Configuration Risk Management

Tutorial

John Weglian
Principal Technical Leader

July 23, 2026
PSAM 2026

About the Instructor

- Project Manager for CAFTA, Phoenix Risk Monitor, and HRA Calculator
- Been with EPRI for 11 years
- Worked as a PRA engineer for FirstEnergy for 7 years supporting the Perry Nuclear Power Plant
- Worked in aerospace (Lockheed Martin, Ohio Aerospace supporting NASA GRC, and FAA)
- Nuclear submarine officer on the USS Tucson

Configuration Risk Management (CRM)

- Configuration Risk Management is the process of assessing and responding to risk as the plant configuration changes
- Changes may be due to:
  - Planned maintenance
  - Routine surveillance tests
  - Emergent conditions/corrective maintenance
  - Changes in the environment
  - Changes in operational mode

When is CRM Beneficial?

- CRM can be beneficial to companies with
  - Redundant systems, especially when redundancy can be reduced during maintenance or testing
  - Accident mitigation relying on diversity and/or redundancy for safety
  - Risk can be quantified with fault tree analysis
  - Risk can be qualitatively assessed with decision trees assessing safety functions
- CRM allows companies to make good risk decisions when risk is elevated

History of CRM in the Nuclear Industry

Background – U.S. Commercial Nuclear Power

- Safety-related components can only be out of service for a limited amount of time (regulatory requirement)
- U.S. plants will intentionally take components out of service during this period to perform maintenance
- The Maintenance Rule regulation in the U.S. (10 CFR 50.65) requires utilities to assess the risk prior to taking components out of service for maintenance
- Utilities use a Configuration Risk Management (CRM) PRA model to make this risk assessment

Effect of the Maintenance Rule

- The combination of the Maintenance Rule and on-line maintenance had a profound effect on the U.S. nuclear industry
- Utilities focused attention on poor performing systems
  - Equipment performance improved
- Capacity factors rose, allowing the companies to sell more electricity (improved economics)
  - Unplanned outages were reduced
  - The use of online maintenance allowed for shorter refueling outages
- PRA models began to be used on a daily basis

Terminology

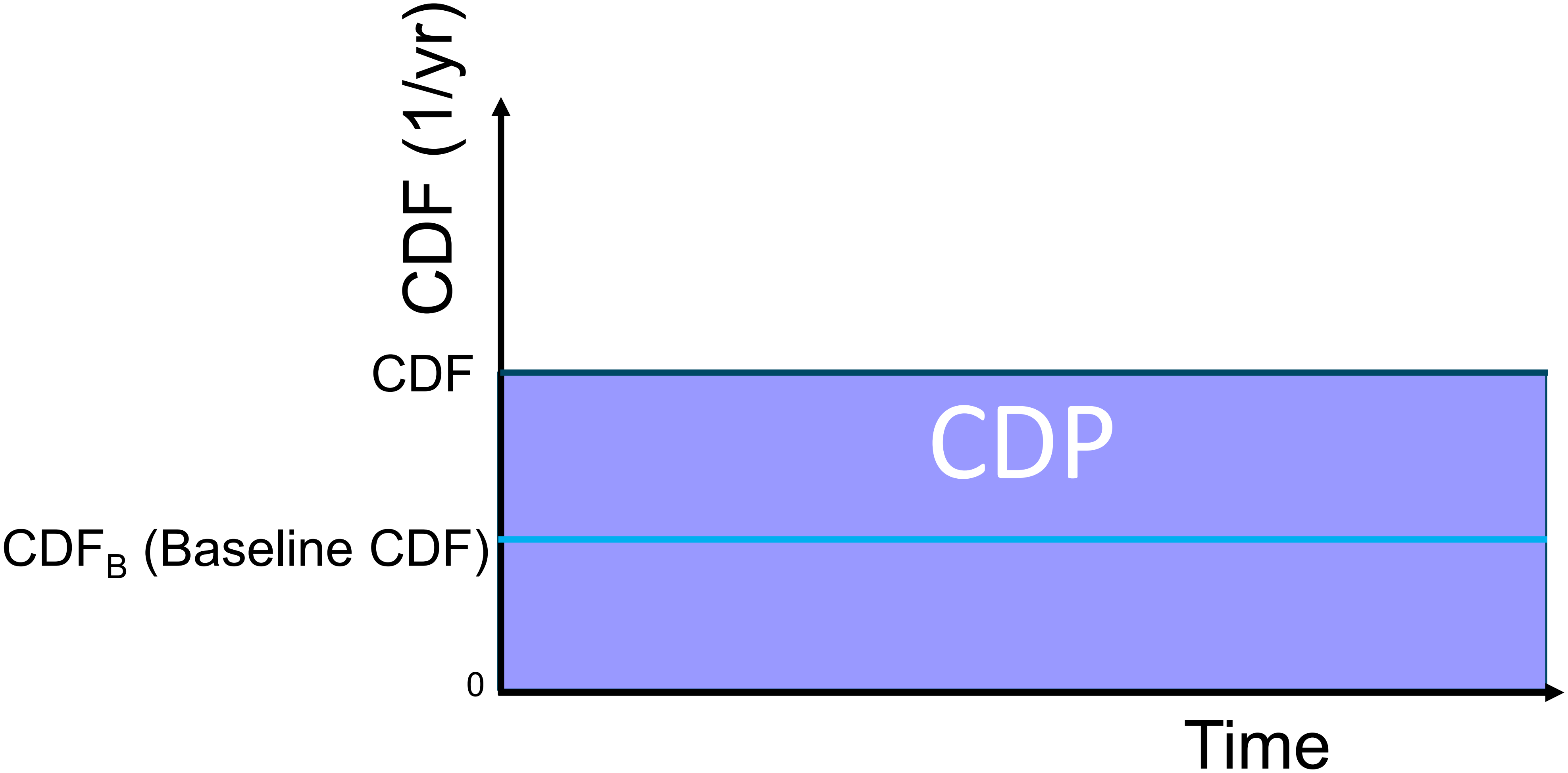
Terminology (Nuclear Example)

- Core Damage Frequency (CDF) – Significant melting of nuclear fuel

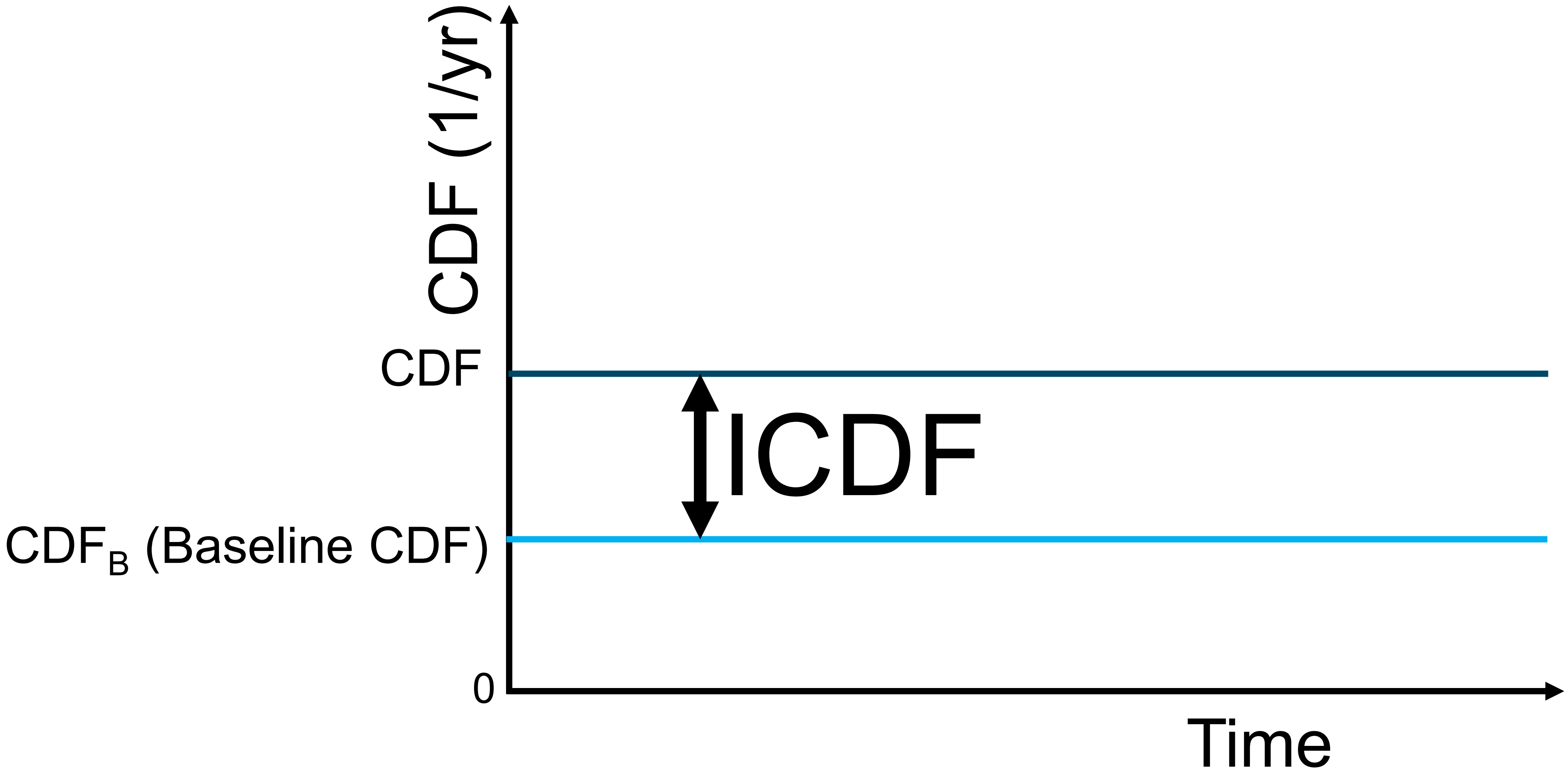
- Plant Risk Factor (PRF) = CDF/CDF_B – can be used in risk monitors as a risk metric

- Risk Metric equations:
  - Core Damage Probability (CDP) = $CDF*\Delta t$
  - Incremental Core Damage Frequency (ICDF) = $CDF - CDF_B$
  - Incremental Core Damage Probability = $ICDF*\Delta t$

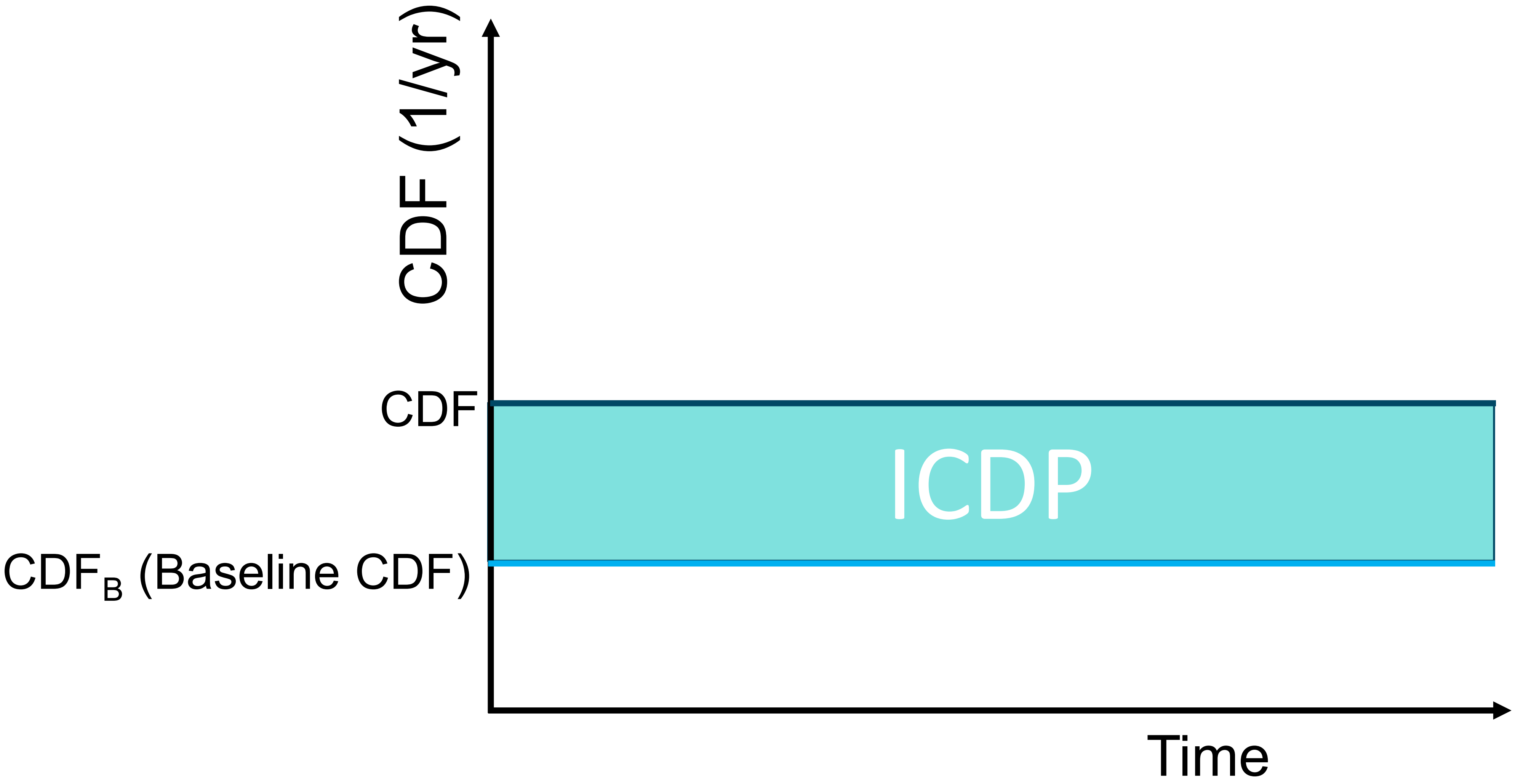
Core Damage Probability



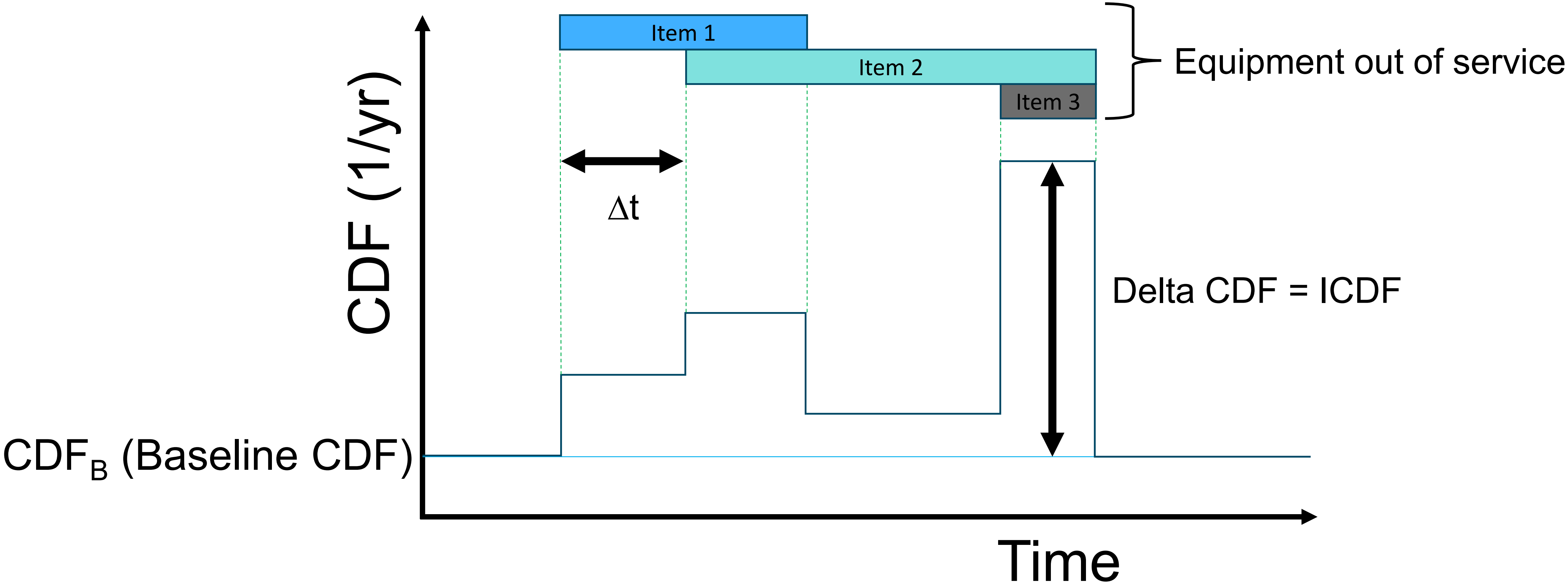
Incremental Core Damage Frequency



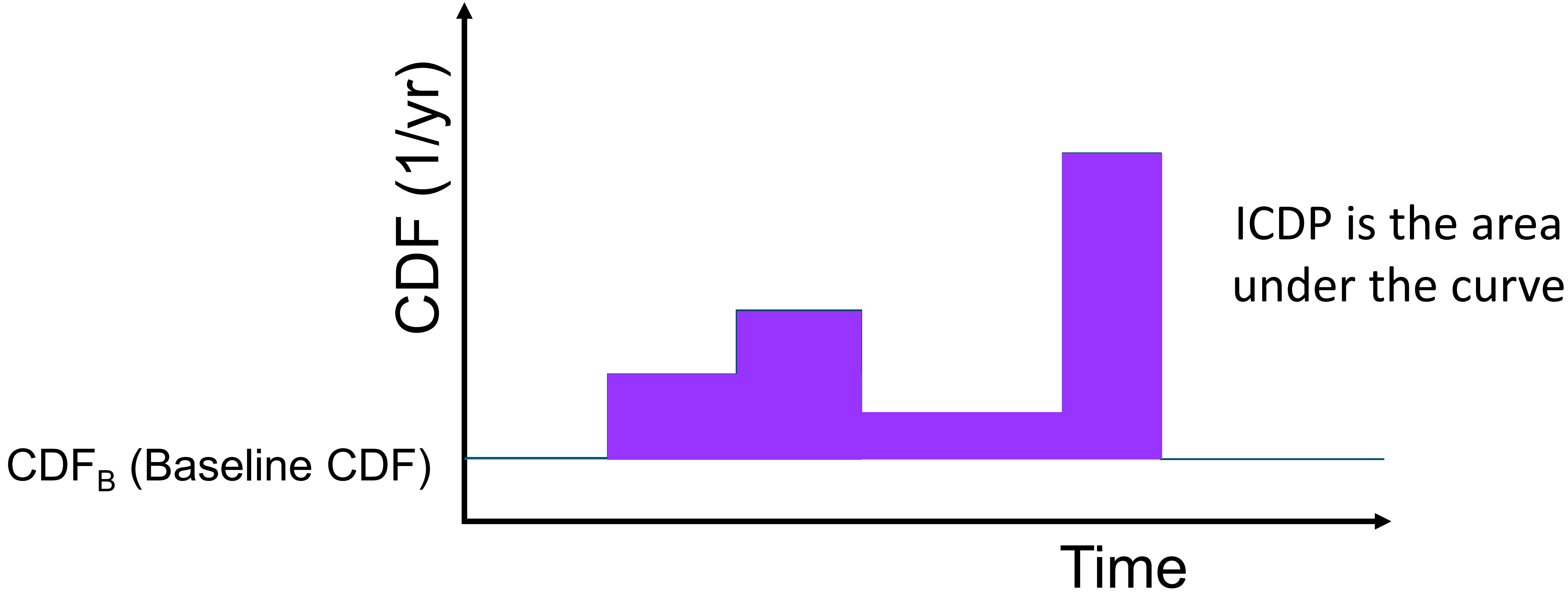
Incremental Core Damage Probability



Configuration Risk



ICDP With Multiple Configurations



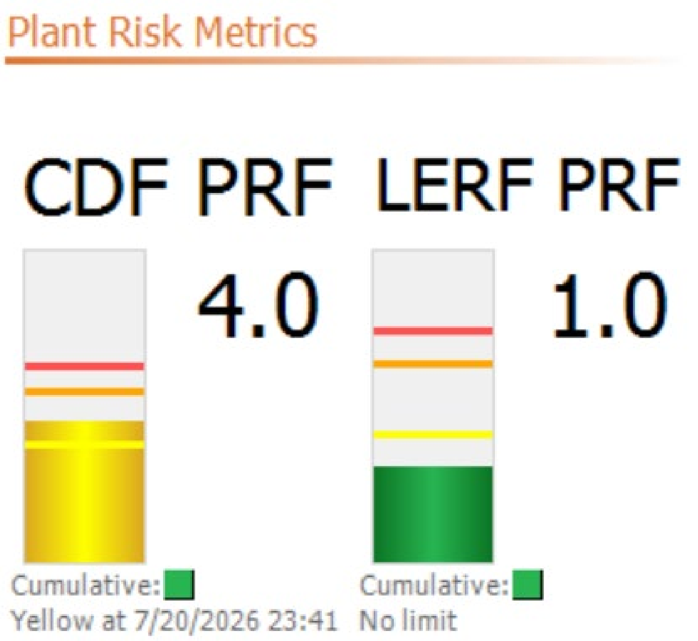
Assigning Risk Thresholds

Risk Thresholds

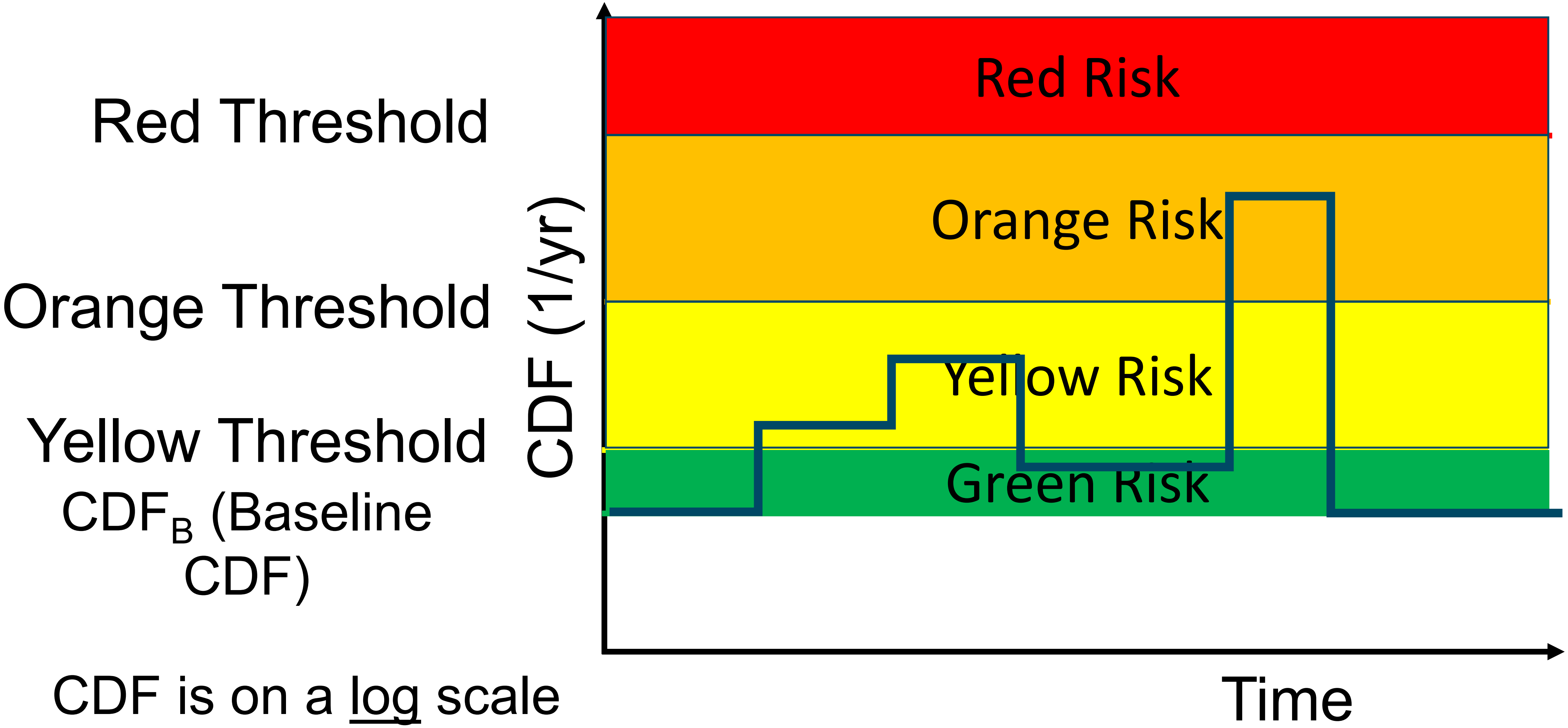
- Risk thresholds are often defined to require specific actions to be taken when a threshold is exceeded
- In the nuclear industry, these are a set of colors based on the risk
  - Green: Normal work controls
  - Yellow: Enhanced sensitivity to risk, some risk management actions implemented
  - Orange: Significant sensitivity to risk, more risk management actions implemented
  - Red: Never entered voluntarily, risk is carefully controlled until risk can be reduced or the plant shut down

Instantaneous Risk

- The simplest risk thresholds are based on instantaneous risk
- When the risk of a new configuration exceeds a threshold, the plant enters the new color and takes the appropriate actions
- Risk thresholds can be set as multiples of base risk
  - Yellow = 2 times base risk
  - Orange = 10 times base risk
  - Red = 20 times base risk
- Problem: If you improve plant safety and base risk goes down, it becomes easier to hit a risk threshold



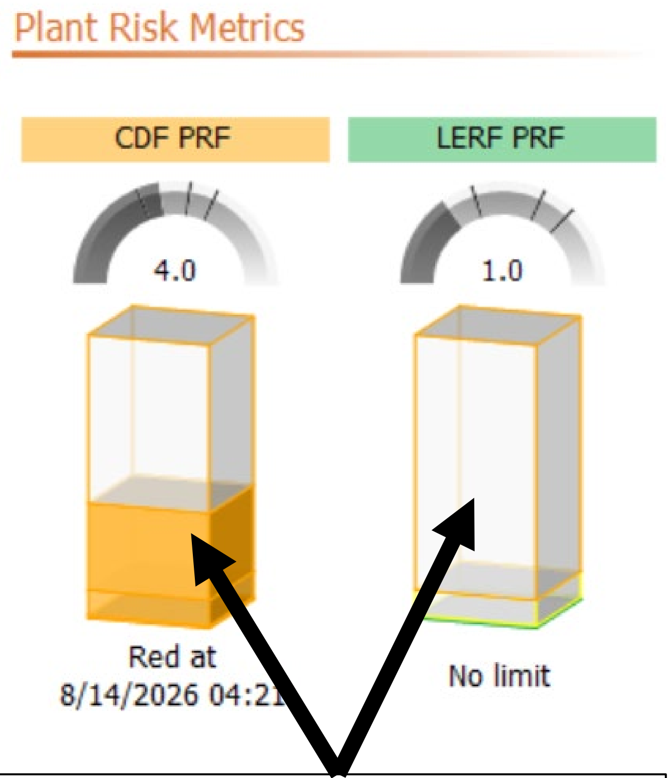
Instantaneous Risk Thresholds



CDF is on a <u>log</u> scale

Cumulative Risk

- Risk is based on the integral of the increased (delta) risk over time
- Risk considers the time in a configuration in addition to the actual (instantaneous) risk value
- Typical risk thresholds in nuclear (CDF):
  - Yellow = ICDP > 1E-6
  - Orange = ICDP > 5e-6
  - Red = ICDP > 1E-5
- Many nuclear utilities are shifting to the use of cumulative risk metrics



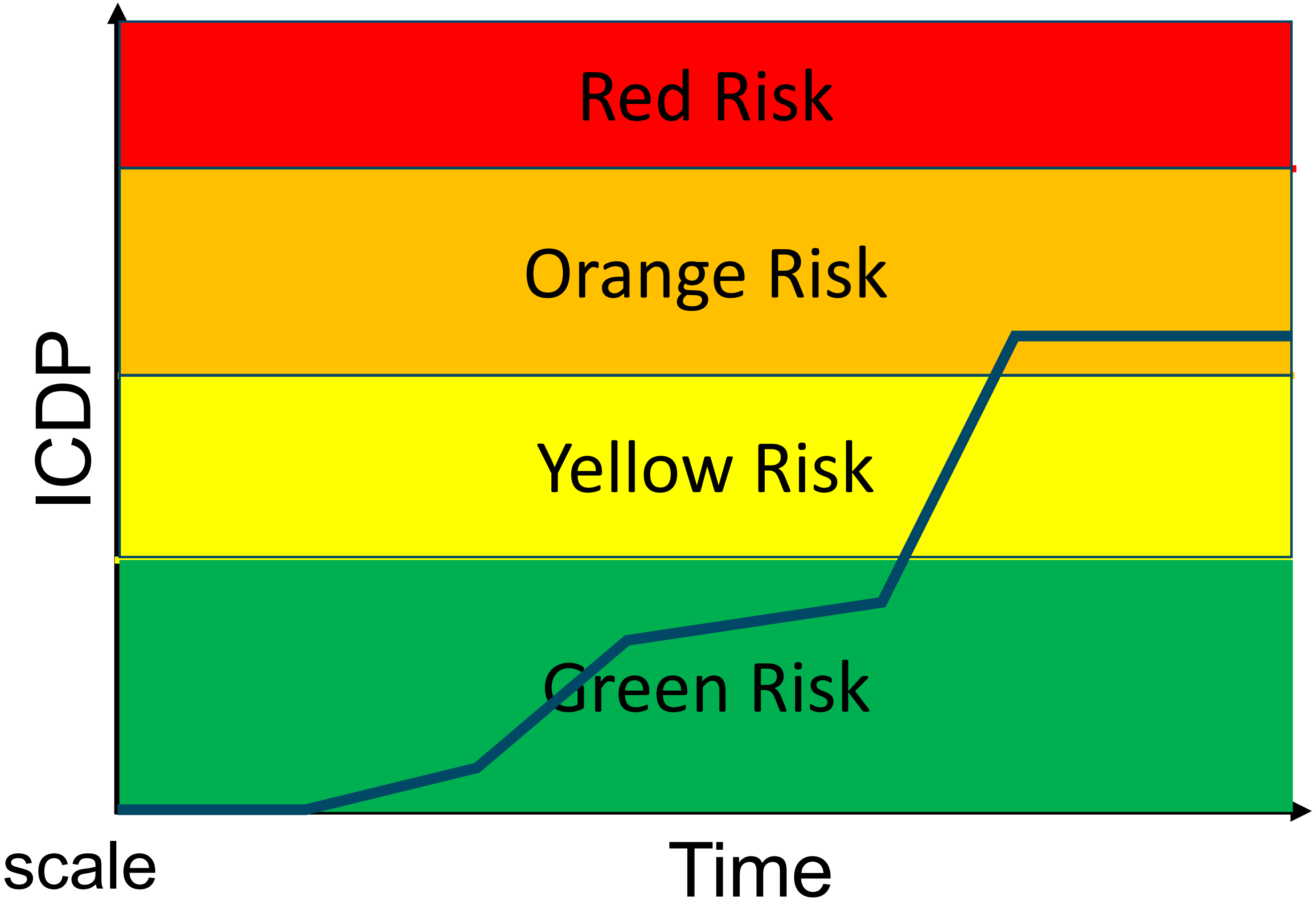
These act like tanks that fill up over time

Cumulative Risk Thresholds

Red Threshold

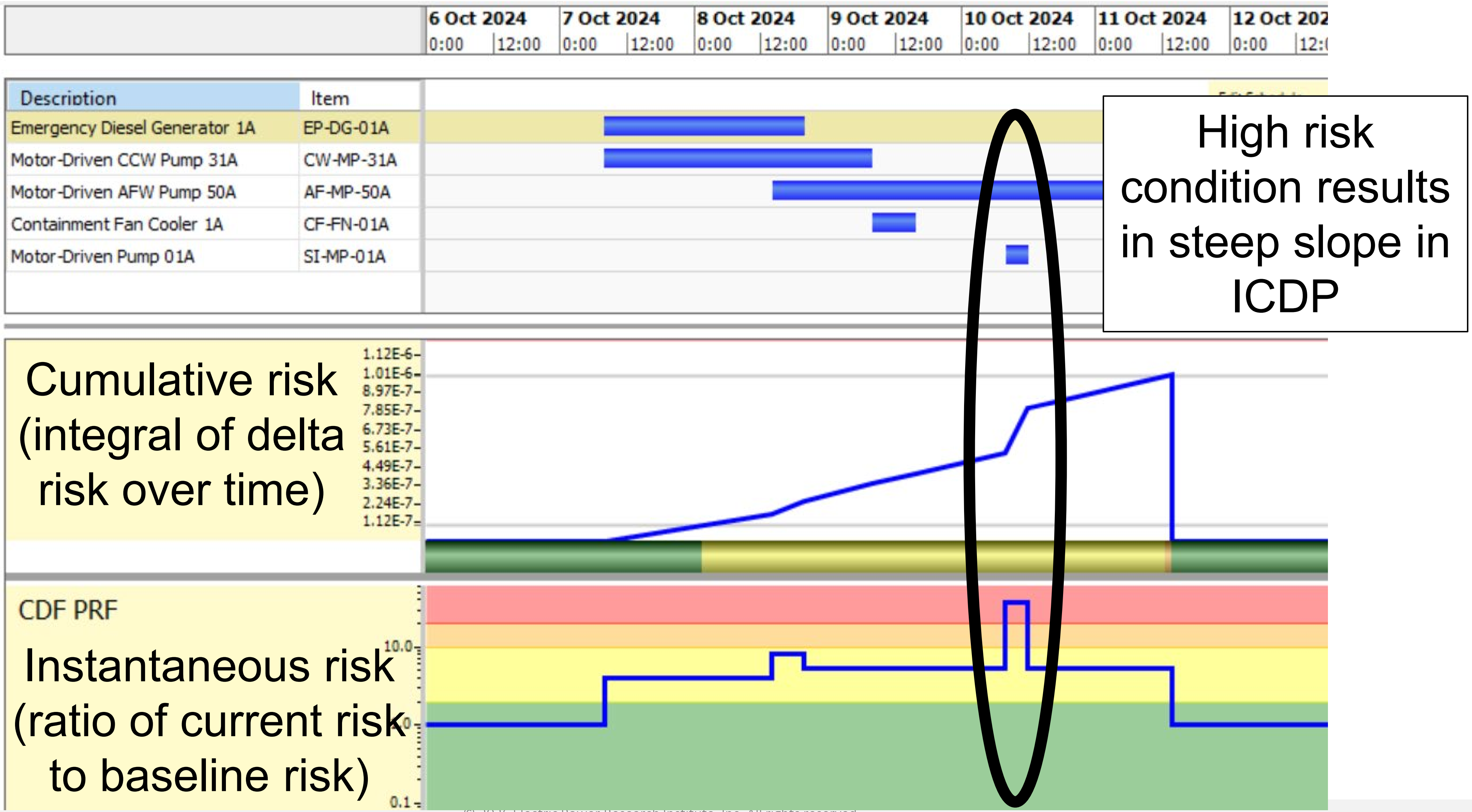
Orange Threshold

Yellow Threshold



ICDP is on a linear scale

Risk Thresholds



“Fixing” the Instantaneous Risk Thresholds

- Instantaneous risk thresholds can be based on a cumulative risk calculation
  - Example 1: Yellow risk = risk that will give an ICDP=1E-6 in 7 days
  - Example 2: Orange risk = risk that will give ICDP=1E-6 in 3 days
  - Example 3: Orange risk = risk that will give ICDP = 5E-5 in 7 days
- With this approach, if base risk goes down, you become less likely to enter Yellow risk (the instantaneous risk to hit Yellow goes up)

Risk Thresholds

- Cumulative risk approach requires criteria to “reset” back to zero
  - Could be one on a weekly basis (based on week-based schedules)
  - Could be based on risk dropping to value close enough to baseline risk
- Instantaneous risk thresholds are (in nuclear) typically much more conservative than cumulative risk metrics
- Most U.S. utilities are moving to use cumulative risk thresholds
- Certain regulatory applications in the U.S. require the use of cumulative risk

Risk Management Actions

Risk Management Actions

- Risk management actions are expected to reduce the actual risk, even if they don't affect the quantitative calculation of risk
- Risk management actions can include any of the following:
  - Announcements/notifications to ensure personnel and management are aware of the risk color
  - Brief important operator actions at shift change or provide just-in-time training to operators
  - Work around the clock until risk is reduced
  - Delay or cancel planned activities that would increase risk

Check Your Understanding

- Why would the risk change from day to day at a nuclear power plant?

- What is the difference between an instantaneous risk metric and a cumulative risk metric?

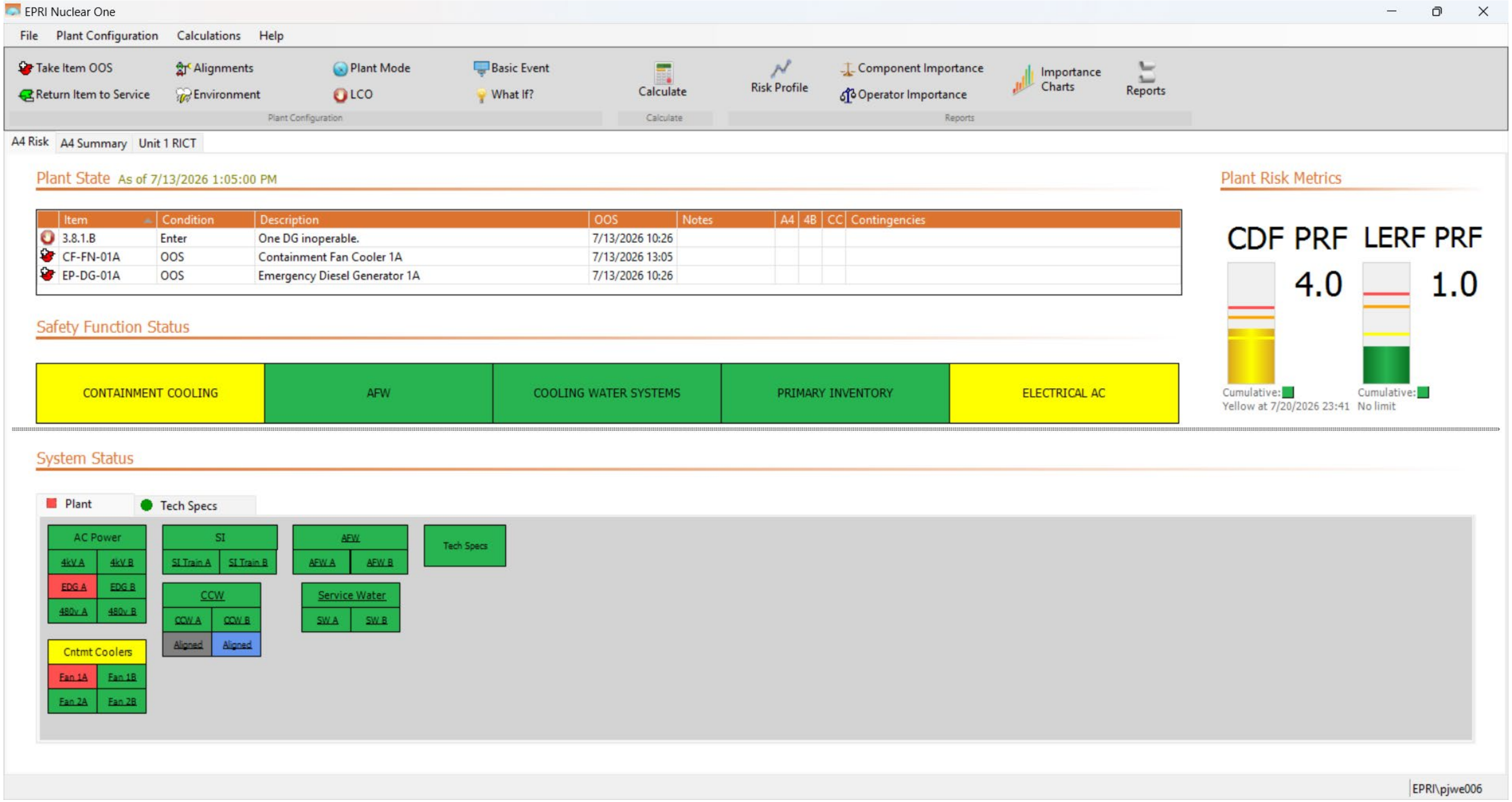
- What actions might a company take when risk is above a defined risk threshold?

Risk Monitors

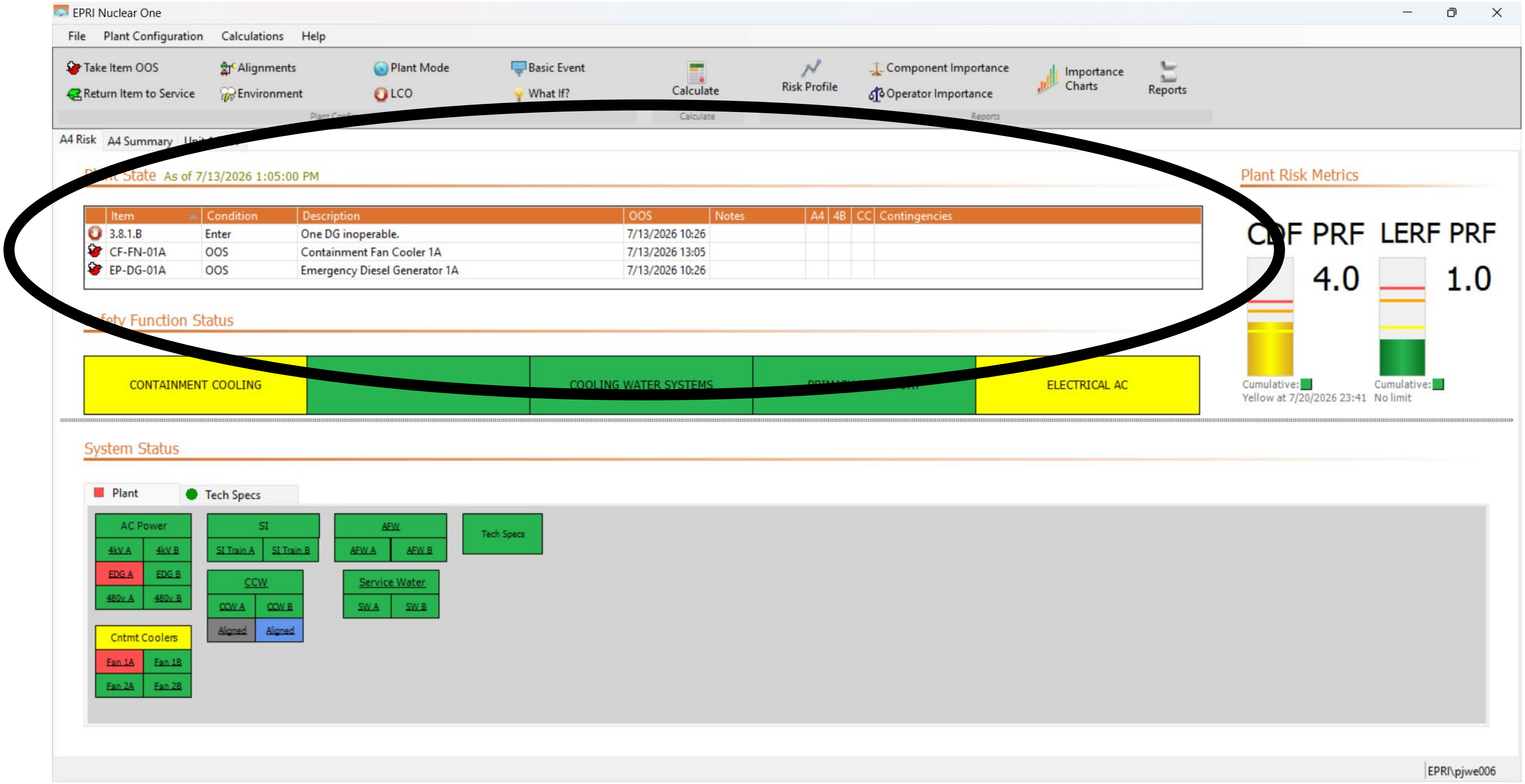
Risk Monitors

- Risk Monitors are software tools designed to:
  - Capture changes in the plant configuration
  - Assess the change in risk
  - Provide risk insights to help plant personnel make good risk decisions
- Risk monitors can provide quantitative and/or qualitative risk insights
- Example risk monitors from nuclear industry:
  - Phoenix Risk Monitor
  - Paragon
  - RiskWatcher

Phoenix Risk Monitor



Phoenix Risk Monitor – Plant State



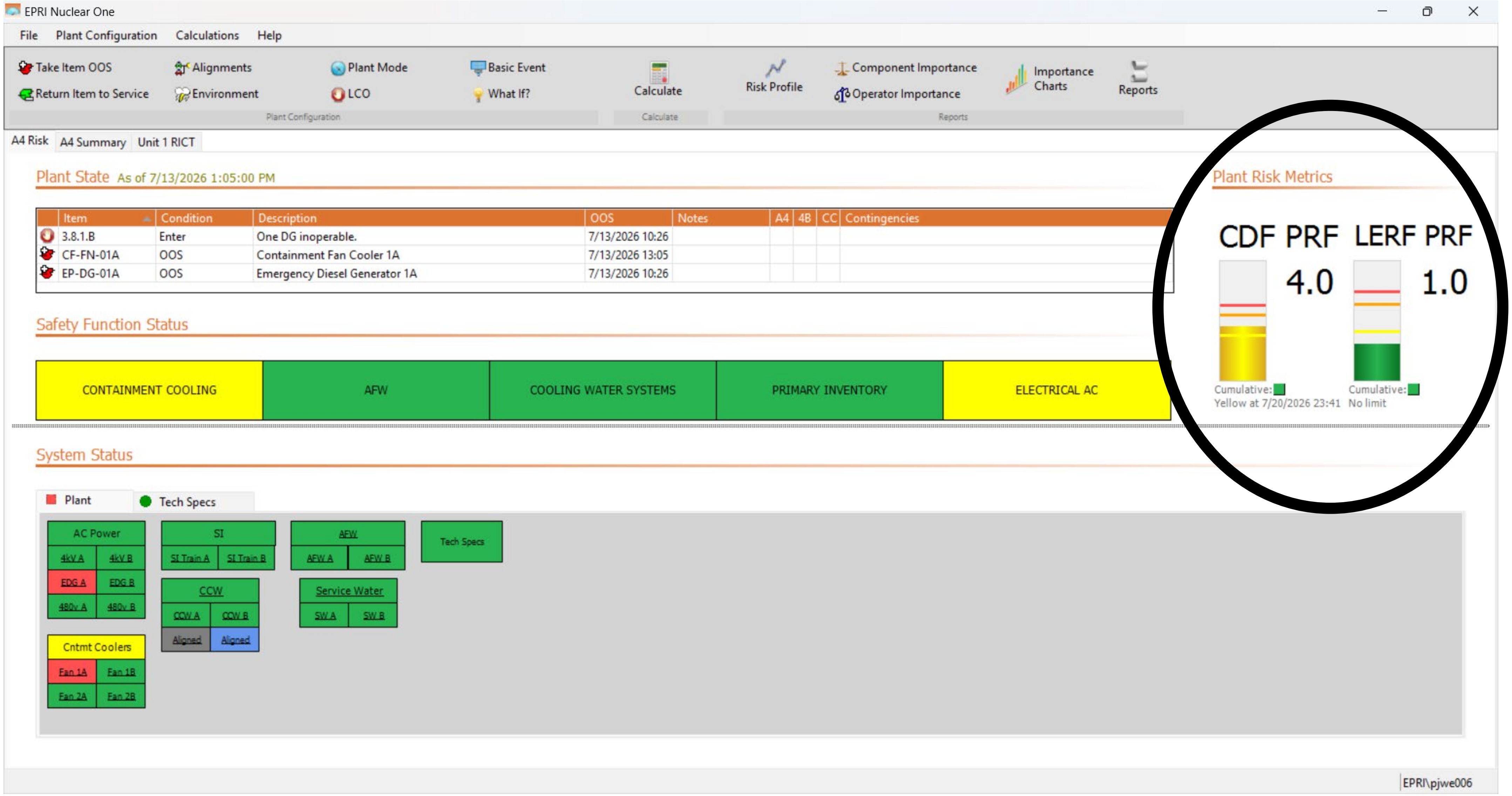
Plant State

Plant State as of 4/15/2018 20:10

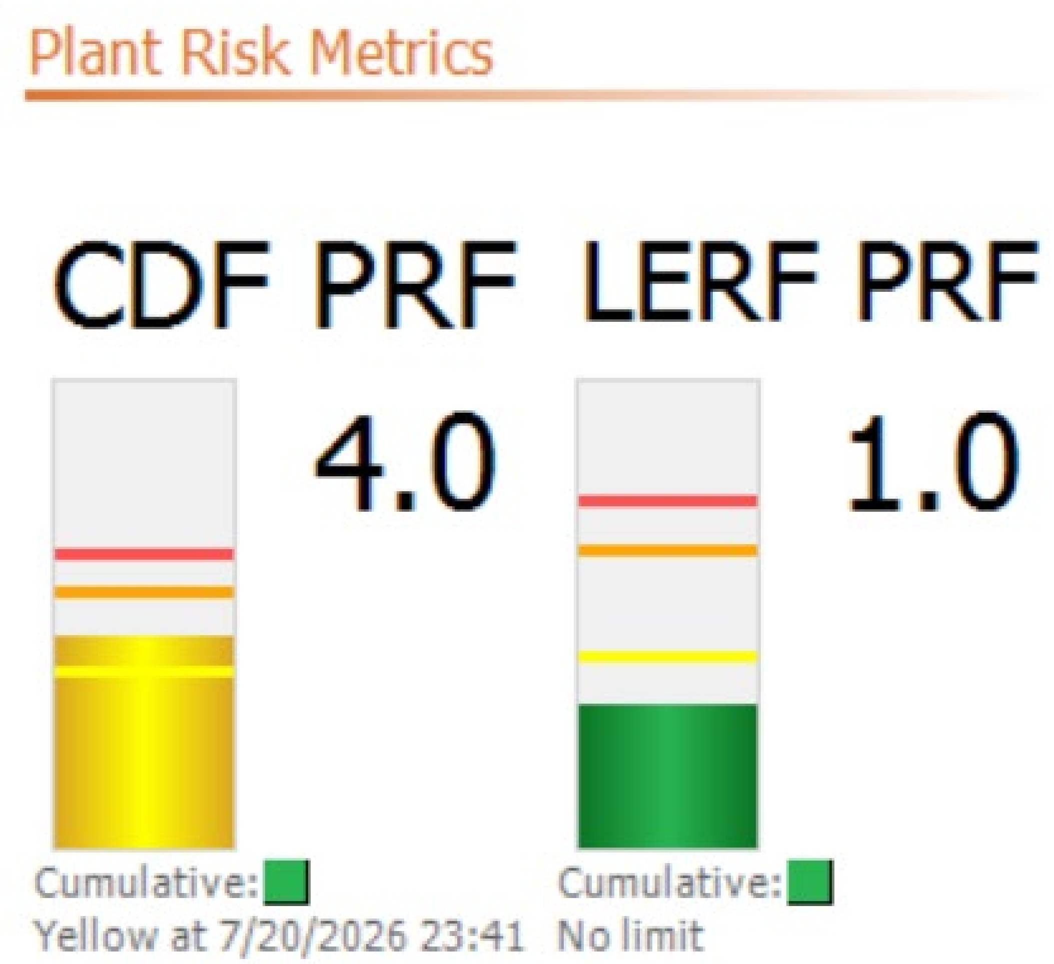
	Item	Condition	Description	OOS	Notes	Contingencies
	CCWLOOPB	Aligned	CC aligned	4/1/2018 20:10		
	CW-MP-31A	OOS	Motor-Driven CCW Pump 31A	4/1/2018 20:10		
	Weather	%LOOP-WEATHE...	Very severe storms	4/1/2018 20:05		

- Shows what is happening in the plant that is affecting current plant risk.
- Includes component unavailabilities
- May include plant alignments, modes, and environmental items

Phoenix Risk Monitor – Risk Meters



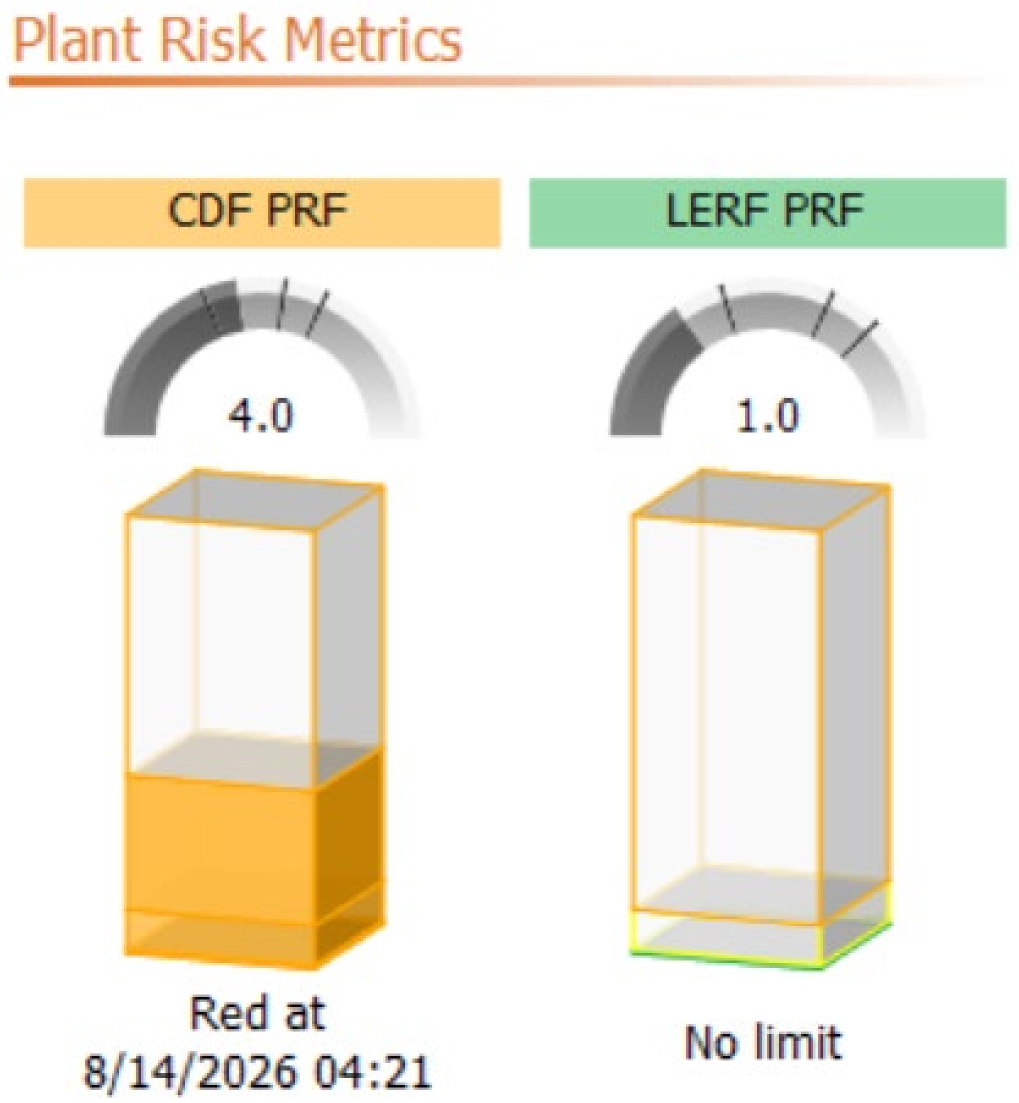
Risk Meters – Instantaneous Risk



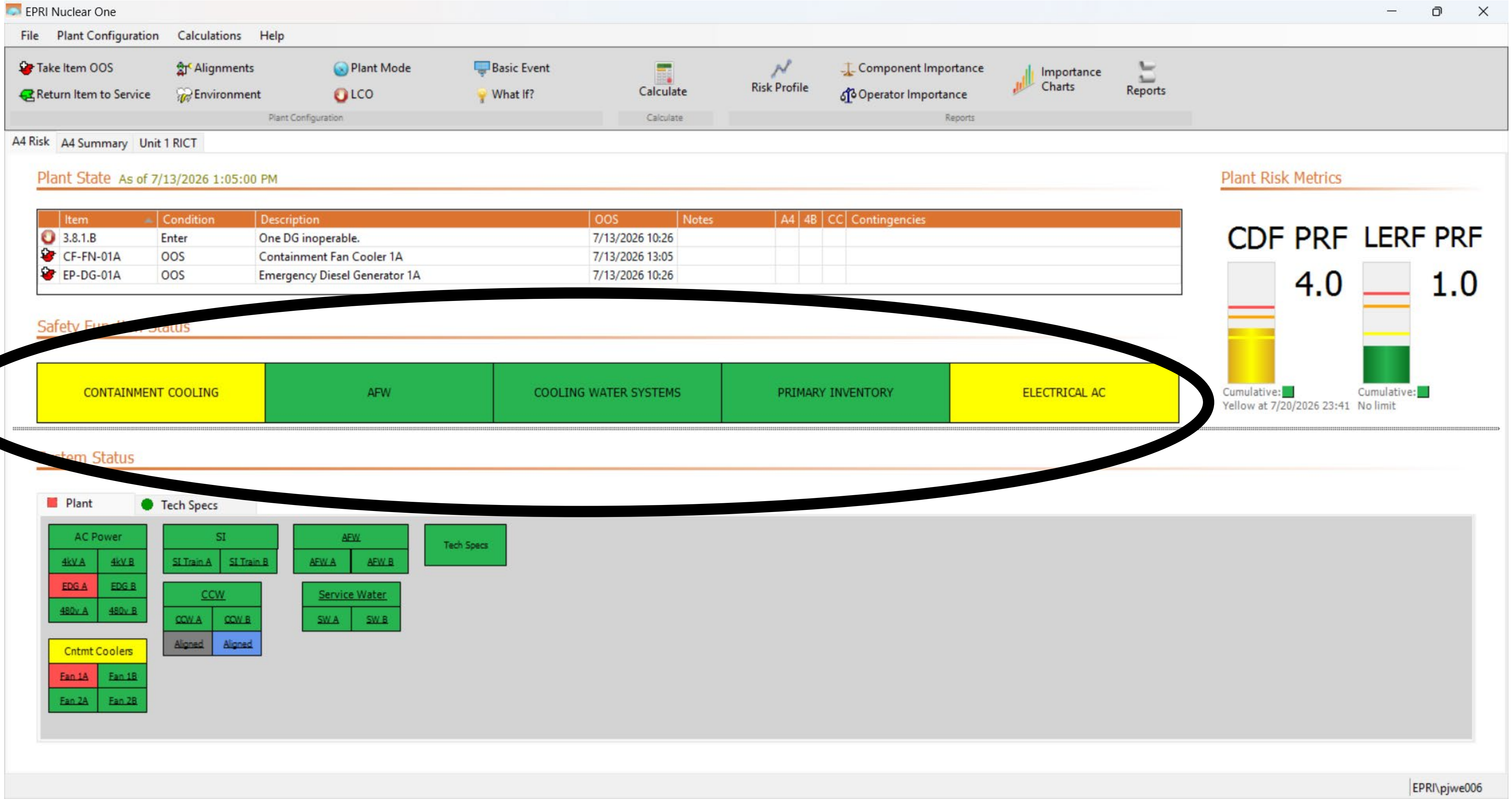
- Shows the current quantitative risk from the probabilistic risk assessment (PRA) model
- Various metrics can be used to show change in risk (e.g., these meters are showing the ratio of current risk to the baseline risk when nothing is out of service)

Risk Meters – Cumulative Risk

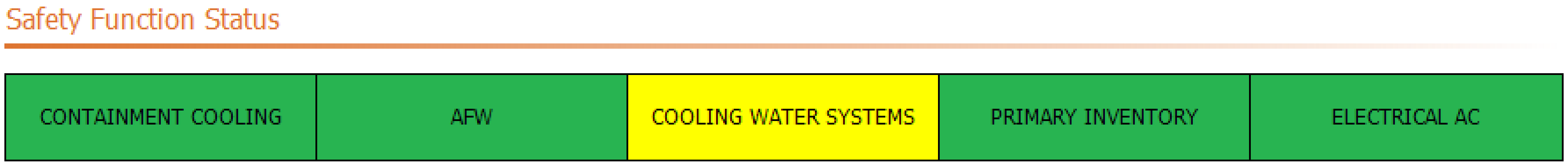
- "Cumulative risk" considers both the instantaneous risk and the length of time spent in each configuration
- Cumulative risk is the integral of the change in risk (from the baseline) over time



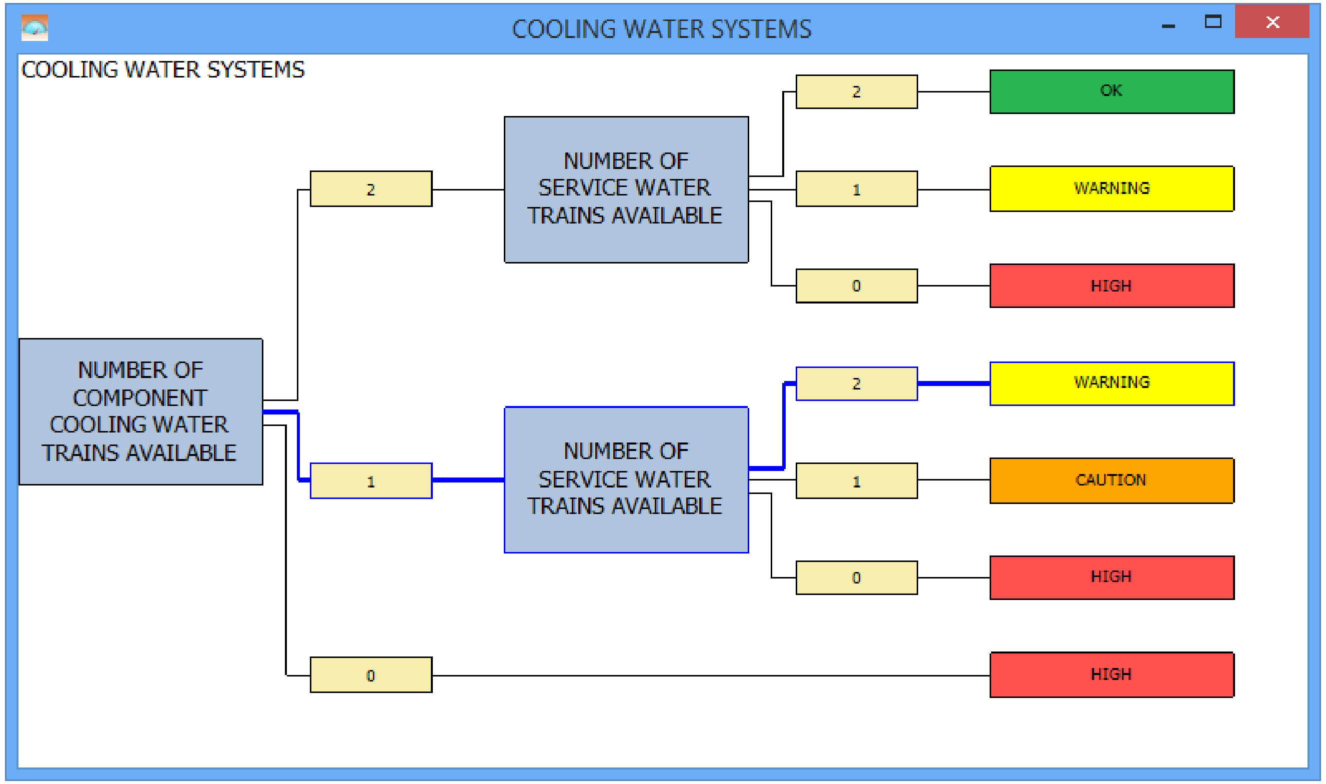
Phoenix Risk Monitor – Safety Function Assessment Trees



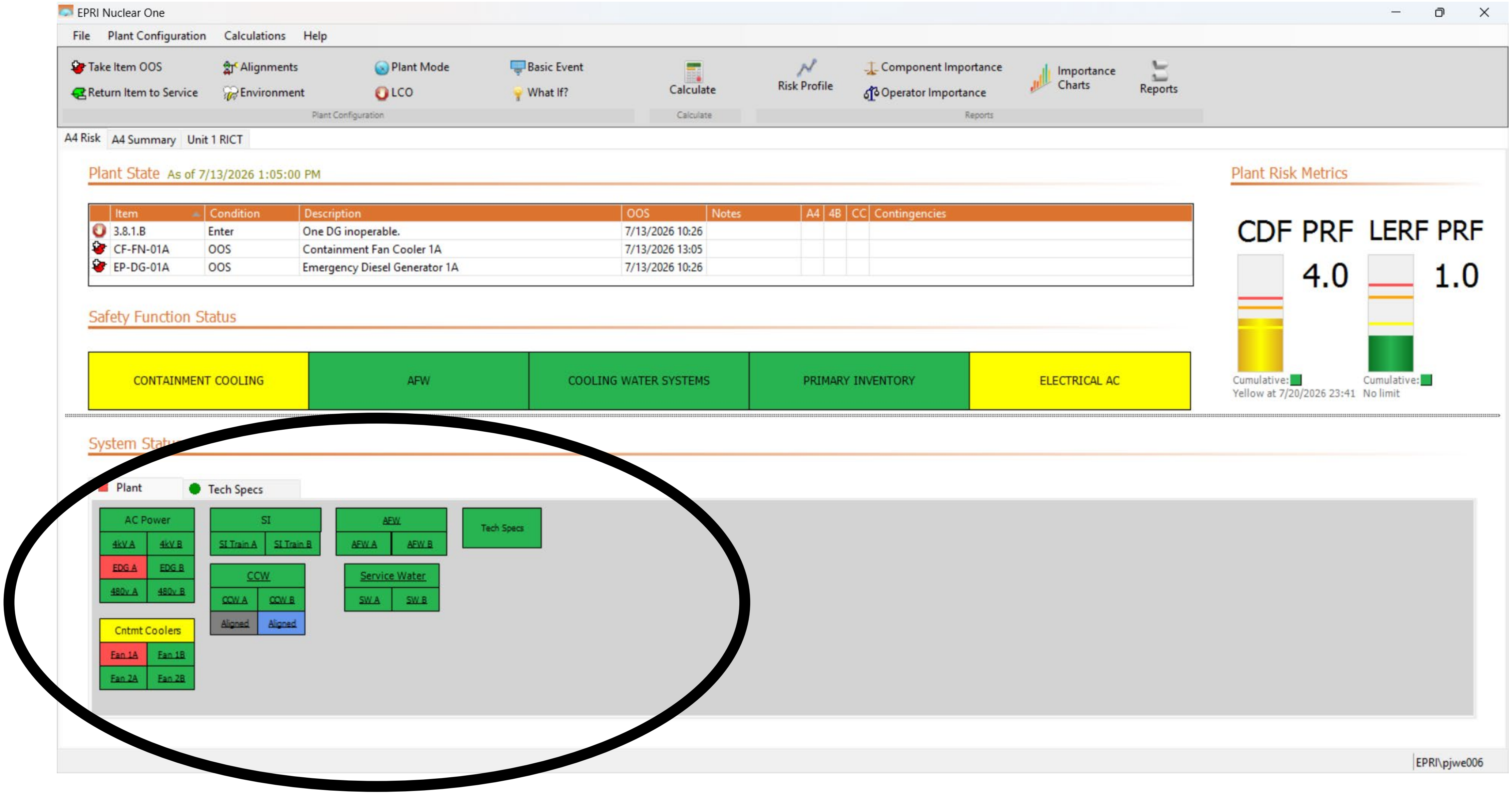
Safety Function Assessment Trees



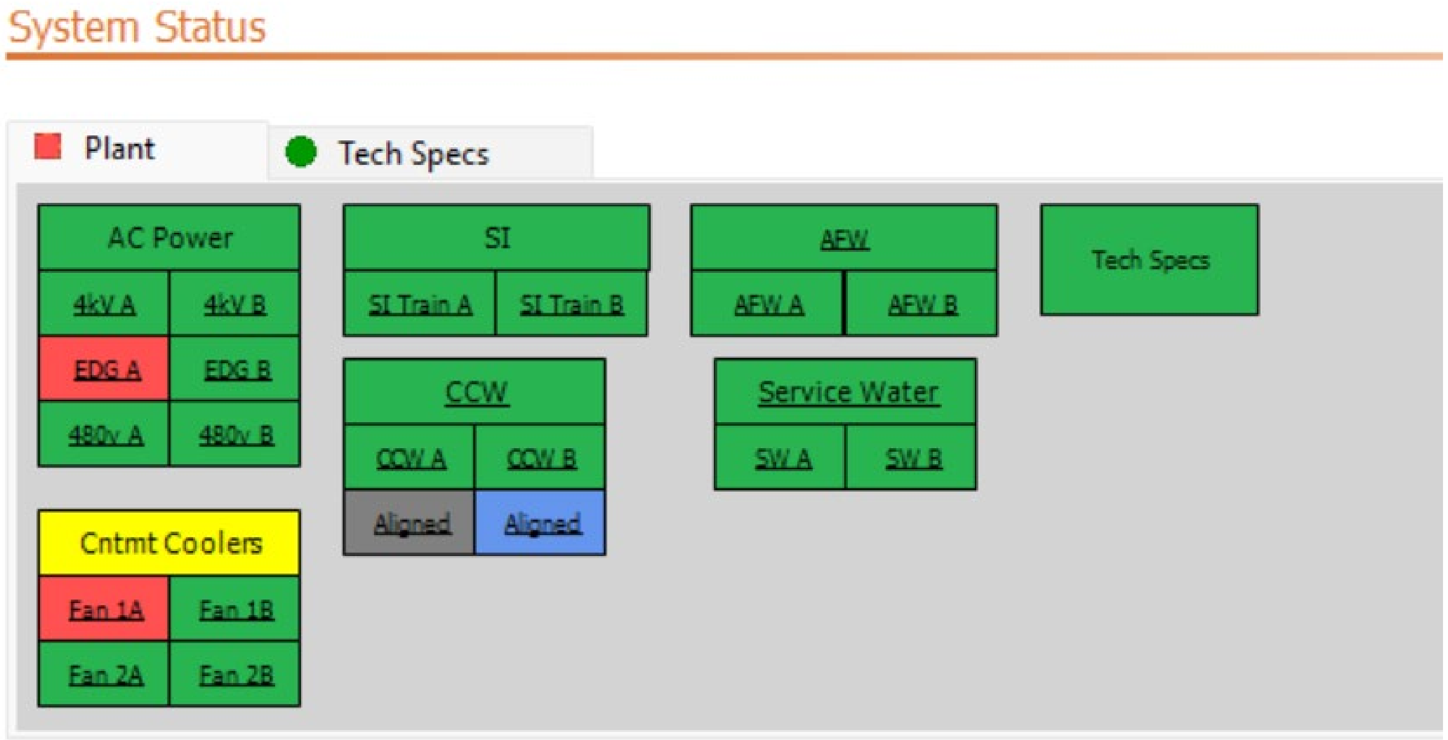
- You can define qualitative safety function analysis logic (decision trees)
- These are often used to assess changes to the defense-in-depth remaining for safety functions



Phoenix Risk Monitor – Status Panel



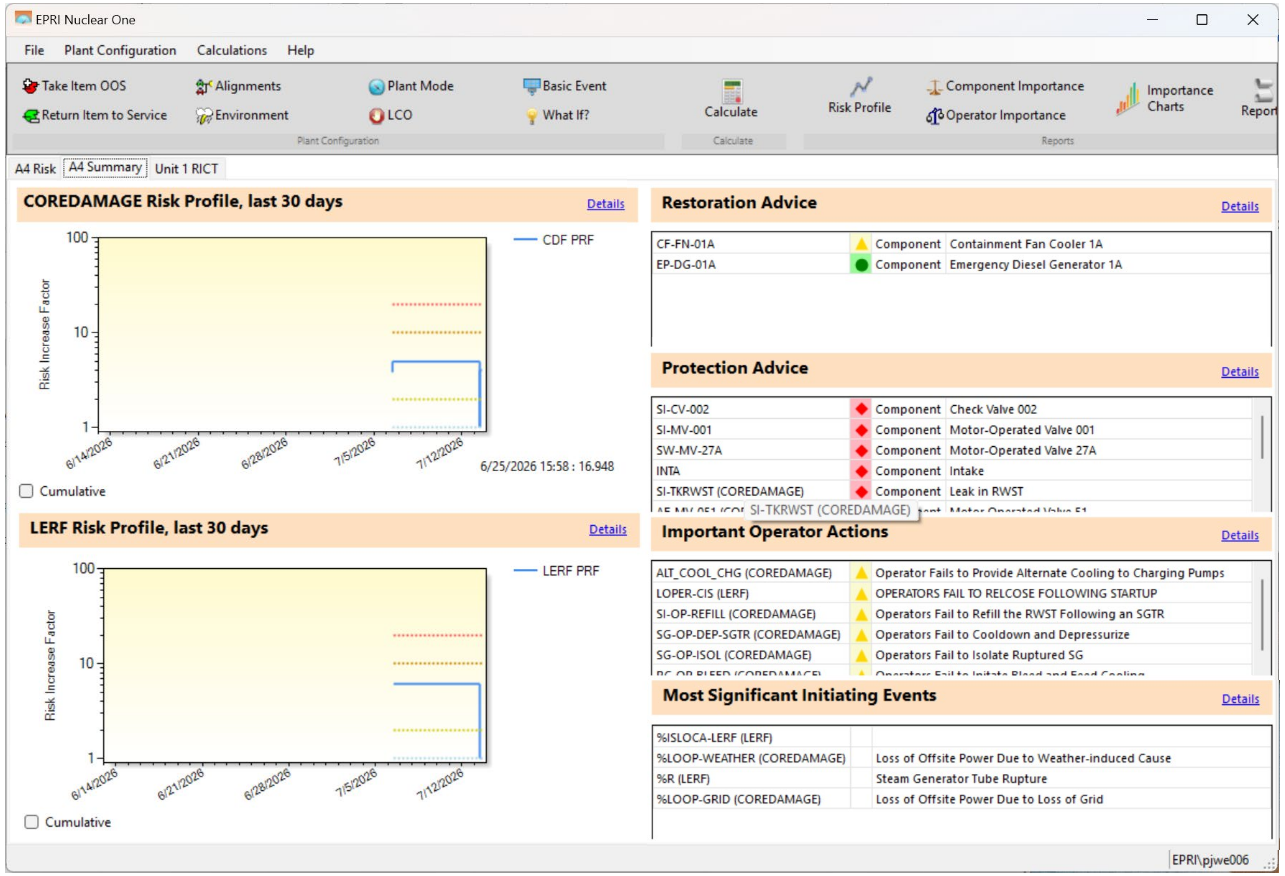
Status Panel



- A status panel can be defined that shows the impact of the plant configuration on systems and functions
- Red indicates system/function failure
- Yellow or orange indicate degraded functions

Risk Insights from Importance Measures

- Risk monitors can provide insights into what is most important, such as:
  - Items that would reduce risk the most, if returned to service
  - Items currently available that would increase risk the most, if lost
  - Most important operator actions
  - Initiating events (events that perturb the steady state operation of the plant) that contribute the most to risk



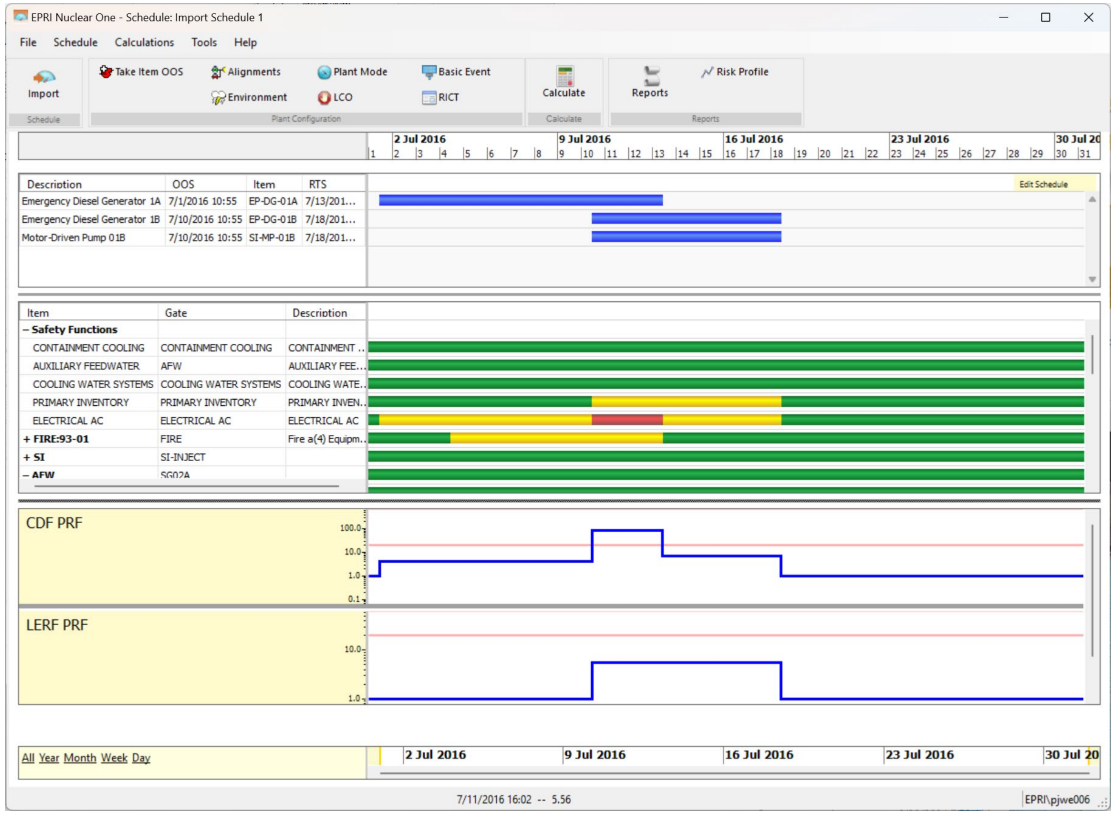
Assessing Risk

Changes to the Plant Configuration

- Routine activities and abnormal conditions can affect the plant's configuration
- Maintenance (preventive and corrective) can make systems/trains unable to respond to a plant upset
- Testing may temporarily prevent equipment from responding to an incident
- Environmental conditions (temperature, weather) may have an impact on what failures can occur (e.g., sensing line freezing) and how often they occur (e.g., severe weather leading to a loss of offsite power)

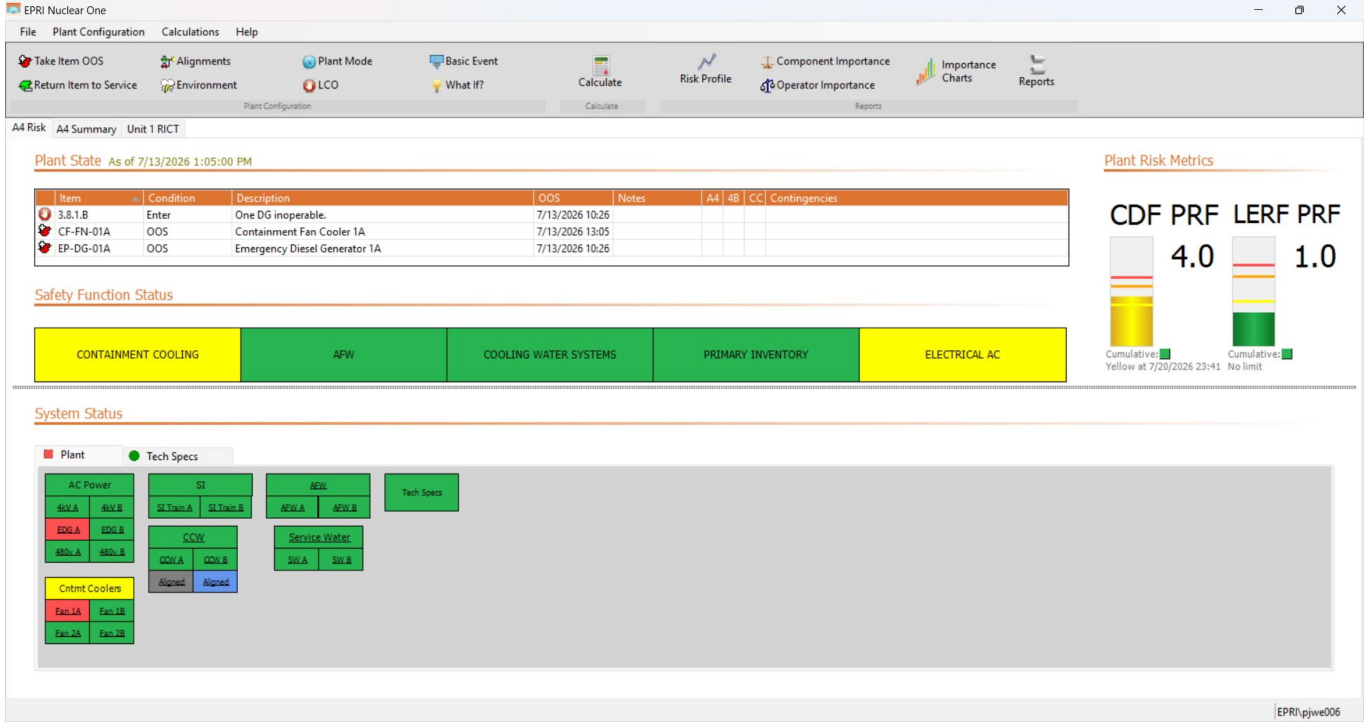
Planned Configurations

- A schedule of activities can be assessed for their impact on risk
- This allows the site personnel to be prepared for the risk imposed by the planned activities
- When combinations of items in the schedule lead to high risk, the schedule is modified to separate those items (if possible)



Real-Time Risk

- The configuration can be assessed in real time to account for any deviations in the planned schedule and any emergent conditions that alter the risk assessment



EPRI

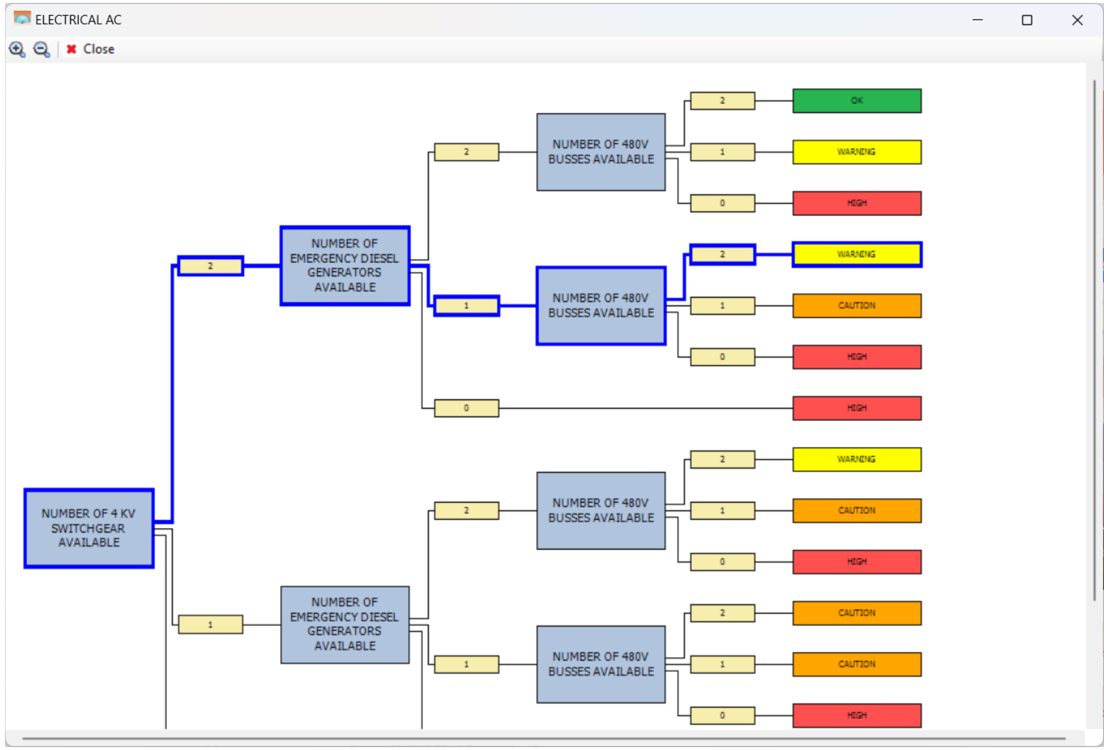
Setting Up a CRM Model

CRM Model – Quantitative

- A CRM model maps changes in the plant configuration to changes in the PRA model
- Components that can be made unavailable to perform their function are mapped to basic events in the fault tree
- Changes in the plant alignment are also mapped to the fault tree basic events (house events)
- Basic events affected by the configuration are set to TRUE, FALSE, or a new probability/frequency and the model is re-quantified
- Risk results from the calculation are provided to the user

CRM Model – Qualitative

- Decision trees are defined to update risk metrics based on the current configuration’s impact on assessed safety functions
- The path through the decision tree is often based on the number of trains available to perform a safety function
- Fault tree logic can be used to assess the path through the decision tree without the need to quantify the fault tree



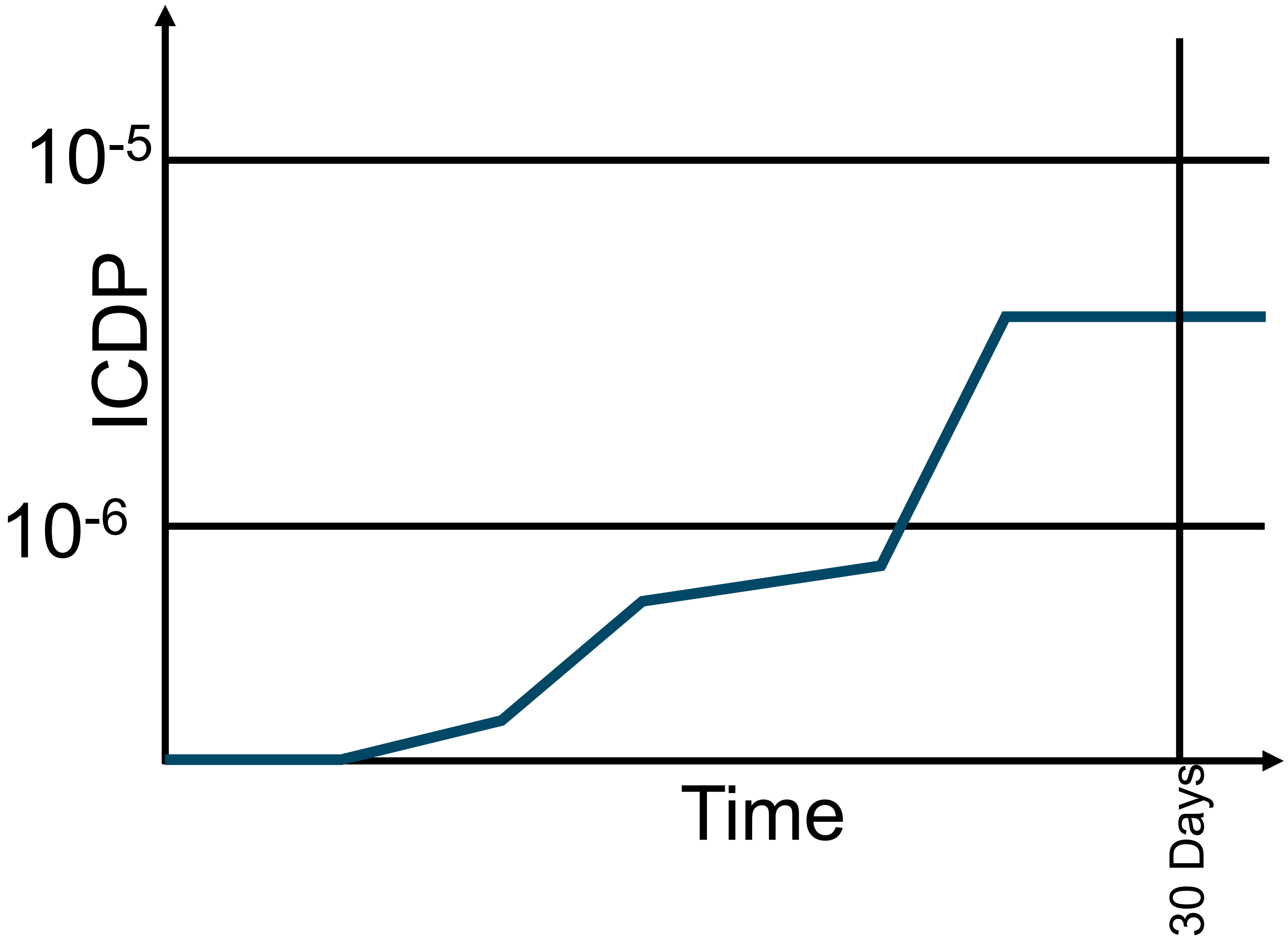
Regulatory Applications (Nuclear) Using CRM

Regulatory Applications That Use CRM Results

- Maintenance Rule
  - Requires utilities to assess the risk prior to taking structures, systems, or components out of service for maintenance
- Notice of Enforcement Discretion (NOED)
  - A NOED is a one-time request to allow the plant to remain at power longer than the Technical Specifications Limiting Condition for Operation (LCO) allows
  - Relies on detailed risk assessment that includes every planned configuration throughout the period covered by the NOED
- Risk-Informed Completion Time
  - The RICT program allows the utility to assess the risk with a cumulative risk metric to extend the LCO without getting prior permission from the regulator

RICT Thresholds

- At ICDP=10^{-6}, risk management actions need to be taken
- ICDP=10^{-5} is the Risk-Informed Completion Time, and the component must be returned to service before this time
- There is also a "backstop" of 30 days, so even if the RICT is longer than 30 days, the plant will have to shut down at 30 days



Summary

Configuration Risk Management

1. Define thresholds where risk management actions are required
2. Identify changes in the plant configuration
   a. Preventive maintenance
   b. Corrective maintenance/emergent condition
   c. Plant alignments, modes, and environmental conditions
3. Reassess the risk for the new configuration
   a. Quantitative – Calculate new risk metrics and assign a risk color
   b. Qualitative – Use decision trees to assess safety functions
4. If risk exceeds thresholds, take risk management actions to help control the risk

Any Questions?

TOGETHER…SHAPING THE FUTURE OF ENERGY®