readiness for flight
SAR — System Acceptance Review	Evaluates acceptance of the system
PSR — Post-Ship Review	Reviews post-delivery status where applicable
DR — Decommissioning Review	Evaluates retirement/decommissioning readiness
DRR — Disposal Readiness Review	Evaluates readiness for disposal/end-of-life activities

The exact review set and terminology can vary by NASA program, mission class, and applicable directives.

F. NASA Risk, Safety, and Reliability

Tool / method	NASA relevance
FMEA / FMECA	Failure and criticality assessment
FTA	Top-event logic and hazardous-event analysis
ETA	Accident/outcome sequence analysis
PRA	Quantitative risk assessment
Hazard analysis	Identifies and controls hazards
Risk matrix	Communicates likelihood/consequence
Risk register	Tracks risks, owners, mitigations, and status
Critical items list (CIL)	Tracks critical hardware/items
Single-failure analysis	Evaluates single points of failure
Common-cause analysis	Evaluates shared failure causes
Failure tolerance analysis	Evaluates ability to tolerate failures
Fault management	Detects, isolates, and responds to faults
FDIR	Failure detection, isolation, and recovery
Hazard controls	Eliminates, reduces, or mitigates hazards
Safety verification	Demonstrates safety requirements are met
Probabilistic modeling	Quantifies uncertain risk
Reliability prediction	Estimates failure performance
Lessons learned	Captures prior failure knowledge
Independent technical assessment	Provides independent review of technical risk

NASA's FMECA guidance describes it as a living risk-assessment document that evolves as designs, materials, operating parameters, and knowledge develop. (**NASA Standards**)

---

13. Systems Engineering Used in Manufacturing

Manufacturing systems engineering is essentially **systems engineering applied to the production system**.

The system is not just the machine.

> **Product + Process + Equipment + Materials + Software + People + Facilities + Quality + Supply Chain + Maintenance + Information + Safety**

Manufacturing systems engineering domains

1. Product systems engineering

- Product requirements.
- Design requirements.
- Product architecture.
- Design for manufacturability.
- Design for assembly.
- Design for reliability.
- Design for testability.
- Configuration management.
- Product lifecycle management.
- Engineering change management.

2. Process systems engineering

- Process requirements.
- Process flow design.
- Process architecture.
- Process characterization.
- Process capability.
- Process windows.
- Process control.
- Process validation.
- Process qualification.
- Process integration.
- Process transfer.

3. Equipment systems engineering

- Equipment requirements.
- Equipment architecture.
- Equipment qualification.
- Equipment acceptance.
- Preventive maintenance.
- Predictive maintenance.
- Condition monitoring.
- Equipment reliability.
- Equipment availability.
- Fault detection and isolation.

- Spare-parts strategy.
- Maintenance strategy.
- Equipment lifecycle management.

4. Quality systems engineering

- Quality requirements.
- Control plans.
- PFMEA.
- Statistical process control.
- Measurement system analysis.
- Nonconformance management.
- CAPA.
- Corrective action.
- Preventive action.
- Supplier quality.
- Audit systems.
- Traceability.
- Change control.

5. Production systems engineering

- Capacity planning.
- Line balancing.
- Factory layout.
- Material flow.
- Work-in-process control.
- Bottleneck analysis.
- Throughput analysis.
- Cycle-time analysis.
- OEE.
- Production scheduling.
- Factory simulation.
- Yield improvement.
- Cost-of-poor-quality analysis.

6. Human and organizational systems engineering

- Job/task analysis.
- Training architecture.
- Qualification systems.
- Skills matrices.
- Human reliability.
- Ergonomics.
- Human-machine interfaces.
- Workload management.
- Shift handoff design.
- Standard work.
- Error-proofing.

- Safety culture.
- Organizational learning.

7. Digital manufacturing systems engineering

- MES architecture.
- SCADA integration.
- PLC/control systems.
- Industrial IoT.
- Equipment data collection.
- Manufacturing data models.
- Digital thread.
- Digital twin.
- Predictive analytics.
- AI-assisted fault detection.
- Cybersecurity.
- Data governance.
- Traceability systems.
- Manufacturing execution integration.

---

14. Manufacturing Frameworks Commonly Used Together

Framework	What it contributes
Lean Manufacturing	Waste reduction and flow
Six Sigma	Variation and defect reduction
Total Productive Maintenance (TPM)	Equipment effectiveness
Reliability-Centered Maintenance (RCM)	Maintenance based on failure consequences
Total Quality Management (TQM)	Organization-wide quality
Theory of Constraints (TOC)	Bottleneck and throughput optimization
Toyota Production System (TPS)	Flow, quality, standard work, continuous improvement
APQP	Advanced Product Quality Planning
PPAP	Production Part Approval Process
IATF 16949 practices	Automotive quality systems
ISO 9001	Quality management systems
ISO 45001	Occupational health and safety
ISO 14001	Environmental management
ISO 31000	Risk management principles
IEC 61508 concepts	Functional safety
SEMI standards	Semiconductor equipment and manufacturing interoperability
CMMI practices	Process maturity and improvement
MBSE	Model-based system definition and traceability

Digital manufacturing	Connected production information and models

Not every manufacturing company uses every framework. The appropriate combination depends on industry, product risk, regulatory requirements, and production maturity.

---

15. NASA vs. Manufacturing: What They Share

The environments differ, but the engineering logic is remarkably similar.

Engineering need	NASA	Semiconductor manufacturing
Define what must be achieved	Mission/system requirements	Product/process/equipment requirements
Break system into manageable parts	Functional decomposition	Process/equipment decomposition
Understand interactions	Architecture and interface management	Tool, recipe, material, facility, and MES interfaces
Predict failure	FMEA, FTA, PRA	FMEA, FTA, reliability analysis
Control hazards	Hazard analysis, safety controls	EHS, process safety, equipment safety
Verify performance	Test, analysis, inspection, demonstration	Qualification, SPC, process validation, equipment acceptance
Manage change	Configuration management	Engineering change control
Manage uncertainty	Risk management, margins, trade studies	Process windows, DOE, capability, risk analysis
Improve reliability	Design redundancy, fault tolerance, FDIR	PM, PdM, spares, fault detection, recovery
Learn from failure	Mishap investigation, lessons learned	RCA, CAPA, yield learning, corrective action
Optimize trade-offs	Decision analysis, trade studies	Cost/yield/throughput/reliability trade-offs
Improve systems	Technology development, TRIZ-like innovation methods	Process innovation, equipment improvement, TRIZ

NASA's handbook emphasizes that systems engineering applies across design, development, operation, maintenance, and closeout—not merely during initial design. (NASA)

---

16. The Most Powerful Combined Problem-Solving Stack

For a complex manufacturing, NASA, medical, or organizational problem, I would use the following hierarchy.

Level 1 — Understand the problem

1. Problem statement.
2. 5W1H.
3. Is / Is Not.
4. SIPOC.

5. Process map.
6. Stakeholder analysis.
7. Baseline data.

Level 2 — Understand how it can fail

8. Fishbone.
9. 5 Whys.
10. FMEA.
11. FTA.
12. Event Tree.
13. Hazard analysis.
14. Human factors analysis.

Level 3 — Verify the causes

15. Pareto.
16. Stratification.
17. SPC.
18. Measurement System Analysis.
19. DOE.
20. Evidence-based RCA.
21. Fault isolation.
22. Change analysis.

Level 4 — Create and select solutions

23. TRIZ.
24. Brainstorming.
25. Morphological analysis.
26. Pugh matrix.
27. Weighted trade study.
28. Cost-benefit analysis.
29. Risk-reduction analysis.
30. Prototype/simulation.

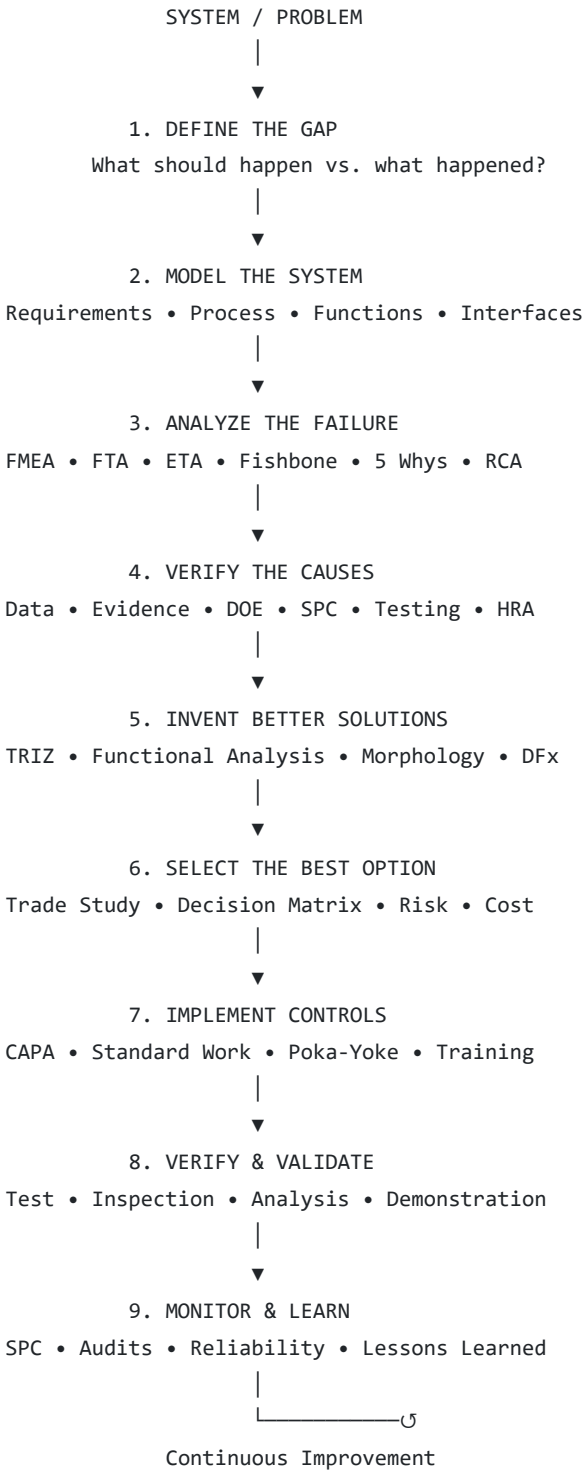
Level 5 — Implement and control

31. CAPA.
32. Standard work.
33. Poka-yoke.
34. Control plan.
35. Verification and validation.
36. Training and qualification.
37. Configuration management.
38. Monitoring and SPC.
39. Audit.
40. Lessons learned.

---

17. My Recommended “Master Problem-Solving Model”

If you want one reusable framework for almost any difficult problem, I would organize it as follows:



The key insight

FTA and FMEA tell you how a system can fail.

5 Whys and RCA investigate why a failure actually occurred.

TRIZ helps you invent a better way to solve the underlying contradiction.

SWOT helps you understand the strategic environment around the system.

Systems engineering connects all of these into a disciplined lifecycle.

---

18. What I Can Do for You Next

I can perform any of these as a full engineering exercise, including:

- **TRIZ analysis** of a CMP process, equipment problem, or training problem.
- **5 Whys** with evidence-based causal chains.
- **Full RCA** with causal factor chart, root causes, corrective actions, and verification.
- **SWOT** of a manufacturing department, new-hire training program, or business.
- **HAZOP** of a manufacturing process.
- **Bow-tie analysis** of a safety or operational hazard.
- **PRA** combining FTA and ETA.
- **DOE plan** for process optimization.
- **NASA-style systems engineering analysis** of a manufacturing system.
- **MBSE/SysML-style functional architecture** for a CMP tool or a medical office.
- **Integrated FMEA + FTA + ETA + RCA + TRIZ** for one problem.
- **A complete problem-solving curriculum** organized from beginner to NASA/manufacturing systems engineer.

My recommendation for your next experiment: Take the **"new CMP Technician 2 fails to become independently qualified within one year"** scenario and run **TRIZ + 5 Whys + RCA + HAZOP + systems engineering + SWOT** on it. That would let you compare *causal analysis, risk analysis, inventive improvement, organizational strategy, and lifecycle engineering* on the exact same system.

What is PRA combining FTA and ETA. Explain more.

Probabilistic Risk Assessment (PRA)

Combining Fault Tree Analysis and Event Tree Analysis

Probabilistic Risk Assessment (PRA) is a structured engineering method for estimating **how likely an undesired event is and what consequences may result**, using a combination of system models, failure data, human reliability, event probabilities, and uncertainty analysis.

The central idea is:

> **FTA asks: "What combinations of failures can cause the accident?"**
> **ETA asks: "Once an initiating event occurs, what happens next, depending on which safeguards succeed or fail?"**
> **PRA asks: "What is the probability of each resulting outcome, and how much risk does the system carry?"**

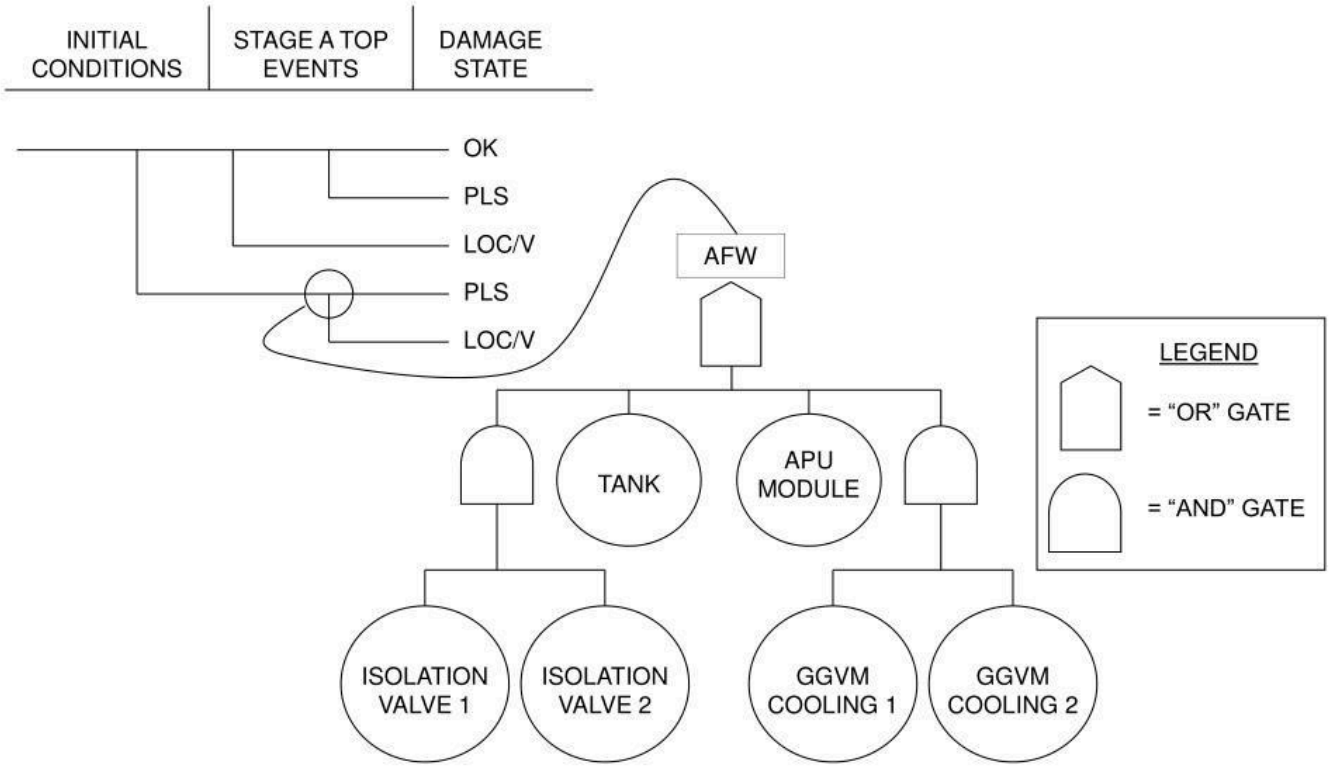
PRA is widely associated with nuclear, aerospace, chemical processing, defense, medical, and other high-consequence systems. NASA uses probabilistic risk methods as part of its broader safety and risk-management practices.

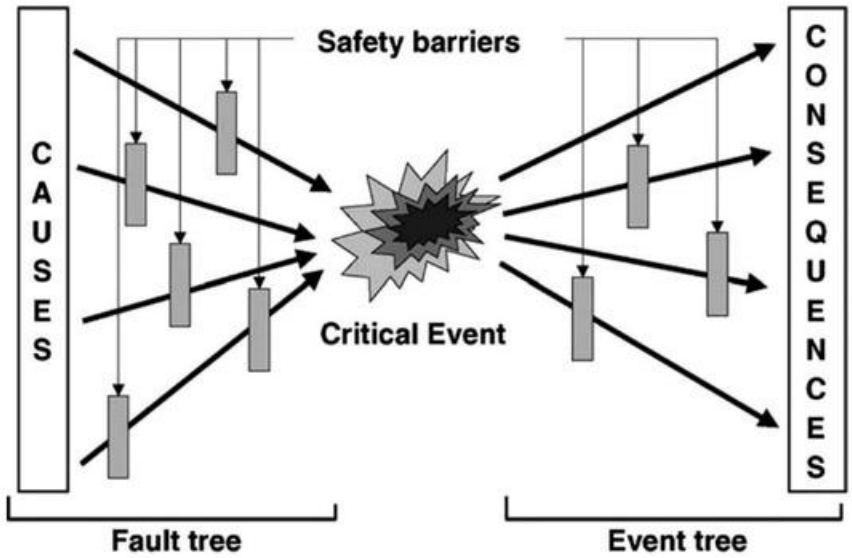
---

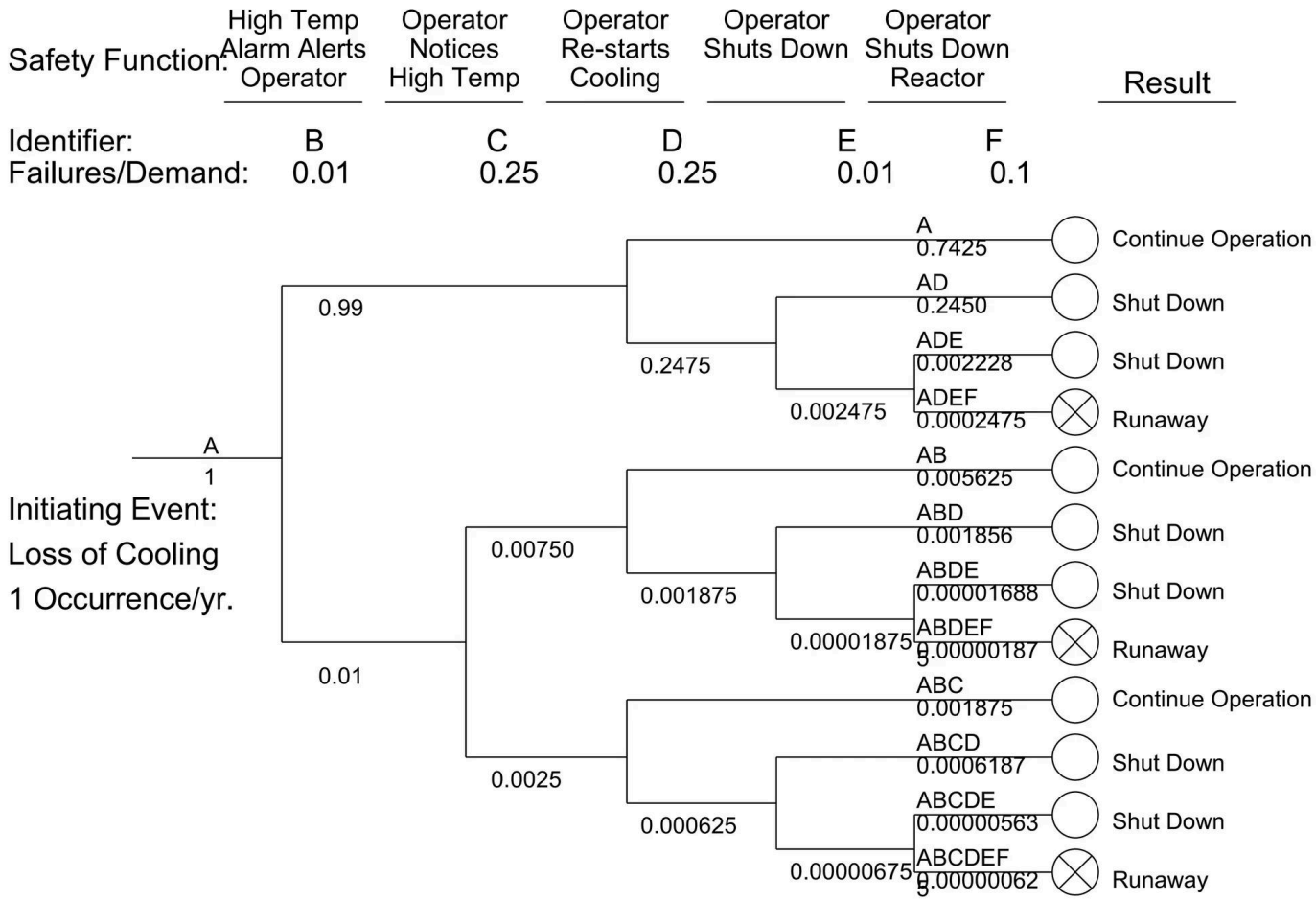
1. The Relationship: FTA + ETA + PRA

Think of the three methods as different views of the same system.

RELATIONSHIP OF FAULT TREES TO EVENT TREES





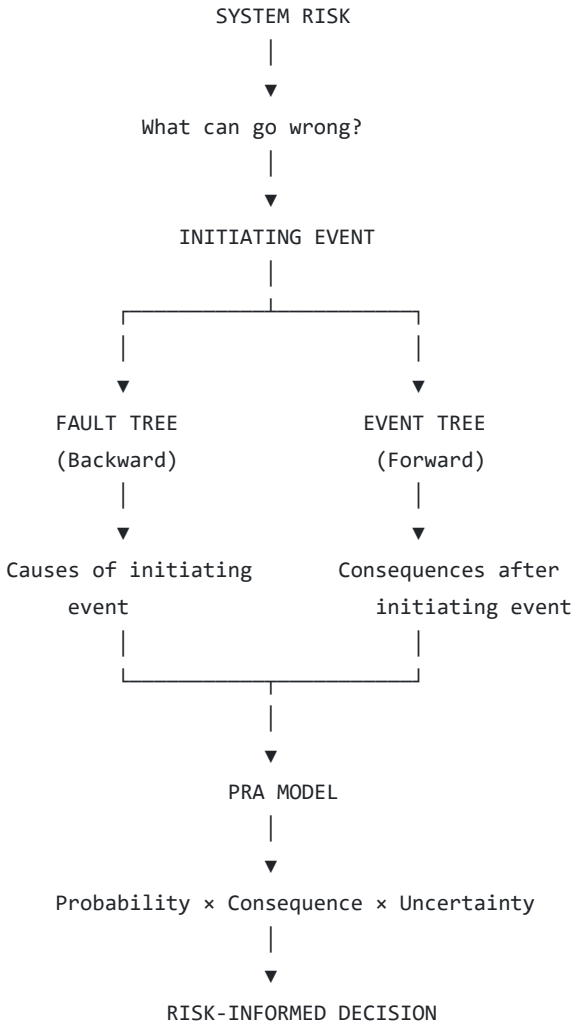


Shutdown = 0.2450 + 0.001856 + 0.00001688 + 0.0006187 = 0.2475 occurrences/yr.

Runaway = 0.0002475 + 0.000001875 + 0.000000625 = 0.0002500 occurrences/yr.

Figure 11-11 Event tree for the reactor of Figure 11-8. This includes a high temperature shutdown


the Risk Bowtie
Preventative Controls
HAZARD
Mitigating Controls
Cause
Cause
Cause
Cause
Cause
Cause
Control
Control
Control
Control
Control
Control
Risk Event
Control
Control
Control
Control
Control
Control
Consequence
Consequence
Consequence
Consequence
Consequence
Consequence
Escalation Factor
Escalation Factor


SYSTEM RISK
What can go wrong?
INITIATING EVENT
FAULT TREE
(Backward)
EVENT TREE
(Forward)
Causes of initiating event
Consequences after initiating event
PRA MODEL
Probability × Consequence × Uncertainty
RISK-INFORMED DECISION

A simple analogy

Imagine a spacecraft has a potential **loss-of-vehicle event**.

- **FTA:** What combinations of propulsion, guidance, power, software, or human failures could lead to loss of vehicle?
- **ETA:** If an initiating failure occurs, does the backup system work? Does the crew respond? Does the vehicle recover?
- **PRA:** What is the calculated probability of each outcome, such as safe recovery, mission loss, or catastrophic loss?

---

2. What Exactly Is “Risk” in PRA?

A simplified engineering expression is:

Risk=∑iPi×Ci\text{Risk} = \sum_i P_i \times C_i

Where:

- PiP_i = probability of outcome ii
- CiC_i = consequence or severity associated with outcome ii

For multiple outcomes:

R=P(Outcome 1)C1+P(Outcome 2)C2+⋯+P(Outcome n)CnR = P(\text{Outcome 1})C_1 + P(\text{Outcome 2})C_2 + \cdots + P(\text{Outcome n})C_n

However, **risk is not always reducible to one number**. In aerospace and safety engineering, teams often retain separate measures for:

- Probability of catastrophic event.
- Probability of mission loss.
- Probability of injury or fatality.
- Probability of equipment damage.
- Expected loss.
- Uncertainty bounds.
- Risk contributors.

A low-probability catastrophic event may deserve more attention than a frequent, low-consequence nuisance.

---

3. FTA: The “How Can It Start?” Side

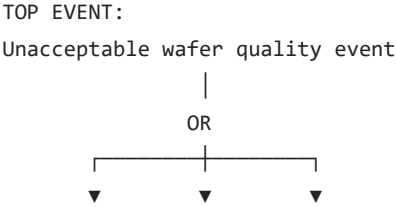
Fault Tree Analysis is deductive

FTA begins with a defined **top event** and works backward.

Example top event

> **Top Event: CMP Tool Causes an Unacceptable Wafer Quality Event**

This is a hypothetical training model, not a claim about a specific Samsung tool.



```
Over-polish  Under-    Contamination
             polish       event
```

Then decompose one branch:

```
OVER-POLISH
     |
    AND
  ┌──┴──────────────┐
  ▼                 ▼
Removal rate      Control failure
exceeds target    fails to detect/
                  correct deviation
```

Continue:

```
CONTROL FAILURE
     |
    OR
  ┌──┼──────────┐
  ▼  ▼          ▼
Sensor  Recipe    Operator/
failure mismatch  system error
```

FTA uses logical gates:

Gate	Meaning
OR	Any listed event can cause the output
AND	Multiple events must occur together
NOT / Inhibit	Conditions prevent or enable a path
Priority AND	Events must occur in a specific order
Transfer	Links to another fault tree

FTA output

FTA produces:

- Causal structure.
- Minimal cut sets.
- Single-point failure identification.
- Common-cause failure candidates.
- Potential probability calculations.
- Critical contributors to the top event.

Example minimal cut set

A minimal cut set is a combination of basic events sufficient to produce the top event.

```
{Sensor failure + alarm failure}
```

Or:

```
{Incorrect recipe + missing verification}
```

The exact cut sets depend on the tree's logic.

---

4. ETA: The “What Happens Next?” Side

Event Tree Analysis is inductive

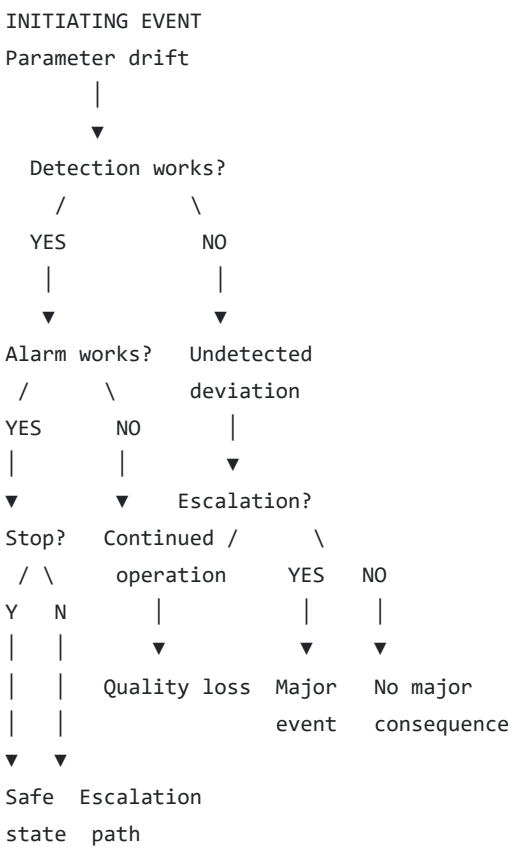
ETA starts with an **initiating event** and follows possible paths depending on whether safety functions succeed or fail.

Example initiating event

> **Initiating Event: CMP process parameter drifts outside the intended operating window.**

Possible barriers:

1. Sensor detects drift.
2. Alarm activates.
3. Tool stops or enters a safe state.
4. Technician responds correctly.
5. Verification confirms recovery.



An actual ETA would be drawn with mutually exclusive branches and clearly defined end states.

ETA output

- Possible accident sequences.
- Success/failure paths.
- Barrier effectiveness.
- Consequence categories.
- Probability of each outcome.
- Identification of weak or missing safeguards.

---

5. How FTA and ETA Combine

The most important connection is this:

> **FTA estimates or structures the probability of the initiating event. ETA distributes that initiating-event probability across the possible consequences.**

Simplified mathematical structure

Suppose:

- $P(I)$ = probability of initiating event.
- $P(B_1)$ = probability the first barrier succeeds.
- $P(B_2)$ = probability the second barrier succeeds.
- $P(B_3)$ = probability the third barrier succeeds.

For a particular event-tree path:

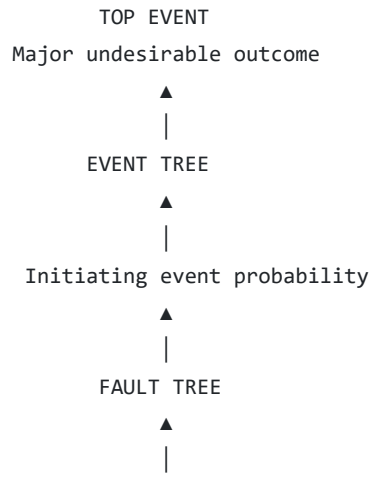
$$P(\text{Path}) = P(I) \times P(B_1 \text{ outcome}) \times P(B_2 \text{ outcome}) \times P(B_3 \text{ outcome})$$

For example:

$$P(\text{Major consequence}) = P(I) \times P(\text{detection failure}) \times P(\text{shutdown failure}) \times P(\text{recovery failure})$$

This multiplication is valid only when the probability model appropriately handles dependencies. Real systems often have common-cause failures, conditional probabilities, time dependencies, and shared resources.

The integrated model



```
Basic component / human /
  software / environment
      failure data
```

---

6. A Complete PRA Example: Hypothetical CMP Equipment Incident

Let's construct a simplified example.

Scenario

A CMP tool experiences a process-control deviation that could lead to a quality excursion.

Objective

Estimate the relative probability of:

- **A. Normal recovery**
- **B. Contained quality excursion**
- **C. Significant production impact**
- **D. Severe equipment/process consequence**

These numbers are illustrative only. They are not Samsung data, actual CMP probabilities, or validated semiconductor reliability estimates.

Step 1 — Define the initiating event

> **I: A critical process parameter deviates beyond its allowable operating range.**

Suppose a hypothetical model estimates:

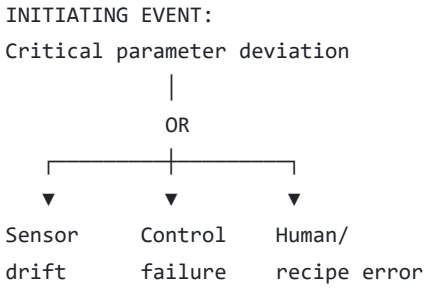
$P(I)=0.001 \text{ per operating cycle}$P(I) = 0.001 \text{ per operating cycle}

That means a **0.1% initiating-event probability per defined cycle**, purely for illustration.

The time basis matters enormously. “Per cycle,” “per wafer,” “per lot,” and “per operating hour” are not interchangeable.

Step 2 — FTA estimates the initiating event

We might model:



For illustration, suppose the estimated contributions are:

Basic cause	Illustrative probability contribution
Sensor drift	0.0003
Control-loop fault	0.0002
Incorrect parameter configuration	0.0003
Other causes	0.0002
Total initiating event	**0.0010**

Caution: These values cannot simply be added in real PRA unless the events are mutually exclusive or the model properly accounts for overlap. A real FTA would use Boolean logic and dependency handling.

Step 3 — Build the event tree

After the deviation begins, consider three barriers:

- **B1:** Detection and alarm.
- **B2:** Automatic safe response.
- **B3:** Correct human recovery and verification.

Illustrative conditional probabilities:

Barrier	Success probability	Failure probability
B1: Detection/alarm	0.98	0.02
B2: Automatic safe response	0.95	0.05
B3: Recovery/verification	0.99	0.01

Again, these are **hypothetical values**.

Event tree paths

Path	Detection	Safe response	Recovery	Outcome
1	Success	Success	Success	Normal recovery
2	Success	Success	Failure	Contained issue
3	Success	Failure	Success	Contained or limited excursion
4	Success	Failure	Failure	Significant quality impact
5	Failure	—	—	Potentially undetected escalation

The dash indicates that downstream barriers may not operate as modeled because the initiating deviation was not detected.

---

7. Calculate the Illustrative Path Probabilities

Path 1 — Detection, safe response, and recovery succeed

P1=0.001×0.98×0.95×0.99P_1 = 0.001 \times 0.98 \times 0.95 \times 0.99P1=0.00092169P_1 = 0.00092169

So:

P1≈9.22×10−4P_1 \approx 9.22 \times 10^{-4}

Path 2 — Detection and safe response succeed, recovery fails

P2=0.001×0.98×0.95×0.01P_2 = 0.001 \times 0.98 \times 0.95 \times 0.01P2=0.00000931P_2 = 0.00000931

Path 3 — Detection succeeds, safe response fails, recovery succeeds

P3=0.001×0.98×0.05×0.99P_3 = 0.001 \times 0.98 \times 0.05 \times 0.99P3=0.00004851P_3 = 0.00004851

Path 4 — Detection succeeds, safe response fails, recovery fails

P4=0.001×0.98×0.05×0.01P_4 = 0.001 \times 0.98 \times 0.05 \times 0.01P4=0.00000049P_4 = 0.00000049

Path 5 — Detection fails

P5=0.001×0.02P_5 = 0.001 \times 0.02P5=0.00002P_5 = 0.00002

The paths should sum to the initiating-event probability if the tree is complete and mutually exclusive:

P1+P2+P3+P4+P5=0.001P_1+P_2+P_3+P_4+P_5=0.001

That is a basic consistency check.

---

8. What Did We Learn?

Even in this tiny model:

Finding 1 — Most initiating events may be contained

The majority of modeled initiating events end in normal recovery or a limited consequence.

Finding 2 — Detection is a powerful risk barrier

A small detection-failure probability can create a disproportionately important risk path if undetected deviations can escalate.

Finding 3 — Automatic response and human recovery are different barriers

They should not be treated as the same control.

- Automatic control may stop the process.
- Human recovery may diagnose the problem.
- Verification may confirm that the system is safe to resume.

Finding 4 — Risk is a system property

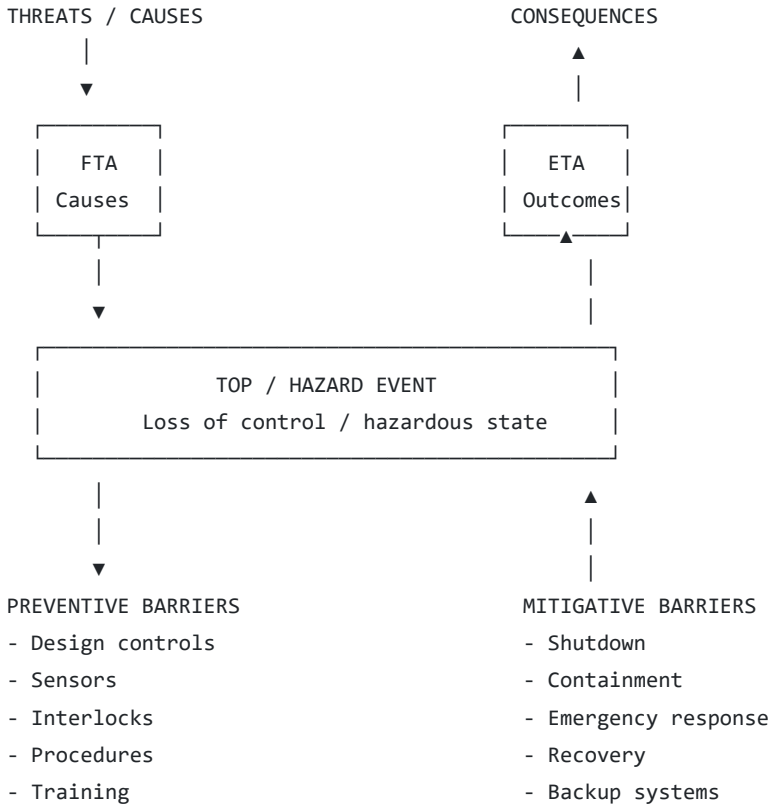
The initiating failure alone does not determine the final consequence.

> **The outcome depends on the initiating failure, the barriers, the environment, the timing, the human response, and the system's ability to recover.**

---

9. The “Bow-Tie” Connection

A **bow-tie analysis** is often the easiest visual bridge between FTA and ETA.



Bow-tie terminology

Side	Meaning
Threats	Conditions or failures that can initiate the hazardous event
Top event / Hazardous event	Loss of control or transition into a hazardous state
Preventive barriers	Stop the initiating causes from reaching the top event
Mitigative barriers	Reduce the consequences after the top event
Consequences	What happens if barriers fail or succeed

FTA is on the left. ETA is on the right.

Bow-tie is often more communicative for operations and safety teams, while PRA adds quantitative probability and uncertainty.

---

10. PRA Is More Than Just Multiplying Probabilities

A professional PRA can become very sophisticated.

A. Reliability data

PRA may use:

- Component failure rates.
- Repair rates.
- Mission duration.
- Operating hours.
- Environmental conditions.
- Historical incident data.
- Test data.
- Supplier reliability data.
- Expert elicitation.
- Bayesian updating.
- Reliability growth data.

B. Human reliability

For systems involving technicians, operators, pilots, or medical personnel:

- Probability of omission.
- Probability of incorrect action.
- Time available for response.
- Alarm detectability.
- Training and experience.
- Workload.
- Fatigue.
- Procedure usability.
- Recovery opportunity.
- Human-machine interface design.

Methods may include:

- **THERP**
- **HEART**
- **SPAR-H**
- **CREAM**
- **ATHEANA**
- **Human error probability modeling**

These methods have different assumptions and applicability.

C. Common-cause failures

This is one of the most important PRA complications.

Suppose a system has two redundant sensors.

A naive model might say:

> Sensor A fails AND Sensor B fails.

But what if both sensors lose power from the same supply?

Or both are affected by:

- Shared software.
- Shared calibration error.

- Shared environmental condition.
- Common maintenance mistake.
- Common communication network.
- Common design defect.

Then redundancy may not provide the expected protection.

PRA must account for dependencies and common-cause failures.

D. Uncertainty analysis

PRA results are not exact predictions.

A result might be represented as:

P(catastrophic event)=2×10−5P(\text{catastrophic event}) = 2 \times 10^{-5}

But the underlying inputs may be uncertain.

A more honest statement might be:

> The modeled mean probability is 2×10−52 \times 10^{-5}, with a substantial uncertainty range due to limited failure data, dependency assumptions, and model uncertainty.

Common techniques:

- Monte Carlo simulation.
- Latin hypercube sampling.
- Sensitivity analysis.
- Parameter uncertainty analysis.
- Model uncertainty analysis.
- Bayesian methods.
- Importance sampling for rare events.

---

11. PRA Terms You Should Know

Term	Meaning
Initiating event	Event that starts an accident or undesired sequence
Top event	Defined undesirable event in an FTA
Basic event	Lowest-level modeled cause in an FTA
Intermediate event	Event formed from lower-level logic
Minimal cut set	Smallest combination of events sufficient to cause the top event
Event sequence	Ordered progression from initiating event to outcome
Barrier	Function that prevents, detects, controls, or mitigates an event
Success path	Event-tree path where required functions succeed
Failure path	Event-tree path where one or more functions fail
Common-cause failure	Multiple components fail due to one shared cause

Common-mode failure	Often used similarly; terminology varies by discipline
Mission success probability	Probability of achieving defined mission objectives
Loss of mission	Failure to achieve required mission objectives
Loss of vehicle	Defined vehicle-level failure outcome
Conditional probability	Probability of an event given another event
Unavailability	Probability a system is not available when needed
Reliability	Probability of performing required function for a specified time
Risk contributor	Cause or sequence contributing materially to total risk
Risk importance	Measure of how much a component or event influences risk
Risk-informed decision	Decision that considers probabilistic risk alongside other factors

---

12. Importance Measures: Where Should We Improve First?

PRA becomes especially useful when you ask:

> **"Which improvement gives us the greatest reduction in risk?"**

Common importance measures include:

Measure	General purpose
Fussell–Vesely importance	How much total risk involves a component/event
Risk Achievement Worth (RAW)	How much risk increases if a component is unavailable
Birnbaum importance	Sensitivity of system reliability to component reliability
Criticality importance	Identifies components strongly associated with system failure
Risk reduction worth	Potential benefit of improving a component
Sensitivity analysis	Shows which assumptions most affect results

Example

Suppose a PRA shows:

Potential improvement	Estimated risk reduction
Improve sensor reliability	10%
Improve alarm detection	35%
Improve automatic shutdown	20%
Improve recovery procedure	5%
Add redundant power supply	25%

The best investment may not be the most obvious component.

The highest-risk contributor is not always the component with the highest individual failure rate.

---

13. PRA Versus FMEA, FTA, ETA, and RCA

Tool	Primary purpose	Typical direction	Quantitative?
FMEA	Explore failure modes and effects	Bottom-up	Usually qualitative/semi-quantitative
FTA	Analyze causes of a defined top event	Top-down/backward	Can be quantitative
ETA	Analyze consequences after initiating event	Forward	Can be quantitative
RCA	Investigate an actual failure	Backward from evidence	Usually evidence-based, may use statistics
HAZOP	Identify hazards from process deviations	Structured guidewords	Usually qualitative/semi-quantitative
Bow-tie	Show causes, barriers, and consequences	Both directions	Usually qualitative; can be quantitative
PRA	Estimate probabilities and risk across event sequences	Integrated	**Yes, often probabilistic**
TRIZ	Generate inventive solutions	Contradiction → solution	Not primarily probabilistic

---

14. NASA Application: A Simplified Spacecraft Example

A NASA-style PRA might examine:

> **Top concern: Probability of loss of mission due to a critical spacecraft subsystem failure.**

FTA side

Potential causes:

- Power subsystem failure.
- Guidance/navigation failure.
- Propulsion failure.
- Thermal-control failure.
- Software fault.
- Communication failure.
- Human operations error.
- Common-cause environmental event.

ETA side

After an initiating failure:

1. Fault detected?
2. Fault isolated?
3. Backup available?
4. Backup operates?
5. Ground/crew response successful?

6. Vehicle remains within safe operating limits?
7. Mission objectives remain achievable?

Possible outcomes

- Full mission success.
- Partial mission success.
- Mission degradation.
- Safe recovery but mission loss.
- Loss of vehicle.
- Catastrophic outcome.

What PRA adds

It estimates the probability of each outcome and identifies the dominant risk contributors.

For a real NASA program, the actual model would depend on the mission, system architecture, applicable safety requirements, available data, and program-specific PRA methodology.

---

15. Manufacturing Application: A More Useful PRA Structure

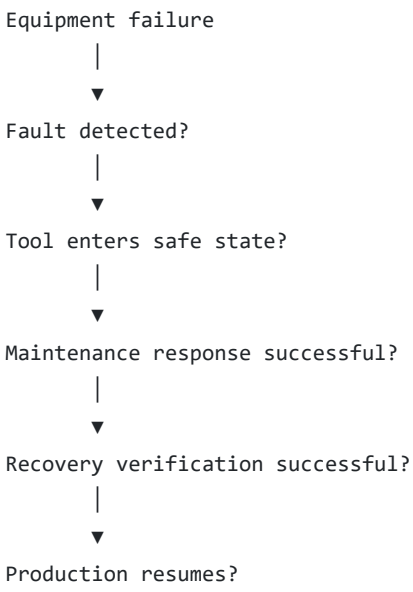
For a semiconductor manufacturing environment, PRA can be applied at several levels.

A. Equipment PRA

Question:

> What is the probability that an equipment failure causes a significant production consequence?

Model:



Potential consequences:

- No production impact.
- Short downtime.
- Extended downtime.

- Wafer scrap.
- Lot loss.
- Equipment damage.
- Safety incident.

B. Process PRA

Question:

> What is the probability that a process deviation escapes detection and causes a significant quality event?**

Potential barriers:

- In-process monitoring.
- Sensor validation.
- Alarm system.
- SPC.
- Recipe controls.
- Interlocks.
- Operator response.
- Metrology.
- Lot disposition.
- Corrective action.

C. Human-performance PRA

Question:

> What is the probability that a critical task is performed incorrectly and the error propagates to a significant consequence?**

Potential factors:

- Procedure clarity.
- Training.
- Qualification.
- Time pressure.
- Shift handoff.
- Alarm design.
- Workload.
- Task complexity.
- Supervision.
- Error detection.
- Recovery opportunity.

This is particularly relevant to your **CMP Technician 2** training model.

---

16. PRA for Your CMP Technician 2 Scenario

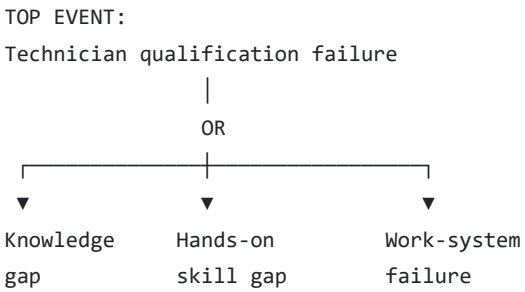
Let's frame a hypothetical PRA.

Top concern

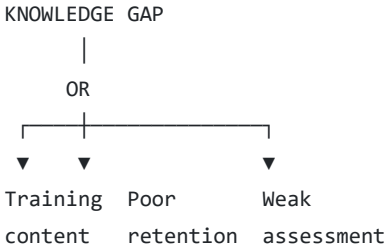
> **A new CMP Technician 2 is unable to perform assigned work safely, correctly, and independently within the expected qualification period, resulting in operational, quality, safety, or personnel consequences.**

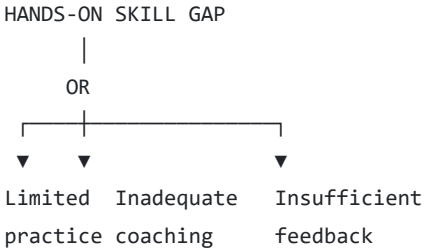
This is not a conventional equipment PRA. It is a **human-performance and organizational systems PRA**.

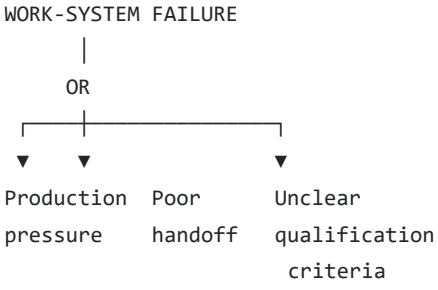
FTA: Why might the undesirable outcome begin?



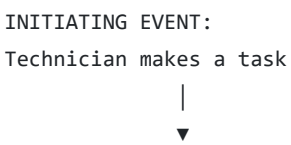
Expand:

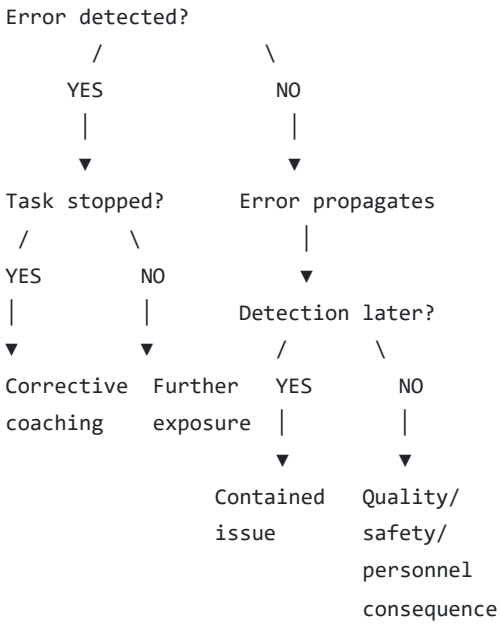






ETA: What happens after a performance gap appears?





PRA questions

- How often do critical task errors occur?
- Which errors are most likely to escape detection?
- Which tasks have the highest consequence?
- Which barriers are preventive?
- Which barriers are detective?
- How effective is supervision?
- How quickly is feedback provided?
- What is the probability of recovery?
- Which training investment reduces risk most?
- Does qualification certification actually predict independent performance?

The powerful insight

A training program should not be evaluated only by:

> "Did the technician complete the training?"

It should be evaluated by:

> **"What is the probability that the technician can perform critical tasks correctly, detect abnormal conditions, respond appropriately, and prevent errors from propagating?"**

That is a PRA-style way of thinking.

---

17. PRA and the Hierarchy of Controls

PRA also helps prioritize controls.

Control type	Example in manufacturing
Elimination	Remove a hazardous task or unnecessary manual step
Substitution	Replace a hazardous process/material with a safer alternative

Engineering controls	Interlocks, automation, sensors, physical safeguards
Administrative controls	Procedures, training, checklists, qualification
PPE	Personal protective equipment

A useful PRA insight is:

> **Controls that depend less on perfect human performance are often more robust, especially when the consequence of failure is high.**

That does not mean training is unimportant. It means training should be complemented by:

- Error-proofing.
- Automation.
- Interlocks.
- Clear alarms.
- Independent verification.
- Standard work.
- Well-designed recovery procedures.

---

18. How PRA Differs from "Just Assigning Risk Scores"

A common misconception is:

> "We have an FMEA RPN score, so we have PRA."

Not necessarily.

FMEA risk score

Often:

$$RPN = S \times O \times D$$

Where:

- SS = Severity.
- OO = Occurrence.
- DD = Detection.

This is a **prioritization score**.

PRA

PRA attempts to model:

- Actual or estimated probabilities.
- Event sequences.
- Conditional dependencies.
- Barrier success/failure.
- Consequence probabilities.
- Uncertainty.
- System interactions.

RPN is not the same as a probability of catastrophic failure.

A high RPN does not automatically mean high PRA risk, and a low RPN does not automatically mean negligible risk.

19. When Should You Use PRA?

PRA is most useful when:

- Consequences are significant.
- Failures interact in complex ways.
- Redundancy and barriers matter.
- Probabilities can be estimated.
- You need to compare risk-reduction options.
- You need to understand rare but severe events.
- You need to justify design or safety investments.
- You need to evaluate system-level risk rather than isolated component risk.

It may be excessive for:

- A simple one-step administrative issue.
- A low-consequence problem with an obvious cause.
- A problem where there is no meaningful probability data and only a qualitative assessment is needed.

In those cases, 5 Whys, RCA, FMEA, or a simple decision matrix may be more appropriate.

---

20. A Practical PRA Workflow

Here is a reusable workflow I can execute with you.

Phase 1 — Define

1. Define the system.
2. Define the mission or operational objective.
3. Define the undesired outcomes.
4. Define the analysis boundary.
5. Define the time basis.
6. Define the risk metrics.

Phase 2 — Build the model

7. Identify initiating events.
8. Construct fault trees.
9. Identify basic events.
10. Identify event-tree barriers.
11. Define success and failure paths.
12. Identify dependencies and common-cause failures.

Phase 3 — Quantify

13. Gather failure data.
14. Estimate event probabilities.
15. Estimate barrier success probabilities.
16. Assign consequence categories.
17. Calculate sequence probabilities.
18. Sum outcome probabilities.

19. Perform uncertainty analysis.
20. Perform sensitivity and importance analysis.

Phase 4 — Improve

21. Identify dominant risk contributors.
22. Develop corrective actions.
23. Apply TRIZ for inventive risk reduction.
24. Compare alternatives using trade studies.
25. Verify that proposed controls actually reduce risk.

Phase 5 — Maintain

26. Update the model after design or process changes.
27. Incorporate incident and reliability data.
28. Reassess assumptions.
29. Track risk-reduction effectiveness.
30. Preserve lessons learned.

---

21. The Most Important Mental Model

The deepest difference is this:

FTA asks:

> **"What must fail for this event to occur?"**

ETA asks:

> **"Given that the event occurs, what happens depending on which defenses work?"**

PRA asks:

> **"Across all credible paths, how likely are the outcomes, how severe are they, and where should we invest to reduce risk?"**

RCA asks:

> **"Why did the actual event happen, and what must change to prevent recurrence?"**

TRIZ asks:

> **"How can we redesign the system to eliminate the contradiction or failure mechanism?"**

Final takeaway

PRA is the quantitative bridge between reliability analysis and consequence analysis.

It combines:

> **FTA = Causes**
> **ETA = Consequences**
> **Probability models = Likelihood**
> **Consequence models = Severity**
> **Uncertainty analysis = Confidence and limits**

> **Importance analysis = Where to improve**
> **Risk-informed decisions = What to do next**

For your engineering experiments, I would consider **PRA the next level after FTA and ETA**—especially when you want to move from *"Here are the ways the system can fail"* to *"Here is the estimated likelihood of each outcome, the dominant risk contributor, and the most effective control."*