Process Safety Analysis Toolkit

How the Tools Fit Together

Overview for facilitators, engineers and course delegates · version 1.0 · October 2026

1 Purpose

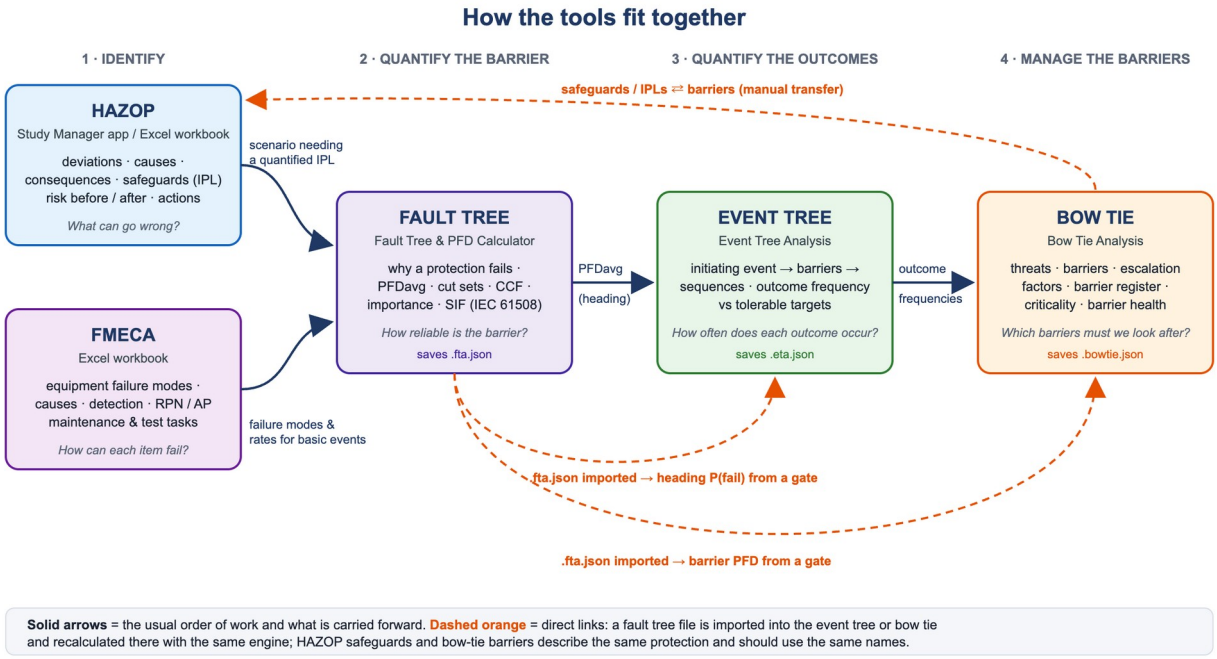
The toolkit contains four offline applications – **HAZOP Study Manager**, **Fault Tree & PFD Calculator**, **Event Tree Analysis** and **Bow Tie Analysis** – plus the **HAZOP and FMECA Excel workbooks** and the **HAZOP guidewords reference**. Each tool answers a different question. Used together they take a hazard from first identification to a quantified, managed set of barriers.

This document explains what each tool is for, how information moves between them, how to choose the right tool, and follows one scenario – a fire on the hot DRI conveyor – through all of them with consistent numbers. Detailed instructions are in each tool's built-in user guide and in the Guides folder.

2 The tools at a glance

Tool	Format	Question it answers	Main outputs
HAZOP Study Manager	Offline app .hazop.json	What can go wrong, why, and what protects us?	Deviations, causes, consequences, safeguards with IPL claims, risk before / after, recommendations register, report
HAZOP Study Workbook	Excel .xlsx / .xlsm	The same, for teams that work in Excel	PSI register, node list, one worksheet per node, 5 × 5 risk matrix
HAZOP guidewords reference	Word / PDF	Which deviations and causes should we consider?	Parameter – deviation – potential causes for chemical and steel & metals plants
FMECA Workbook	Excel .xlsx / .xlsm	How can each equipment item fail, and how critical is it?	Failure modes, causes, detection, RPN and Action Priority, maintenance and test tasks
Fault Tree & PFD Calculator	Offline app .fta.json	How likely is a protection system – or an event – to fail?	Exact PFDavg, top-event frequency, minimal cut sets, importance, uncertainty, IEC 61508 SIF calculator
Event Tree Analysis	Offline app .eta.json	After an initiating event, how often does each outcome happen?	Sequence and consequence-category frequencies against tolerable targets, sensitivity, uncertainty
Bow Tie Analysis	Offline app .bowtie.json	Which barriers control the hazard, how good are they, which are critical?	Bow-tie diagram, barrier register (owner, performance standard, verification, status), risk ranking, barrier criticality

3 How the tools fit together



The work normally moves through four stages. Not every scenario needs every stage – most HAZOP findings are closed qualitatively; only the high-risk or IPL-dependent ones are taken further.

Stage 1 – Identify (HAZOP, FMECA)

- **HAZOP** (app or workbook, prompted by the guidewords reference) works through the process node by node and finds deviations, their causes and consequences, the existing safeguards and a first risk ranking. It produces recommendations, among them “quantify this protection” where a high risk depends on an engineered or instrumented safeguard.
- **FMECA** works at equipment level: how each item can fail, how the failure is detected and how critical it is. It sets maintenance and test priorities and supplies the failure modes, rates and test intervals that fault trees need.

Stage 2 – Quantify the barrier (fault tree)

- A **fault tree** explains why a protection system fails on demand – sensors, logic, valves, utilities, human actions, common-cause failures – and calculates its **PFDavg** exactly, including redundancy, voting, shared equipment and proof-test intervals. The **SIF calculator** gives the IEC 61508-6 formula result for standard architectures for comparison.
- With an initiating-event frequency at the top, the same tool gives the frequency of the undesired event.

Stage 3 – Quantify the outcomes (event tree)

- An **event tree** starts from the initiating event and follows the barriers in time order (restart, ignition, suppression, fire fighting, containment …) to every outcome. Each outcome gets a frequency and is compared with the tolerable frequency for its consequence category. A heading can take its failure probability directly from a fault-tree gate.

Stage 4 – Manage the barriers (bow tie)

- The **bow tie** puts all threats, barriers and consequences for one hazard on one page – the view operations and management use. Its **barrier register** gives every barrier an owner, a performance standard, a verification activity and a status, and the **condition view** shows the risk actually being run when barriers are degraded or out of service. The criticality analysis identifies safety-critical elements.

4 What moves between the tools

From	To	What	How
HAZOP	Fault tree	Scenario (top event), the safeguard to be quantified, cause frequencies	Manual. Put the HAZOP deviation reference (e.g. N01-01) in the fault-tree title or notes.
FMECA	Fault tree	Failure modes as basic events; failure rates; detection (λDU / λDD split); proof-test interval	Manual. Use the same equipment tags in both.
Fault tree	Event tree	Failure probability of a heading = PFDavg of a gate	**Automatic:** File ▸ Import fault tree; set the heading source to “fault tree” and choose the gate.
Fault tree	Bow tie	PFD of a barrier = PFDavg of a gate	**Automatic:** File ▸ Import fault tree; set the barrier’s PFD source to “fault tree gate”.
Event tree	Bow tie	Threat frequency, conditional probabilities, consequence categories and targets	Manual. Keep the same values in both (the example shows how).
HAZOP	Bow tie	Safeguards / IPLs ⇄ barriers; recommendations ⇄ barrier improvements	Manual. Use the same barrier names and tags.
Bow tie	FMECA / HAZOP	Safety-critical barriers and their status → maintenance priority, close-out of recommendations	Manual. Mark SCE equipment in the FMECA; review impaired barriers in HAZOP revalidation.

Imported fault trees are stored inside the event-tree and bow-tie files and recalculated with the same engine, so the numbers always agree. After changing a fault tree, use “Replace with newer version” on the Fault tree links tab.

5 Choosing the right tool

If you need to …	Use
Find hazards and deviations systematically in a process design or modification	HAZOP Study Manager or HAZOP Study Workbook, with the guidewords reference
Set maintenance, inspection and test priorities for equipment	FMECA Workbook
Show whether a SIF or protection system meets its PFD / SIL target, and why it fails	Fault Tree & PFD Calculator (SIF calculator tab for standard architectures)
Find the frequency of an undesired event from its causes	Fault Tree & PFD Calculator with an initiating-event frequency
Know how often an event escalates to each outcome and compare with tolerable frequencies	Event Tree Analysis
Explain the barriers to operations, assign barrier owners, judge an impaired barrier	Bow Tie Analysis
Do a quick LOPA-style check of one scenario	Bow Tie (one threat and one consequence line) or an event tree with two or three headings

6 One scenario through all the tools – hot DRI conveyor fire

The examples in the toolkit share one scenario so that the results can be compared: the enclosed hot DRI transfer conveyor trips or stops while loaded, the stationary hot DRI can self-heat and ignite the belt, and an automatic nitrogen inerting / extinguishing system protects the conveyor. **All data are illustrative.**

6.1 HAZOP – identify

The HAZOP example study (File ▸ Load example study, or Examples/Example - Hot DRI transfer conveyor.hazop.json) covers two nodes: **N01 the hot DRI transfer conveyor** (shaft discharge to the EAF charging bin) and **N02 the N2 fire detection, inerting & extinguishing system**. Seven deviations are recorded, among them:

- **N01-01 No flow – conveyor stopped under load** (about 6 per year): stationary hot DRI self-heats, belt fire, possible spread to the transfer tower / silo. Safeguards: restart / emergency discharge, the N2 system XS-210 (claimed as IPL), manual fire fighting, fire separation of the gallery (IPL). Risk Very High before and still High after safeguards → recommendation R-001 to quantify the N2 system and the escalation, R-002 emergency discharge without power, R-003 review fire separation.
- **N01-02 More hot DRI temperature**, **N01-03 water / air ingress**, **N01-04 fines accumulation** – with a recommendation to confirm the design DRI discharge temperature and belt rating.
- **N02-01 No N2 flow on demand**, **N02-02 loss of N2 supply** and **N02-03 N2 leak / release into the enclosure** (asphyxiation – a hazard introduced by the protection itself).

R-001 is where the quantitative tools take over.

6.2 FMECA – equipment failure modes and maintenance

The FMECA workbook example (Workbooks folder, .xlsx or .xlsm) has two systems that mirror the HAZOP nodes: **S01 hot DRI transfer conveyor** (HAZOP N01) and **S02 N2 fire detection, inerting & extinguishing system** (HAZOP N02). Its equipment register holds 15 items with the same tags as the fault tree and bow tie – CV-201, M-201, GB-201, SS-201, WT-201, TSHH-202, DC-203, V-212, PCV-211, XV-210A/B, GD-201A/B, PSL-205 and UCP-210 – and the tag drop-down on each system sheet lists only that system's items. Two example rows show the method:

Item	Failure mode / causes	S · O · D → RPN	Action Priority	Recommended action (after action)
CV-201 belt (S01, HAZOP N01-01)	STD – belt tear / damage overheating, abrasive wear, incorrect maintenance	7 · 5 · 6 → **210**	M action required (RPN ≥ 125)	Monthly belt thermography and cover-thickness measurement; confirm the belt temperature rating against the design DRI discharge temperature (HAZOP R-004) → 7 · 4 · 3 = 84
XV-210A actuator (S02, HAZOP N02-01)	FTO – fail to open on demand sticking / seizure, contamination, dust ingress	9 · 4 · 8 → **288**	**H**	Six-monthly staggered function test, partial-stroke where possible; model as a fault-tree basic event with CCF β = 10 % → 9 · 3 · 5 = 135 (M)

- **FMECA → fault tree:** the N2-system rows become basic events of the fault tree (XV-210A/B fail to open, PCV-211 fails closed, nozzles blocked by fines, GD-201A/B fail to detect), with the failure rates, detection (λDU / λDD split) and proof-test intervals the FMECA records.
- **Read the two together:** the FMECA ranks XV-210A highest (Action Priority H), but the fault tree shows the release valves are only about 5 % of the N2 system's failure probability (Fussell-Vesely 0.045 for their common cause). Testing them every six months instead of yearly halves the valve contribution ($1.5 \times 10^{-3} \rightarrow 7.0 \times 10^{-4}$) yet lowers the N2 system PFDavg only from 0.0285 to 0.0278. The bigger gains are in enclosure sealing, the regulator PCV-211 and nozzle blockage – the FMECA should give those items equal attention.
- **FMECA → HAZOP:** the belt row closes the loop on HAZOP recommendation R-004 (confirm DRI discharge temperature and belt rating); the HAZOP ref column links each failure mode to its deviation.

6.3 Fault tree – quantify the N2 system

- Gate **G-002 "N2 system fails to inert / extinguish on demand": PFDavg ≈ 0.029** (risk reduction factor ≈ 35, SIL 1 band).
- With 6 trips under load per year and a 0.05 chance of fire developing, the uncontrolled-fire frequency is **≈ 8.6 × 10^{-3} /yr**.
- Dominant cut sets: enclosure not sealed, regulator fails closed, nozzles blocked by fines, isolation valve left closed, system left isolated – detection and initiation are not the weak point.

6.4 Event tree – quantify the outcomes

- 6 /yr × restart fails (0.25) × ignition (0.2) = **0.30 fires /yr**; the N2 heading takes 0.029 directly from gate G-002.
- Fire spreads to the transfer tower / silo (C5): **1.7 × 10^{-4} /yr**, above the illustrative tolerable 10^{-4} /yr by a factor of about 1.7.
- Fire not extinguished by N2 (C3 + C4 + C5) = **8.56 × 10^{-3} /yr** – the same as the fault-tree result.

6.5 Bow tie – manage the barriers

- Five threats; top event **≈ 0.31 /yr**, of which 0.30 /yr comes from trips under load – the same as the event tree.
- The N2 system is one shared barrier on two consequences, linked to gate G-002; its failure would raise the major-fire frequency about 35-fold, so it is a **safety-critical element** with escalation factors (low N2 pressure, enclosure doors open) and their controls.
- The bow tie also shows a hazard introduced by the barrier itself – **asphyxiation after N2 release** (≈ 1.5 × 10^{-4} /yr) – which needs its own barriers.

6.6 The numbers agree

Quantity	Fault tree	Event tree	Bow tie
N2 system PFDavg	0.0285 (gate G-002)	0.0285 (linked)	0.0285 (linked)
Fires per year after trips under load	input: 6 /yr × 0.05	0.30 /yr	0.30 /yr (of 0.31 total)
Fire not extinguished by N2	8.56 × 10^{-3} /yr	8.56 × 10^{-3} /yr (C3+C4+C5)	–
Major gallery fire or worse	–	1.71 × 10^{-3} /yr (C4+C5)	1.75 × 10^{-3} /yr *
Fire spreads to transfer tower / silo	–	1.71 × 10^{-4} /yr	1.75 × 10^{-4} /yr *

** The bow tie is slightly higher because it also includes the four smaller threats (over-temperature DRI, friction, hot work, fines accumulation).*

6.7 What it tells management

- Most of the risk comes from **trips under load** – fewer stoppages, or a faster restart / emergency discharge that works without power, reduce every fire outcome.
- The **N2 system is the key barrier**; its weak points are in the delivery path, not the detection – enclosure sealing, the regulator and nozzle blockage need inspection, testing and possibly redundancy.
- The **spread scenario exceeds the illustrative target** – options are better fire separation of the gallery, a more reliable N2 delivery path, or both; the event-tree sensitivity table shows the effect of each.
- The N2 system introduces an **asphyxiation hazard** that needs release warning, access lock-out and O2 checks before entry.

7 Working with the files

Tool	File type	Example in the Examples folder
HAZOP Study Manager	.hazop.json	Example - Hot DRI transfer conveyor.hazop.json
Fault Tree & PFD Calculator	.fta.json	Example - Hot DRI conveyor N2 fire protection.fta.json
Event Tree Analysis	.eta.json	Example - Hot DRI conveyor fire.eta.json (contains the fault tree)
Bow Tie Analysis	.bowtie.json	Example - Hot DRI conveyor fire.bowtie.json (contains the fault tree)
HAZOP / FMECA workbooks	.xlsx / .xlsm	Workbooks folder – example rows for the hot DRI transfer conveyor (N01 / S01) and the N2 system (N02 / S02)

- Save studies in **My studies** with **File ▸ Save as… (link file)** – every change is then written to the file on the stick. Browser storage stays on each computer.
- Name files consistently, for example **Unit_Scenario_Tool_v1** (e.g. DRI-Conveyor_Fire_FT_v2.fta.json), and keep the version that was used in an event tree or bow tie.
- When a fault tree changes, replace it in the event tree and bow tie (Fault tree links ▸ Replace with newer version) so all three show the same PFD.

8 Good practice for consistent models

- Use the **same names and tags** for equipment, safeguards and barriers in all tools.
- **Avoid double counting:** link the event-tree heading or bow-tie barrier to the protection-system gate (e.g. G-002), not to a fault-tree top event that already contains the initiating event.
- **Watch dependencies:** barriers that share equipment (power, control panel, operator) are not independent. Model the shared item in one fault tree, or use a branch-specific probability in the event tree.
- Credit a barrier only if it is effective on its own, independent of the cause and of the other barriers, and auditable.
- Record **data sources and assumptions** in the notes fields; run the sensitivity and uncertainty analyses on the dominant inputs.
- Review every model with operations and maintenance, and keep barrier status current.

9 Limitations

- All example data are illustrative – replace them with site, vendor and plant-history data before use.
- The fault tree gives PFDavg only; hardware fault tolerance, safe failure fraction and systematic capability (IEC 61508 / 61511) must be checked separately for a SIL claim.
- Event-tree headings and bow-tie barriers are treated as independent unless you model the dependency.
- The tools support analysis, training and design comparison. Confirm SIL verification and risk decisions with your organisation’s approved methods and tools.

10 Where to find more

- **Guides folder** – user guides for each tool (PDF); each tool also has its guide built in (User guide tab).
- **Reference folder** – HAZOP guidewords, deviations and potential causes for the chemical and steel & metals industries.
- **START HERE.html** and **READ ME FIRST.txt** – starting the tools and saving work on the USB stick.