Idaho National Laboratory

MODULE Q

CONFIGURATION RISK MANAGEMENT

Configuration Risk Management

- **Purpose: To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.**
- **Objectives:**
  - **Explain why base case or nominal PRA results cannot be used for maintenance planning**
  - **Explain what is meant by "configuration risk management" and how it related to risk-informed regulation**
  - **Evaluate "risk" profiles quantitatively**
- **Reference: NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications**

Configuration Risk Management

- **Three primary elements to configuration risk management;**
  - **Configuration: Assess the plant configuration accounting for the status of plant components**
  - **Risk: Quantify a risk metric (e.g., core damage frequency, core damage probability, large early release frequency) for the assessed plant configuration which typically includes comparison against nominal plant configuration**
  - **Management: Take measures to avoid risk-significant configurations, acquire better understanding of the risk level of a particular plant configuration, and/or limit the duration and frequency of such configurations that cannot be avoided**

Configuration Risk Management Why an Issue?

- **Economics - Plants perform increased amounts of maintenance while at power, to reduce outage durations**
- **Safety**
  - **Increased maintenance while at power not covered in IPEs/PRAs**
  - **Increased on-line maintenance can produce high-risk plant configurations**

Configuration Risk Management Why an Issue?

"In general, the industry appears to be adopting the practice of on-line maintenance faster than it is developing and implementing effective controls to manage the safety (risk) implications of this practice."

[Temporary Instruction (TI) 2525/126, "Evaluation of On-line Maintenance, February 1995," page 5]

Observed Preventive Maintenance Practices of Concern

- **Multiple components simultaneously out of service, as allowed (implicitly) by technical specifications**
- **Repeated entries into Action Statements to perform PM + long equipment downtimes**
- **Significant portions of power operations may be spent in Action Statements to carry out PMs**

Configuration Risk Management Traditional Approaches

- **Technical Specifications and Limiting Conditions for Operation**
  - **Identifies systems/components important to safety based on traditional engineering approach**
  - **Limit component out-of-service times for individual and combinations of component outages (not based on formal risk analysis)**
- **Maintenance planning guidelines such as 12-week rolling schedule, etc.**
  - **Based on train protection concept and Technical Specifications**
  - **Provide guidance to work week planners on allowable maintenance/testing**
- **Operator judgment**
  - **If emergent work arises, decision to continue with schedule maintenance/testing**

Configuration Risk Management Traditional Approaches

- **Weaknesses of Traditional Approaches**
  - **Generally based on engineering judgment and limited to Technical Specification equipment**
  - **No limit on frequency of equipment outages - only on duration of each outage**
- **Is the traditional approach good enough, given the increased emphasis on on-line maintenance?**
- **How can PRA help?**

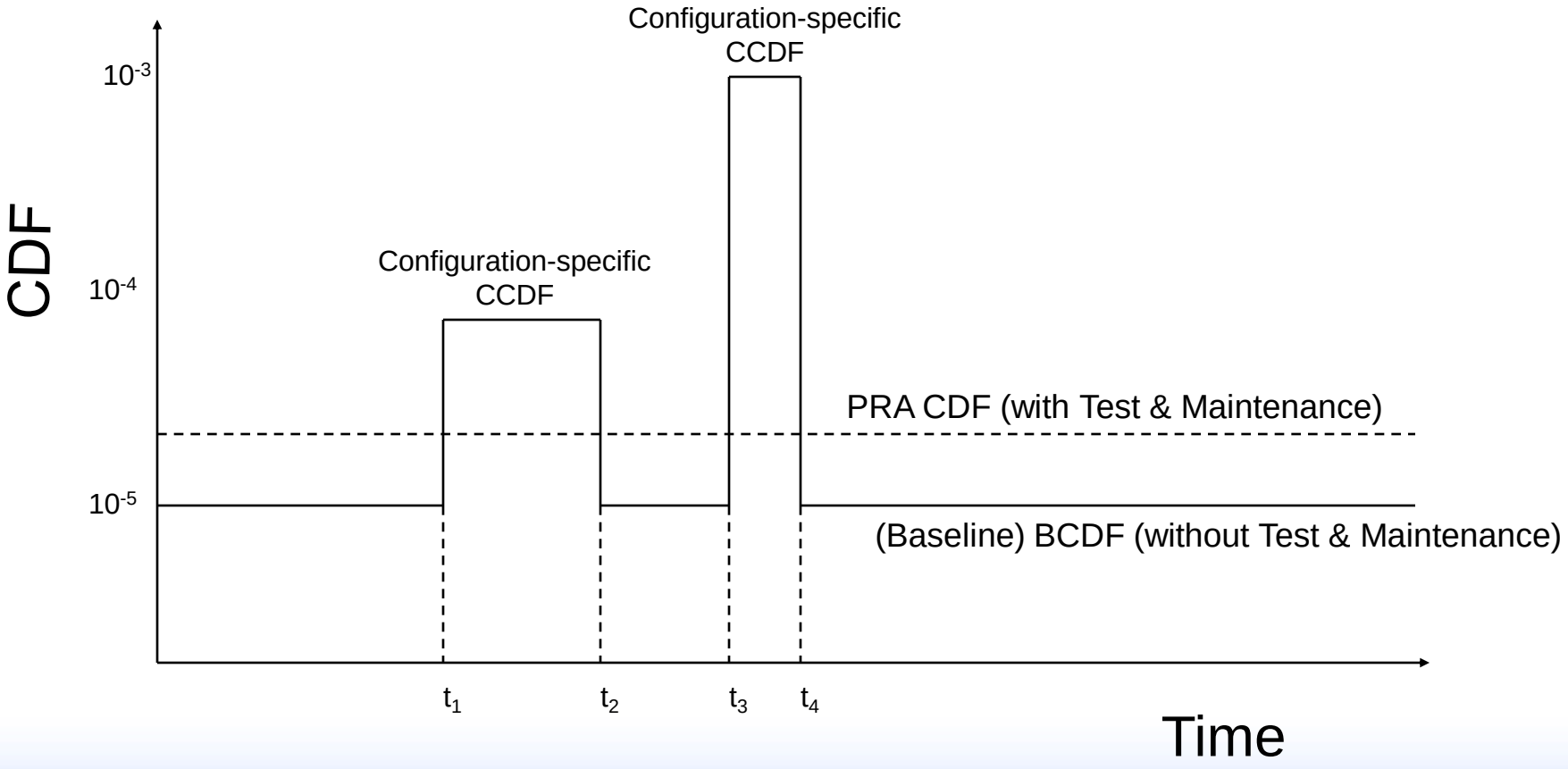
Configuration Risk Management

- **Configuration risk management: one element of risk-informed regulation**
- **Can be forward-looking or retrospective**
  - **Forward-looking to plan maintenance activities & outage schedules**
  - **Retrospective to evaluate risk significance of past plant configurations (e.g., Accident Sequence Precursor analyses or Significance Determination Process)**

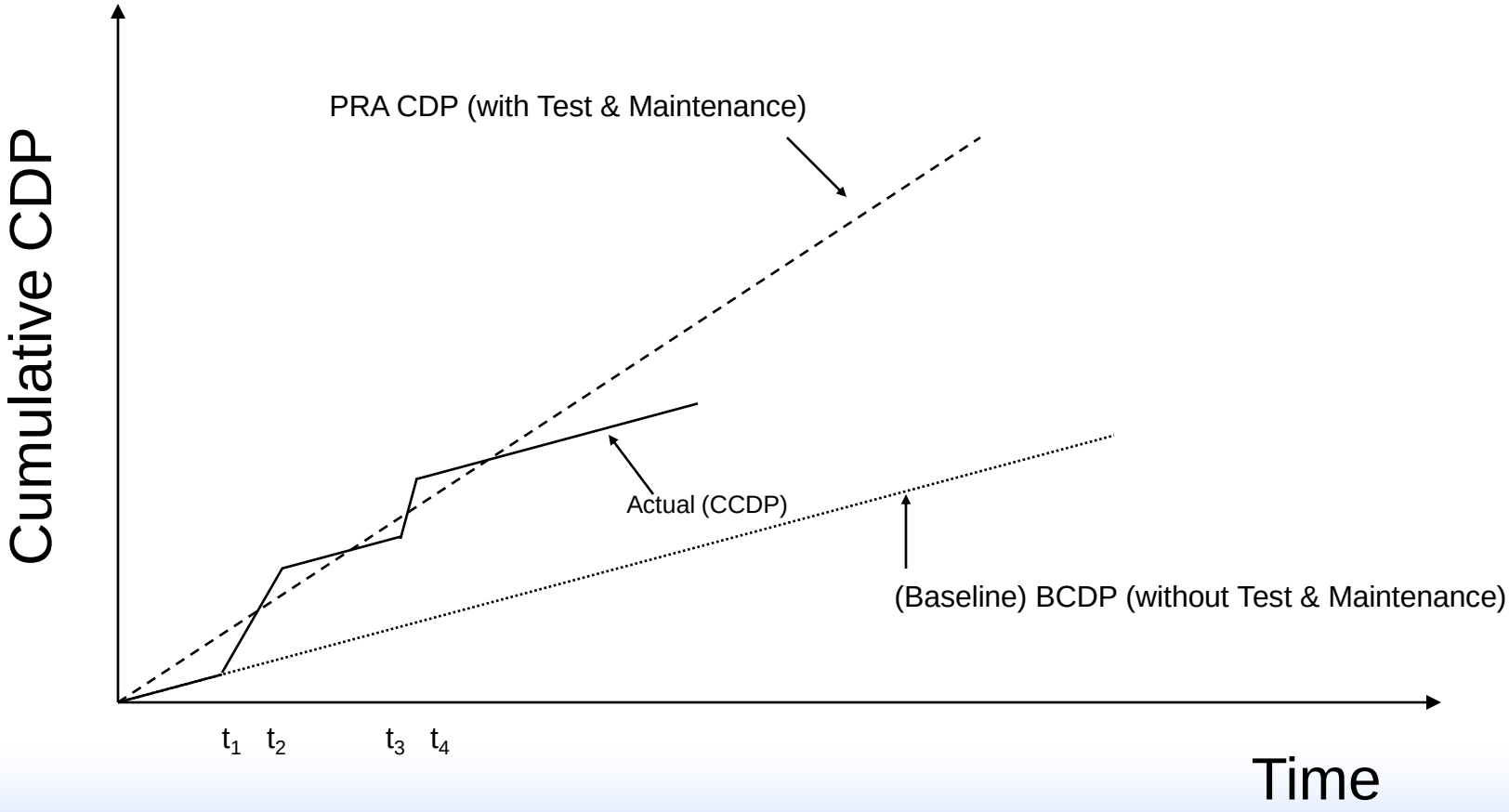
Configuration Risk Management

- **Configuration risk has various measures**
  - **Core damage frequency profile (instantaneous)**
    - **Baseline CDF (BCDF, i.e., the zero maintenance CDF)**
    - **Configuration-specific (conditional) CDF (CCDF)**
  - **Incremental CDF (ICDF)**
    - **= CCDF - BCDF**
  - **Core damage probability (CDP)**
    - **≈ CDF * duration**
  - **Incremental core damage probability (ICDP)**
    - **≈ ICDF * duration**
    - **= CCDP - BCDP**
  - **Incremental large early release probability (ICLERP)**
    - **≈ ILERF * duration**
    - **= CLERP - BLERP**

CDF Profile


Configuration-specific
CCDF
Configuration-specific
CCDF
CDF
10^{-3}
10^{-4}
10^{-5}
PRA CDF (with Test & Maintenance)
(Baseline) BCDF (without Test & Maintenance)
t_1
t_2
t_3
t_4
Time

Cumulative CDP Profile



Configuration Risk Management

- **Includes management of:**
  - **OOS components**
    - **Instantaneous CCDF (configuration-specific CDF)**
  - **Outage time of components & systems**
    - **Configuration duration**
    - **CCDP**
    - **ICDP**
  - **Backup components**
    - **Instantaneous CCDF**
  - **Frequency of specific configuration**
    - **Cumulative CDP over time (slide Q-12)**

  (each of these discussed on the following slides)

Managing OOS Components

- **Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently**
  - **For Maintenance Rule, 10 CFR 50.65 NUMARC 93-01 suggest a ceiling configuration-specific CCDF of 1E-3/year**
    - **Subject of such a ceiling value being studied by the NRC**
    - **NRC endorses the Feb. 22, 2000 revision of section 11 of NUMARC 93-01, but neither endorses nor disapproves the numerical value of 1E-3/year**

Managing Outage Time

- Must determine how long configuration can exist before risk incurred becomes significant
- Many utilities using EPRI PSA Application Guide numerical criteria, although not endorsed by NRC
  - NRC has no numerical criteria for temporary changes to plant
  - For Maintenance Rule (NUMARC 93-01, section 11),
    - If >1E-5 ICDP or >1E-6 ILERP
      - Then configuration should not normally be entered voluntarily
    - If 1E-6 to 1E-5 ICDP or 1E-7 to 1E-6 ILERP
      - Then assess non quantifiable factors and establish risk management actions
    - If <1E-6 ICDP or <1E-7 ILERP
      - Then normal work controls
- For risk-informed Tech. Specs., single permanent change to AOT acceptable if (RG 1.177):
    - ICDP < 5E-7 (called ICCDP in Reg. Guide)
    - ICLERP < 5E-8
- Must know compensatory measures to take to extend outage time without increasing risk

Managing Backup Components

- **Must determine which components can carry out functions of those out of service (OOS).**
- **Ensure availability of backup components while primary equipment OOS.**

Controlling Frequency

- **Must track frequency of configurations and modify procedures & testing to control occurrences, as necessary and feasible.**
- **Repeated entry into a specific configuration might violate PRA assumptions with respect to assumed outage time.**

Why Configuration Risk Management is Needed…

- PRA assumes random failures of equipment (including equipment outages for testing & maintenance)
  - Importance measures based on random, independent maintenance of components
- PRA does not correctly model simultaneous outages of critical components
  - Treats maintenance as independent, so simultaneous outages unlikely
- Simultaneous outages (i.e., plant configurations) can increase risk significantly above the PRA average risk level
- Lack of configuration management can affect initiating events and equipment designed to mitigate initiating events, leading to increased risk

Preventive Maintenance Risk Calculations

- Risk impact of PM on single component
- Risk impact of maintenance schedule
- Risk impact of scheduling maintenance (power operations versus shutdown)

Risk Monitors

- **On-line risk monitors can be used to evaluate plant configurations for a variety of purposes:**
  - **To provide current plant risk profile to plant operators**
  - **As a forward-looking scheduling tool to allow decisions about test and maintenance actions weeks or months in advance of planned outages**
  - **As a backward-looking tool to evaluate the risk of past plant configurations**

Current Risk Monitor Software Packages

- Erin Engineering Sentinel
- Scientech/NUS Safety Monitor
  - The NRC acquired this package from Scientech, and has an agency-wide license covering its use
- EPRI R&R Workstation (EOOS)
  - The NRC acquired this package from EPRI, and has an agency-wide license covering its use
- Specialized packages developed for specific plants, e.g., South Texas Project

Requisite Features

- **Risk monitor software requires (at a minimum) the following features:**
  - **PRA solution engine for analysis of the plant logic model**
    - **Can be ET/FT, single FT, or cut set equation**
  - **Database to manage the various potential plant configurations**
    - **That is, a library of results for configurations of interest**
  - **Plotting program to display results**

Risk Monitor Capabilities

- **As a tool for plant operators to evaluate risk based on real-time plant configuration:**
  - **Calculates measure of risk for current or planned configurations**
  - **Displays maximum time that can be spent in that particular configuration without exceeding pre-defined risk threshold**
  - **Provides status of plant systems affected by various test and maintenance activities**
  - **Operators can do quick sensitivity studies to evaluate the risk impacts of proposed plant modifications**

Risk Monitor Capabilities

- **As a tool for plant scheduling for maintenance and outage planning:**
  - **Generates time-line that shows graphically the status of plant systems and safety functions**
  - **Generates risk profile as plant configuration varies over time**
  - **Identifies which components have strongest influence on risk**

Risk Monitor Strengths and Limitations

- **Risk Monitor Strengths**
  - **Provides risk determinations of current and proposed plant configurations**
  - **Compact model**
  - **Many current PRA models can be converted into risk monitor format**
  - **Can obtain importance and uncertainty information on results**
  - **Provides risk management guidance by indicating what components should be restored first**

Risk Monitor Strengths and Limitations

- **Risk Monitor Limitations**
  - **For some PRA codes, difficulty of converting PRA models into master logic diagram (e.g., Large Event Tree approach models)**
  - **Effort required to set up databases to link master logic diagram events to plant components and electronic P&IDs, and interface with scheduling software (e.g., map PRA basic events into component IDs and procedures)**
  - **Analysis issues**
    - **Effects on IE frequencies**
    - **Human recovery modeling**
    - **CCF adjustments**
    - **Consideration of plant features not normally modeled in PRA studies**
    - **Truncation limits**

Student Exercise

- **Review your IPE and identify component out-of-service modeling**
  - **What types of outages are modeled?**
    - **Testing**
    - **Preventive maintenance**
    - **Corrective maintenance**
  - **Any "special" events that cover multiple, simultaneous component outages?**
  - **What are the basis for the component outage probabilities?**
    - **Generic**
    - **Plant-specific**
    - **Time period covered**
    - **Sources for data collection**
    - **Definition of outage duration**