

PSA Basics

International Workshop

on

Use of PSA in Operation of NPPs and in Regulatory Decision-Making

May 17 - 21, 2004

Kyiv, Ukraine

What is PSA?

Probabilistic Safety Assessment is an organized methodology for making a realistic estimate of the likelihood of combinations of component failures and/or human errors that will lead to a catastrophic event.

Realistic, not Conservative

PSA is a tool to help the user determine:

- the magnitude of the risk
- where the risk lies
- what components and operator actions are most important to risk
- where resources can be most effectively applied to reduce risk

A realistic PSA model serves these objectives.
A conservative one does not.

Abbreviations

- **PSA** - Probabilistic Safety Assessment
- **PRA** - Probabilistic Risk Assessment
- **PSA = PRA**

PSA Levels

<u>Level</u>	<u>End State</u>	<u>Model</u>
1	Core Damage	Core Cooling and Support Systems
2	Radioactive Release	+ Containment
3	Public Health Impact	+ Site

PSA Formula

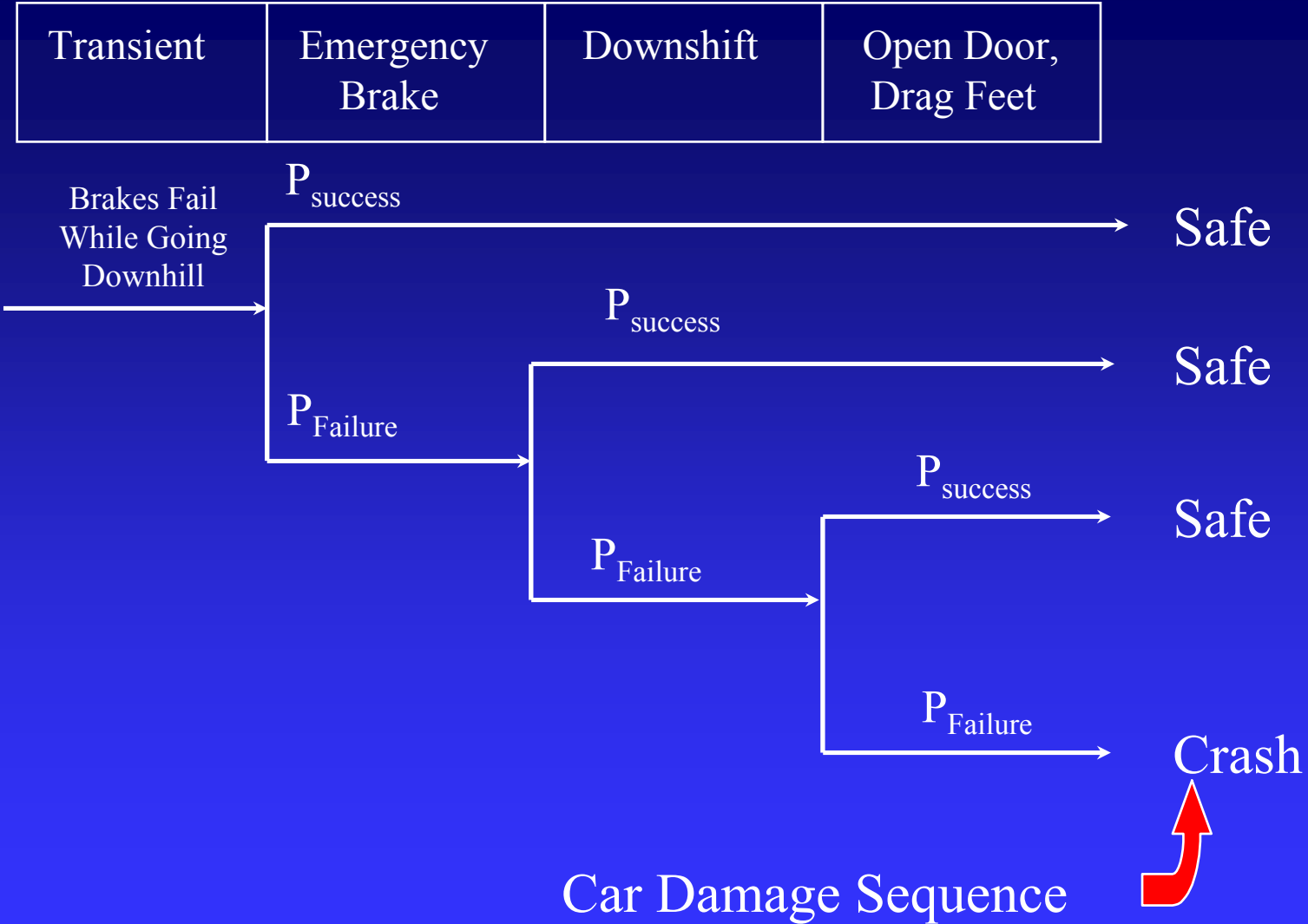
$$\begin{array}{l} \textit{Initiating} \\ \textit{Events} \\ \textit{Frequency} \end{array} * \begin{array}{l} \textit{Mitigating Systems} \\ \textit{Failure Probability} \end{array} = \begin{array}{l} \textit{Core Damage} \\ \textit{Frequency} \end{array}$$

- Complexities
 - Size (many events and systems)
 - Support Systems (power, cooling, etc.)
 - Thermal-Hydraulic Behavior
 - Human Performance
 - External Events

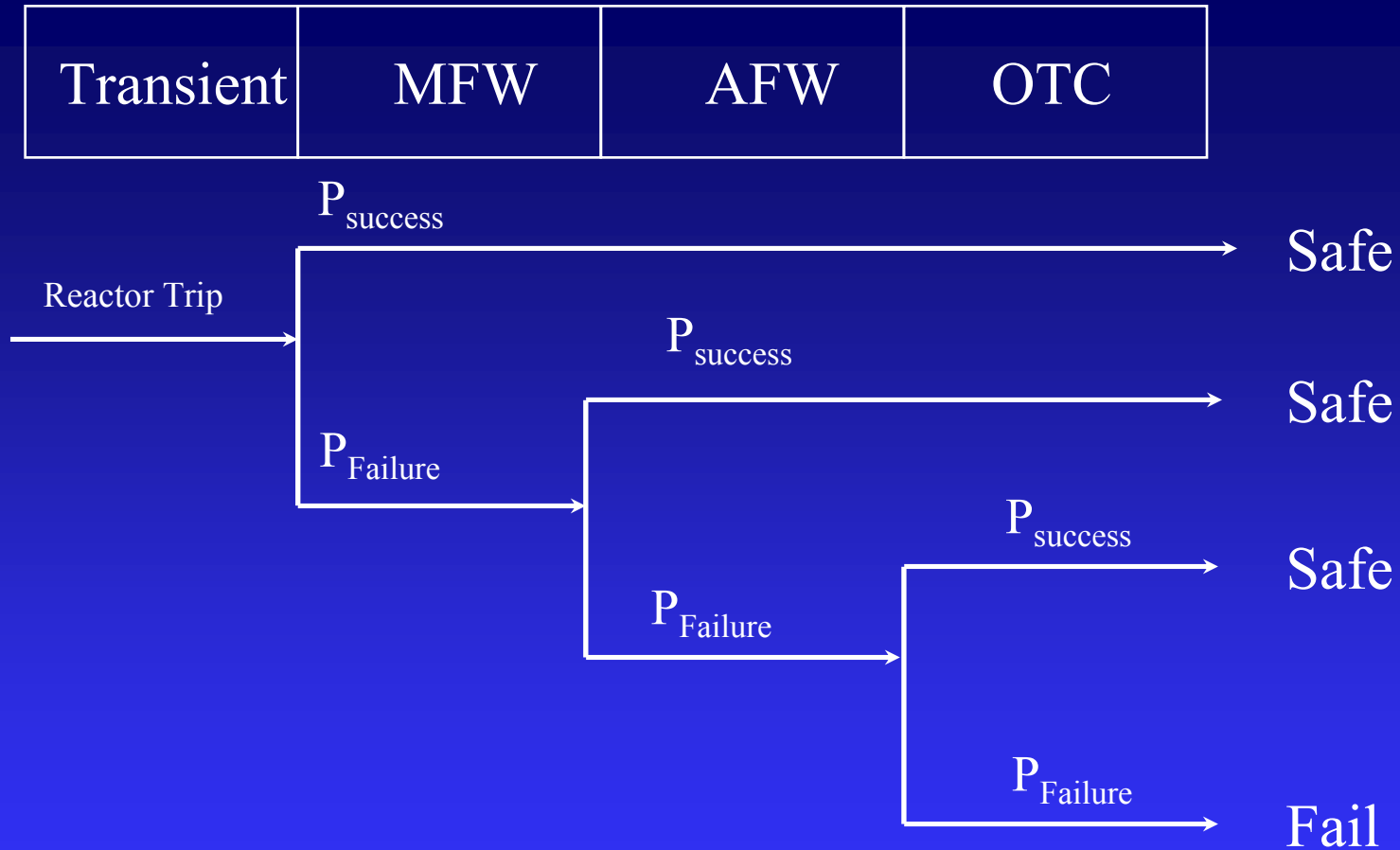
Modeling

- Event Trees
 - flow charts defining the systems and functions needed for mitigation of an initiating event

Event Tree



Event Tree



Core Damage Sequence



Modeling

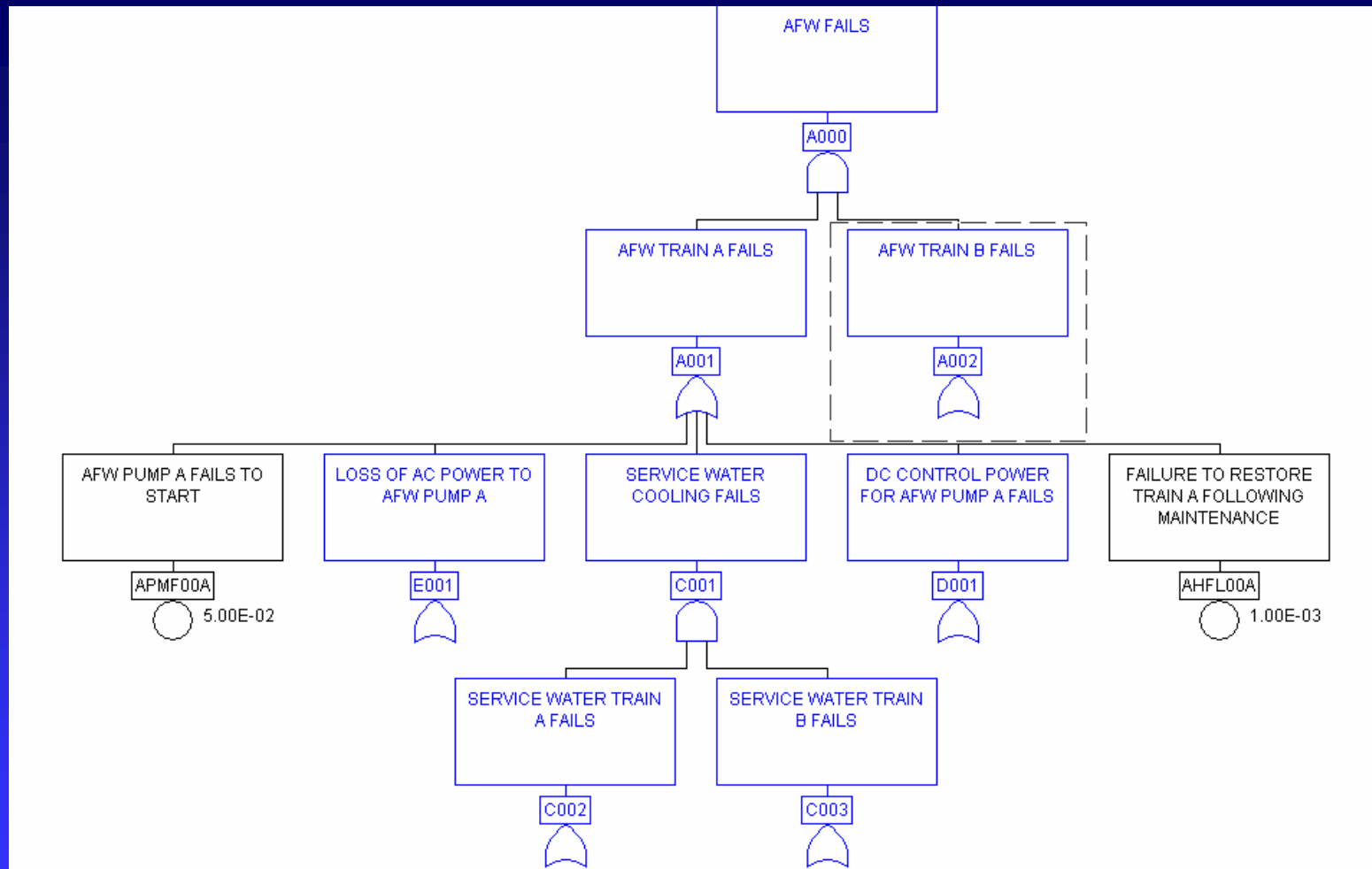
- Event Trees

flow charts defining the systems and functions needed for mitigation of an initiating event

- Fault Trees

logic trees modeling how a system or function can fail - models redundancies and dependencies

Fault Tree



Systems Modeled

- AC Power
- Accumulators
- Auxiliary Feedwater
- Chemical Volume and Control
- Containment Isolation
- Containment Spray
- Containment Ventilation
- DC Power
- Engineered Safeguards
- Heating, Ventilation, and Air Conditioning (HVAC)
- High Head Safety Injection
 - High Head Injection
 - High Head Recirculation
- Instrument Air
- Power Conversion
- Primary Pressure Control (PORV/SRVs)
- Residual Heat Removal
 - Residual Heat Removal
 - Low Head Injection
 - Low Head Recirculation
- Service Water
 - Component Cooling Water
 - Intake Cooling Water
 - Service Water
 - Turbine Plant Cooling Water

Modeling

- Event Trees

flow charts modeling the systems needed for mitigation (accident scenarios)

- Fault Trees

logic trees modeling how a system or function can fail - models redundancies and dependencies

- Data

frequency, availability, and reliability information used as input to the fault trees

Data Types

- Initiating Event Frequencies
- Component Failure Rates
- Common Cause Failure Rates
- Maintenance Unavailabilities
- Human Reliability Estimates

basic events

Initiating Events

- Reactor/Turbine Trip
- Loss of Main Feedwater
- Loss of Offsite Power
- Excessive Feedwater
- Steam Line Line Break
- Feedwater Line Break
- Spurious ES Actuation
- Loss of Engineered Safeguards Bus A
- Loss of Engineered Safeguards Bus B
- Loss of Cooling Water
- Loss of 'A' DC Power Bus
- Loss of 'B' DC Power Bus
- Small Break LOCA
- Medium Break LOCA
- Large Break LOCA
- Steam Generator Tube Rupture

Plant-Specific Data

- Failures based on plant maintenance records and other databases
- Demands based on maintenance records, operating logs, surveillance frequencies
- Times based on operator logs, monthly operating reports, procedures
- Used for pumps, valves, diesels, fans, compressors, batteries, chargers, inverters

Generic Data

- based on combined industry data and/or expert opinion
- used when plant-specific data is limited or unavailable

Maintenance Unavailability

$$= (\textit{Hours Unavailable} / \textit{Total Hours})$$

- Unavailable hours based on plant equipment clearance databases and/or Maintenance Rule database
- Total hours based on time on-line, Modes 1-3

Human Error

- Latent Errors
 - Errors occurring before the event sequence, such as a failure to restore a valve to operability following maintenance
- Dynamic Errors
 - Errors occurring during the event sequence, such as a failure to switch to sump recirculation mode

Human Reliability Analysis

HRA

- Human Error Event
 - Probability that the operating crew fails to perform an action correctly
- Factors
 - time available to perform action
 - guidance (procedures)
 - stress levels
 - training
 - opportunities for review (self-review or review by other operators)

Human Reliability Analysis

HRA

- Quantification of human error probabilities is one of the most uncertain aspects of PSA.
- Human Error Events are usually dominant contributors to risk.

Cutsets

Combinations of events which
lead to core damage

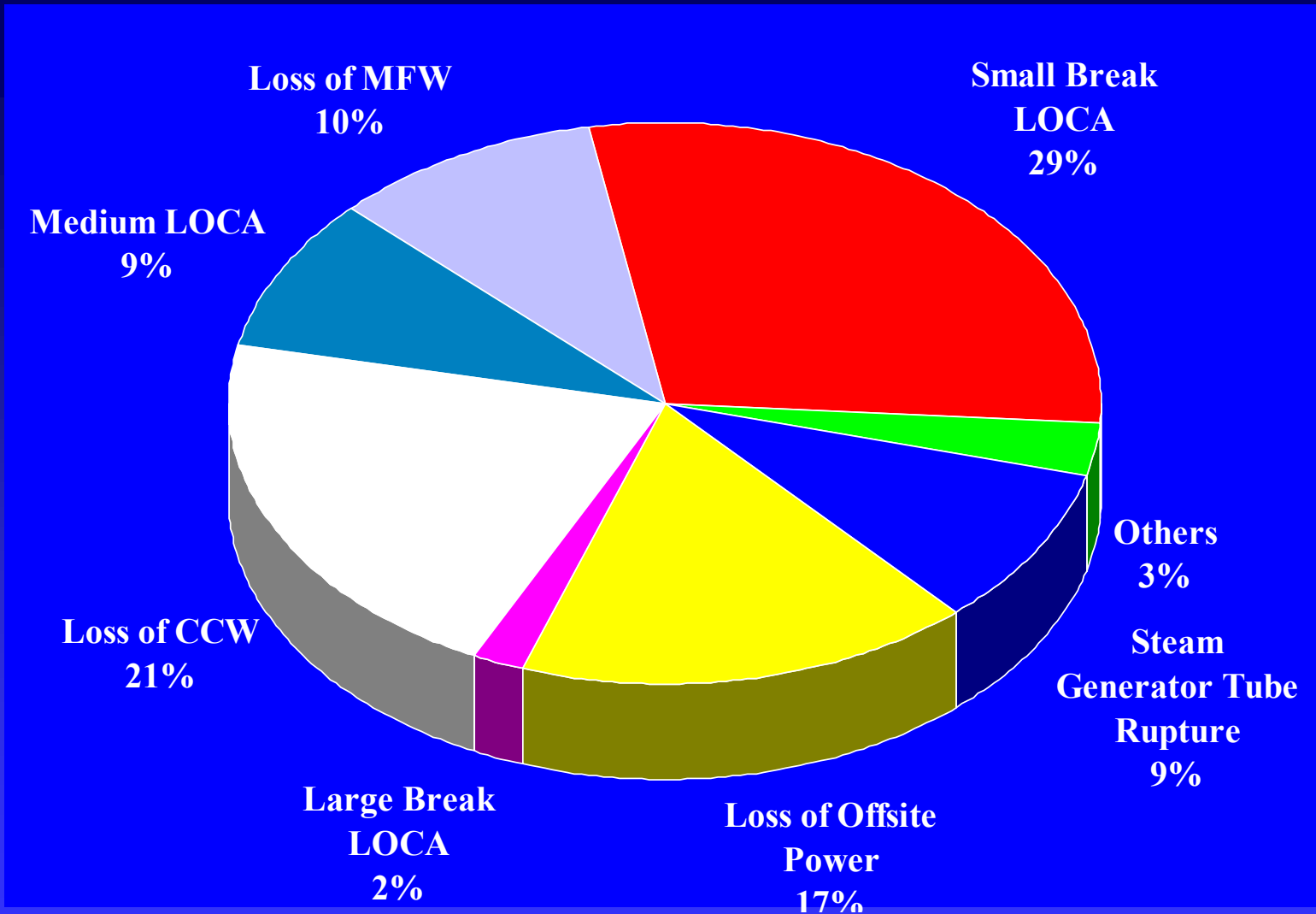
Also referred to as:

- core damage sequences
- accident sequences

Cutset Examples

- Loss of Offsite Power (LOOP), Diesel Generators fail to start, Batteries deplete, offsite power not recovered.
(5E-6 per year)
- Small-break LOCA, Operating crew fails to transition to high-pressure recirculation. (1E-5 per year)
- Loss of main feedwater, failure of auxiliary feedwater, common cause failure of high-head safety injection pumps.
(7E-7 per year)
- Loss of component cooling, failure of seal injection, RCP-seal LOCA, no high-head safety injection due to loss of component cooling. (3E-6 per year)

CDF and Initiators



Core Damage Frequency = 3E-05/yr

PSA Applications

Question

- How do I use my PSA to determine priorities based on relative risk significance?

Answer

- Use risk importance measures to rank components.

There are two basic importance measures:

**Risk Achievement Worth (RAW) and
Fussell-Vesely Importance (FV).**

Risk Achievement Worth (RAW)

The RAW of Component X is the ratio of the CDF with component X out of service to the normal (baseline) CDF.

- $RAW(X) = CDF(X=1) / CDF_{baseline}$

where

- $CDF_{baseline}$ = total baseline CDF
- $CDF(X=1)$ = total CDF with failure probability of component X set to 1.0

RAW (cont.)

- Larger RAW \rightarrow greater importance
- If the $RAW(X) = 1.00$, then taking component X out of service has *no* impact on risk.
- If the $RAW(X) = 1.05$, then the baseline CDF increases 5% when component X is taken out of service.
- If the $RAW(X) = 2.00$, then the baseline CDF doubles when component X is taken out of service.

RAW (cont.)

- Large RAW if ...

- Component is relatively reliable, and
- Component function is important: few or no functional redundancies.
- Example: Refueling Water Storage Tank (RWST)

- Typical RAWs (Turkey Point)

- | | |
|--------------------------------------|------|
| - 4KV ES Bus | 1173 |
| - 125V Vital DC Bus | 302 |
| - Refueling Water Storage Tank | 21 |
| - Suction MOV for Safety Injection | 10 |
| - Pilot-Operated Relief Valve (PORV) | 3 |

RAW (cont.)

- Use RAW to evaluate the risk significance when a component is out of service or failed.
 - Primary application:
 - On-Line Maintenance - component out of service
 - Other potential application
 - Maintenance Prioritization - which components would have the highest impact on risk, and which would have the least impact on risk.
 - Procedure / Training Review - rank procedures and prioritize training based on the RAWs of operator actions.

Fussell-Vesely Importance (FV)

The FV of Component X is the fraction the normal (baseline) CDF would be reduced if Component X was always available (never failed and never OOS).

$$- \text{FV}(X) = (\text{CDF}_b - \text{CDF}(X=0)) / \text{CDF}_{\text{baseline}}$$

where

- $\text{CDF}_{\text{baseline}}$ = total baseline CDF
- $\text{CDF}(X=0)$ = total CDF with failure probability of component X set to 0.0

FV (cont.)

- Larger FV \rightarrow greater importance
- If the $FV(X) = 0.0$, then improving the reliability of component X has *no* impact on risk.
- If the $FV(X) = 0.2$, then if component X never failed or was never out of service, the CDF would decrease by 20%.

FV (cont.)

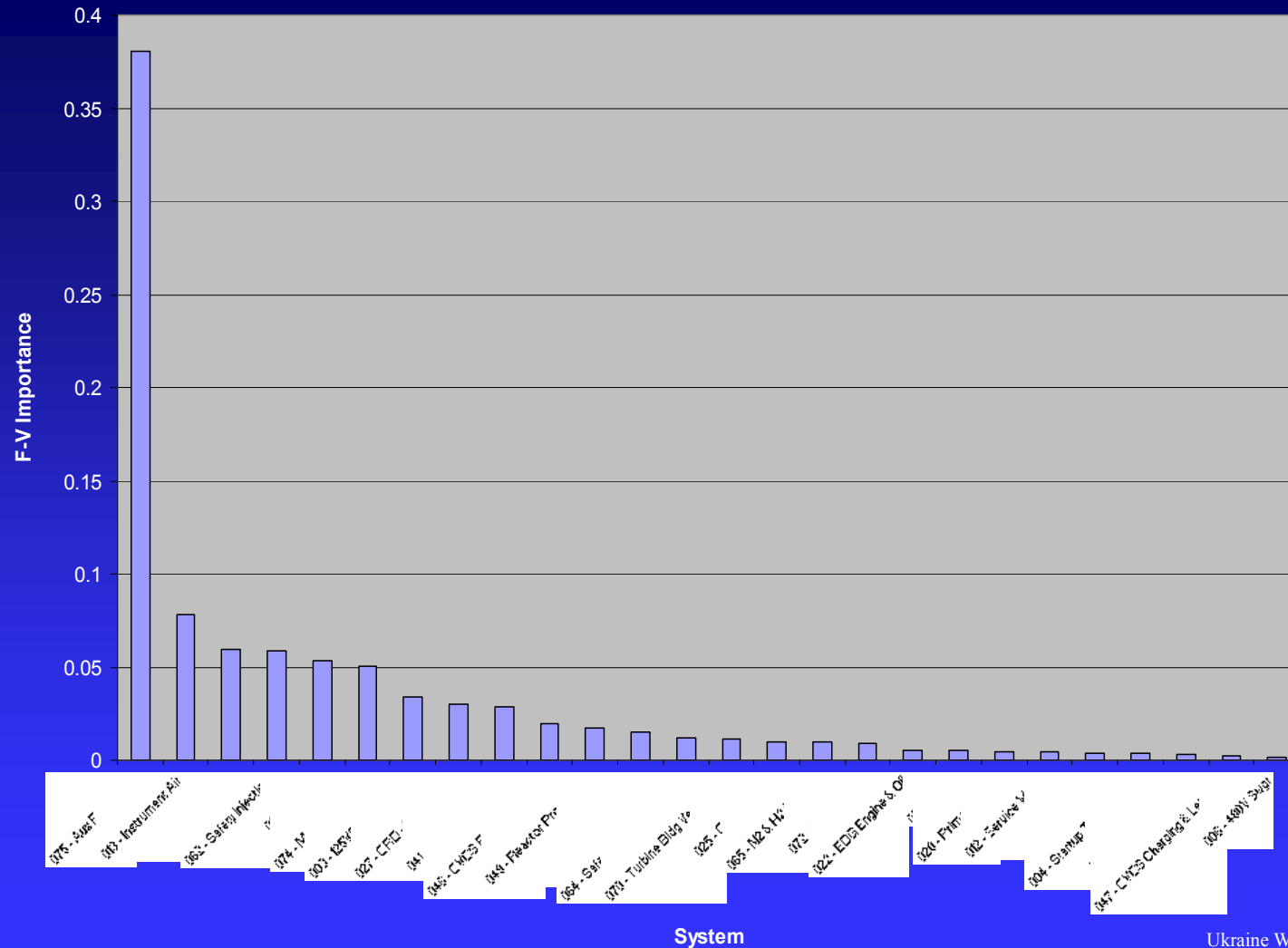
- Large FV if ...

- Component is relatively unreliable, or
- Component function is relatively important:
 - Few functional redundancies or relatively unreliable redundancies.

- Typical FVs (Turkey Point)

- Auxiliary Feedwater Pump	0.07
- Standby SG Feedwater Pump	0.06
- Instrument Air Compressor	0.03
- Diesel Generator	0.02
- Pilot-Operated Relief Valve (PORV)	0.01

System FVs



FV (cont.)

- Fussell-Vesely Importance is used primarily as a guide to prioritize resources, i.e., to show where improvements in reliability will result in the most improvements in safety.
- Fussell-Vesely Importance is also used with Risk Achievement Worth in ranking of systems, components, or operator actions.

Applications of Risk Importance Measures (RAW and FV)

- On-Line Maintenance
 - Optimize Maintenance Schedule to Minimize Risk
 - Monitor Risk
- Resource Prioritization
 - MOV/AOV Rankings (testing frequency)
 - Risk-Based ISI (inspection frequency)
 - Graded QA (degree of quality assurance)
- Operator Training
 - Focus Training on Critical Operator Actions

Questions?

The End



“According to this PSA, It’s strongly improbable that anything should ever happen anytime, anywhere.”

Ukraine Workshop, May 17-21, 2004