Integrating Dual Error Propagation into Dynamic Event Trees to Support Fission Battery Probabilistic Risk Assessments

Arjun Earthperson

Department of Nuclear Engineering
North Carolina State University
Raleigh, NC

Masters Defense

Committee Members: Dr. Mihai A. Diaconeasa, Dr. Nam Dinh, Mr. Steven R. Prescott, Dr. Ge Yang

Biography

- Graduated from University of California, Los Angeles (UCLA) in 2017 with a BS in electrical engineering.

- 2018 - 2020:
  - Developed PRA tools at The B. John Garrick Institute for the Risk Sciences, UCLA

PRA: Probabilistic Risk Assessment

Funding

- **INL LDRD -** “Quantitative Reliability Analysis for Unattended Operation of Fission Batteries”

- Nuclear Reactor Sustainment and Expanded Deployment - Fission Battery Initiative

- **Objective -** Develop R&D methods for enabling risk and reliability modeling of autonomous control systems and adversarial human actions for fission batteries.

INL: Idaho National Lab, LDRD: Lab Directed Research and Development

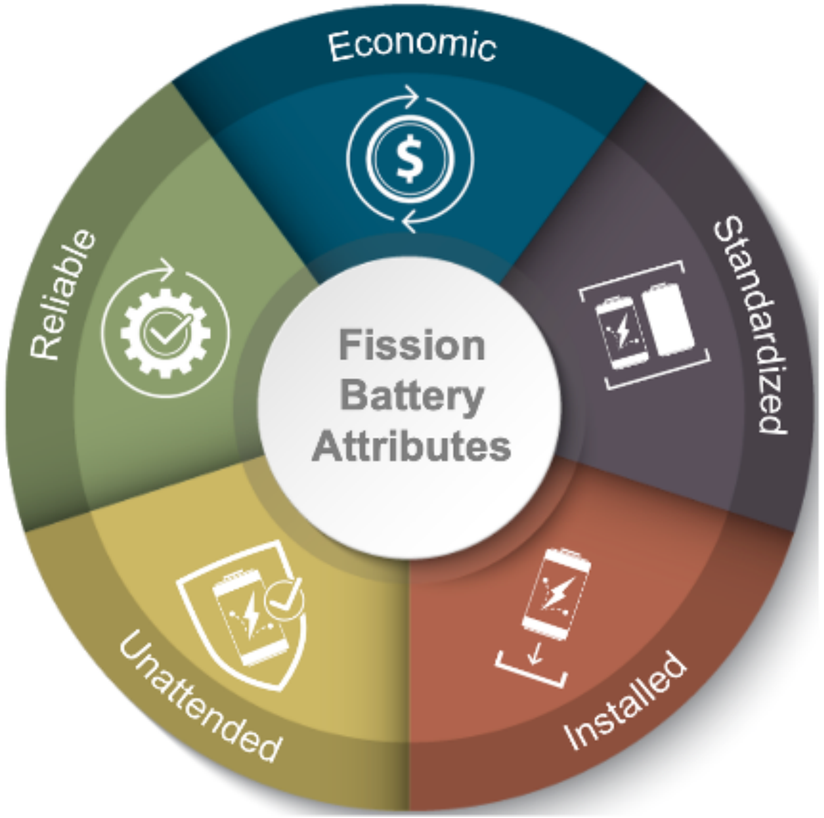
Outline

- **Introduction**
  - Fission Batteries
  - Need for Dynamic PRA
- **Methodology**
  - The Dual Error Propagation Method
- **Case Study**
  - System & Scenario
  - Three Modeling Variations
- **Results & Discussion**
  - Dynamic Event Trees with DEPM
  - DEPM vs Alternatives
- **Conclusion**
  - Limitations
  - Future Work

Fission Batteries

- Plug-&-play nuclear reactor
- Should function just like a battery

- **Attributes**
  - Economical
  - Standardized
  - Installed
  - Unattended
  - Reliable



source: INL/EXT-21-61275

The Dual Error Propagation Method

Motivation

- Need for accurately modeling digital I&C reliability.

- Some challenges include:
  - Exploding state-spaces
  - CCF effects
  - Hardware-Software combination failures

CCF: Common Cause Failure, I&C: Instrumentation and Control

What is DEPM?

- DEPM
  - is a method for mapping system states onto failure states.
  - combines two* Markov chains.
  - splits state transitions into control flows and data paths.
  - can be used for fault injection, error propagation analysis, etc.

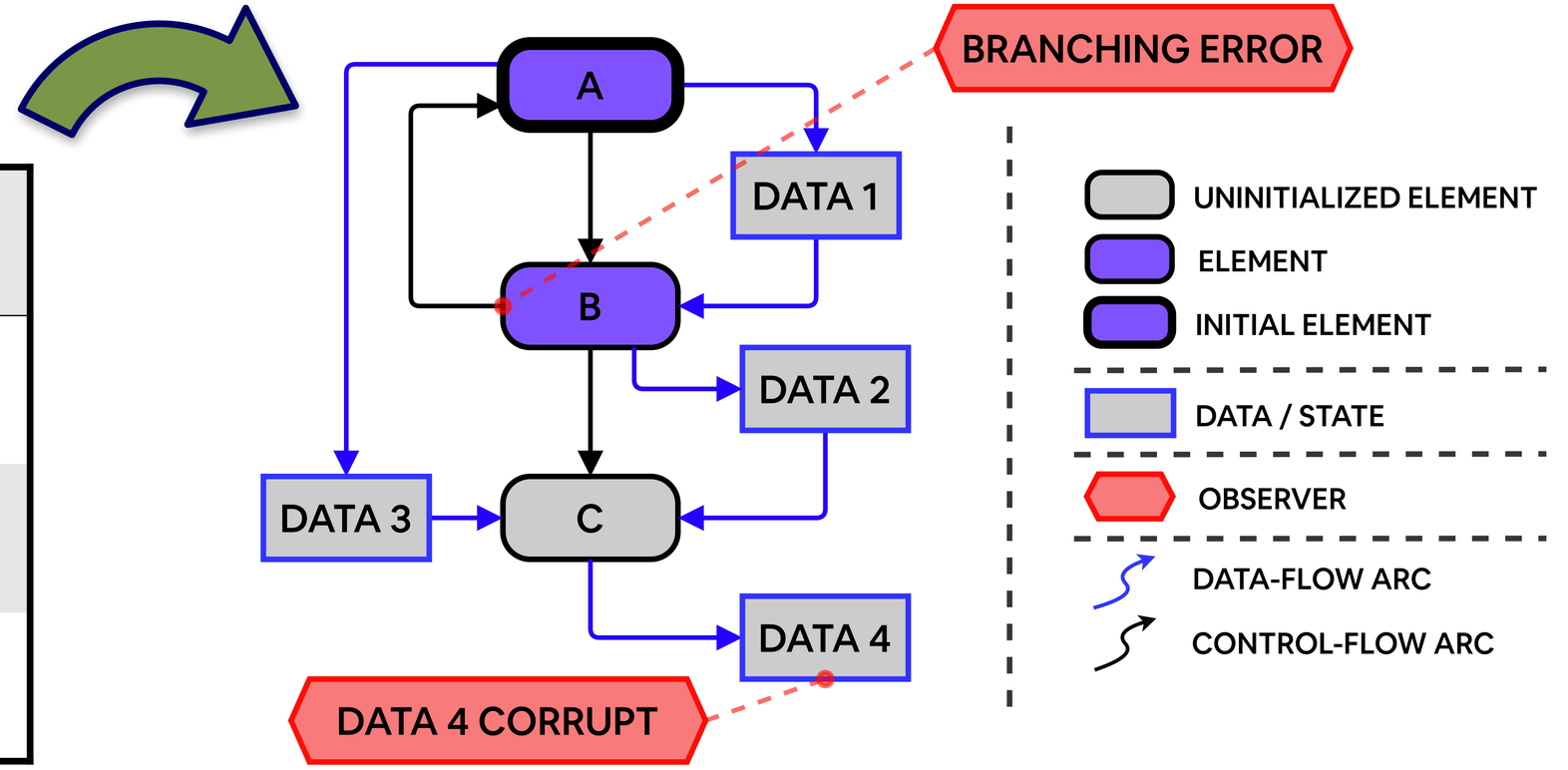
*hence, dual

A Software DEPM Example

#	Example Source Code
1	`{DATA_1, DATA_3} = function A();`
2	`DATA_2 = function B(DATA_1);`
3	`DATA_4 = function C(DATA_2, DATA_3);`

The Dual Error Propagation Method - Software Example

#	Example Source Code
1	`{DATA_1, DATA_3} = function A();`
2	`DATA_2 = function B(DATA_1);`
3	`DATA_4 = function C(DATA_2, DATA_3);`

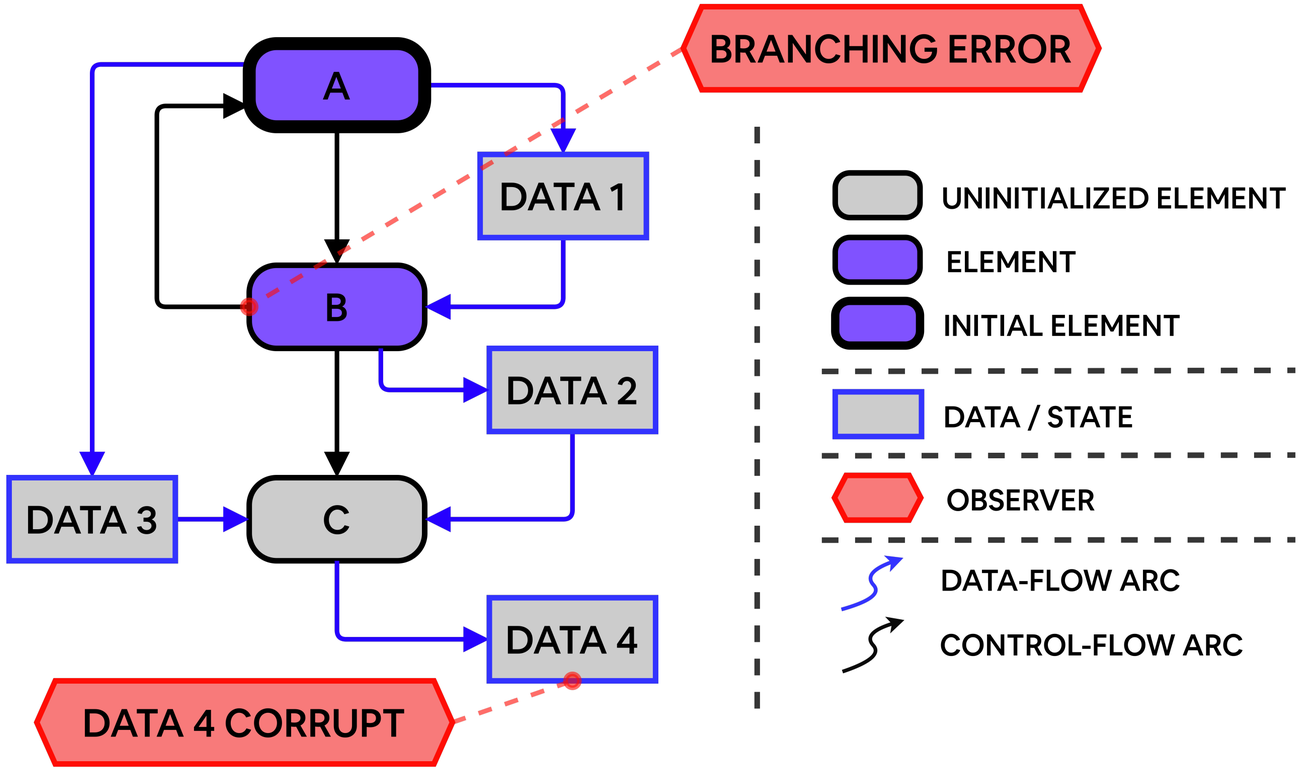


The Dual Error Propagation Method - Software Example

ID	Data Flow (DF)	Control Flow (CF)
A	always: • with P(0.9): DATA 1 = ok & DATA 3 = ok • with P(0.1): DATA 1 = error & DATA 3 = error	always: • with P(1.0): GOTO **B**

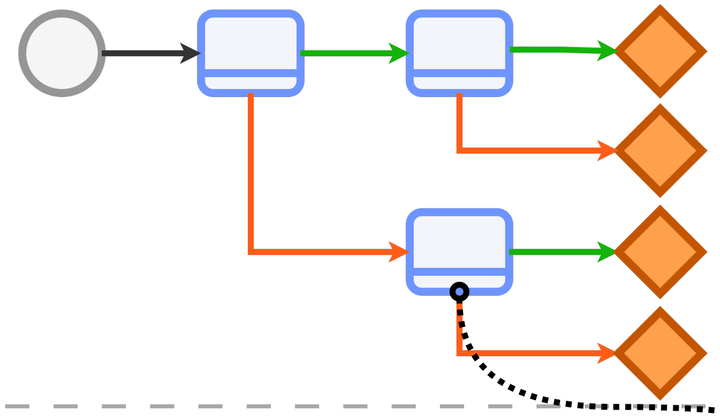
B	if DATA 1 = ok, then:
	• with P(1.0): DATA 2 = ok
	else:
	• with P(0.8): DATA 2 = ok
	• with P(0.2): DATA 2 = error
		always:
		• with P(0.3): GOTO **A**
		• with P(0.7): GOTO **C**

C	if DATA 2 = ok & DATA 3 = ok, then:
	• with P(1.0): DATA 4 = ok
	else:
	• with P(0.8): DATA 4 = error
	• with P(0.2): DATA 4 = ok
		–

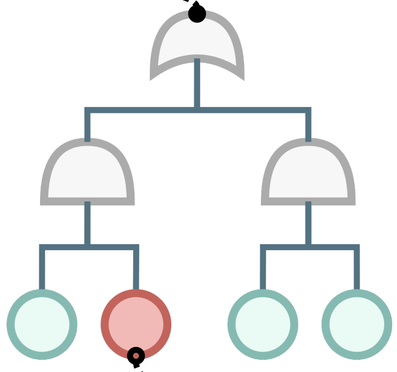


Observer Term	Logical Expression
BRANCHING ERROR	(CF = B) AND (CF′ = A)
DATA 4 CORRUPT	(DATA 4) != (‘OK’)

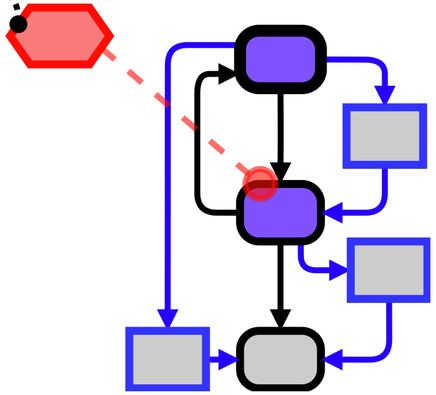
The Dual Error Propagation Method - Integration



Event Sequence Diagram / Event Tree



Fault Tree



Dual Error Propagation Graph

Case Study

Case Study - Scenario Description

- Wildfire
- Four Phases
  - Ignition
  - Propagation
  - Peak
  - Mitigation

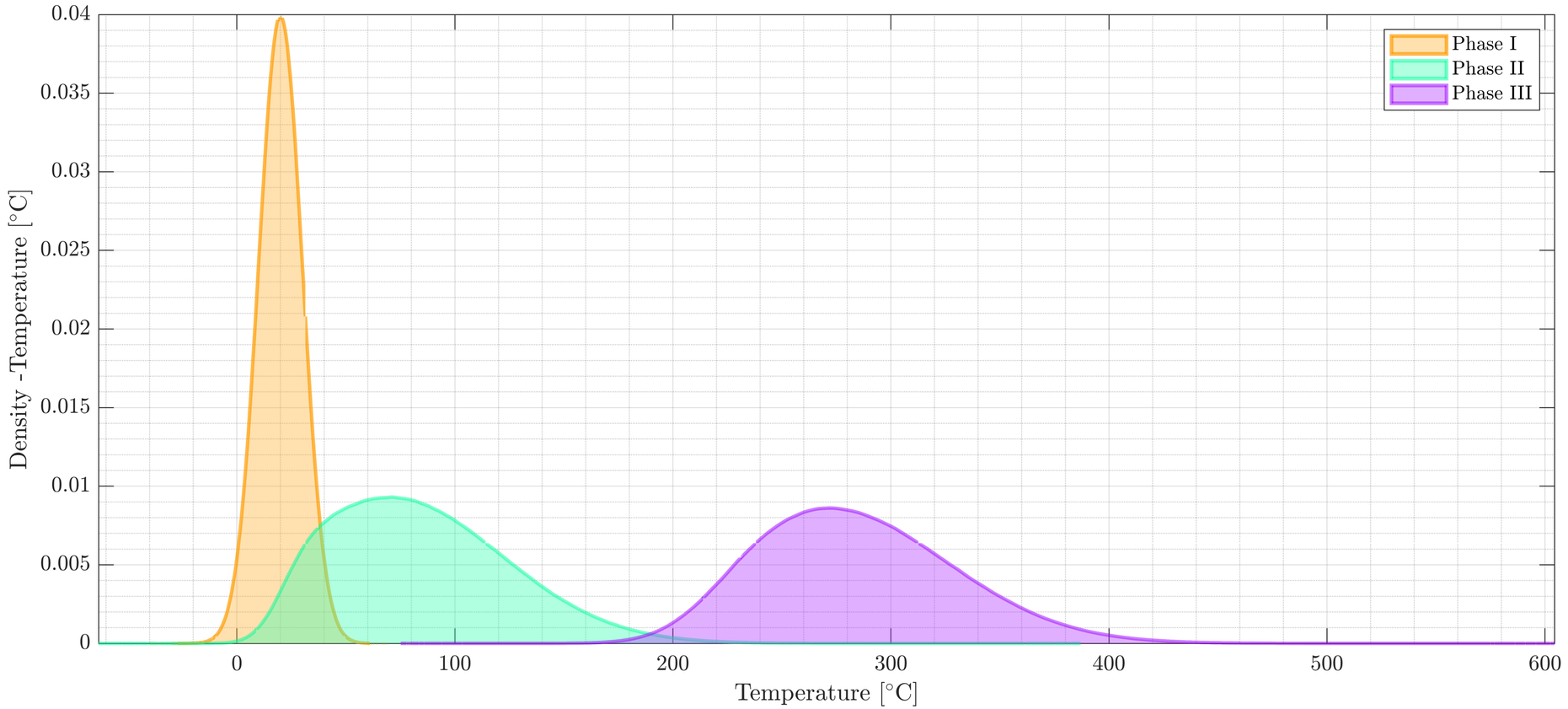


Table 4.3. Ambient temperature, phase durations and total elapsed time since ignition for fire phases I through IV.

Ø	Phase	Temperature [˚C]	Phase Duration [min]	Elapsed Time t_{Φ_i} $[min]$
I	Ignition	$\mathcal{N}(\mu = 20\,℃, \sigma = 10\,℃)$	$\mathcal{N}(\mu = 120m, \sigma = 10m)$	$0m$
II	Propagation	$\mathcal{N}(\mu = 75\,℃, \sigma = 45\,℃)$	$\mathcal{N}(\mu = 15m, \sigma = 5m)$	$\mathcal{N}(\mu = 120m, \sigma = 10m)$
III	Peak	$\mathcal{N}(\mu = 275\,℃, \sigma = 50\,℃)$	$\mathcal{N}(\mu = 30m, \sigma = 10m)$	$\mathcal{N}(\mu = 135m, \sigma \approx 11.2m)$
IV	Mitigation	$\mathcal{N}(\mu = 20\,℃, \sigma = 10\,℃)$	–	$\mathcal{N}(\mu = 165m, \sigma = 15m)$

Case Study - Scenario Description

- However, notification of wildfire event may be delayed
- Lagged notification is modeled as Phase Alert Delay

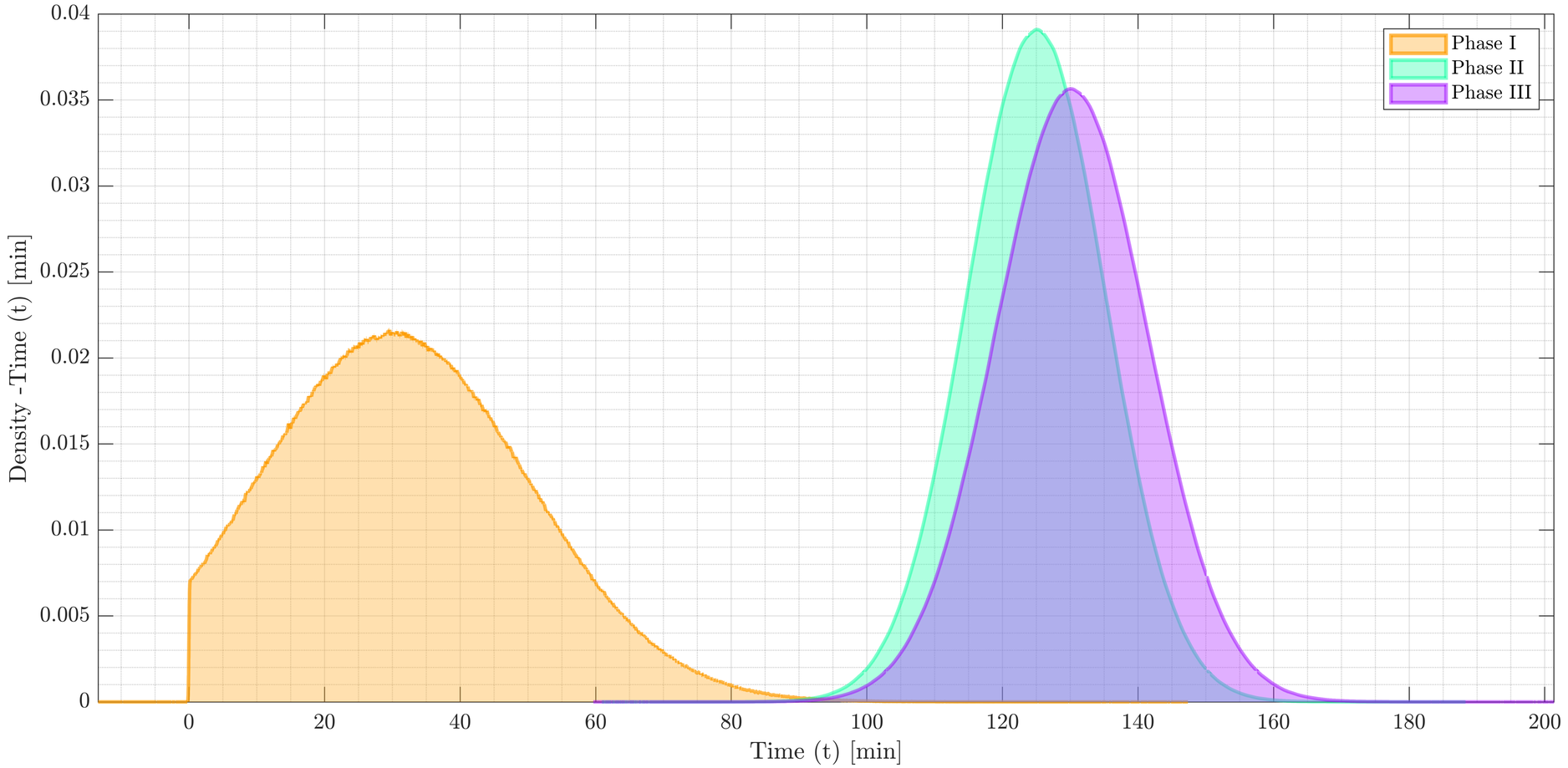


Table 4.4: Alert delays and elapsed time for fire alerts during phases I, II, and III.

Ø	Phase	Phase Alert Delay $\delta_i t\ [min]$	Elapsed Time $t_{\alpha_i}[min]$
I	Ignition	$\mathcal{N}(\mu = 30\ min\ , \sigma = 20\ min)$	$\mathcal{N}(\mu = 30\ min\ , \sigma = 20\ min)$
II	Propagation	$\mathcal{N}(\mu = 5\ min\ , \sigma = 2\ min)$	$\mathcal{N}(\mu = 125\ min\ , \sigma \approx 10.2\ min)$
III	Peak	$\mathcal{N}(\mu = 10\ sec\ , \sigma = 5\ sec)$	$\mathcal{N}(\mu \approx 135.17\ min\ , \sigma \approx 11.1\ min)$

Case Study - Scenario Description

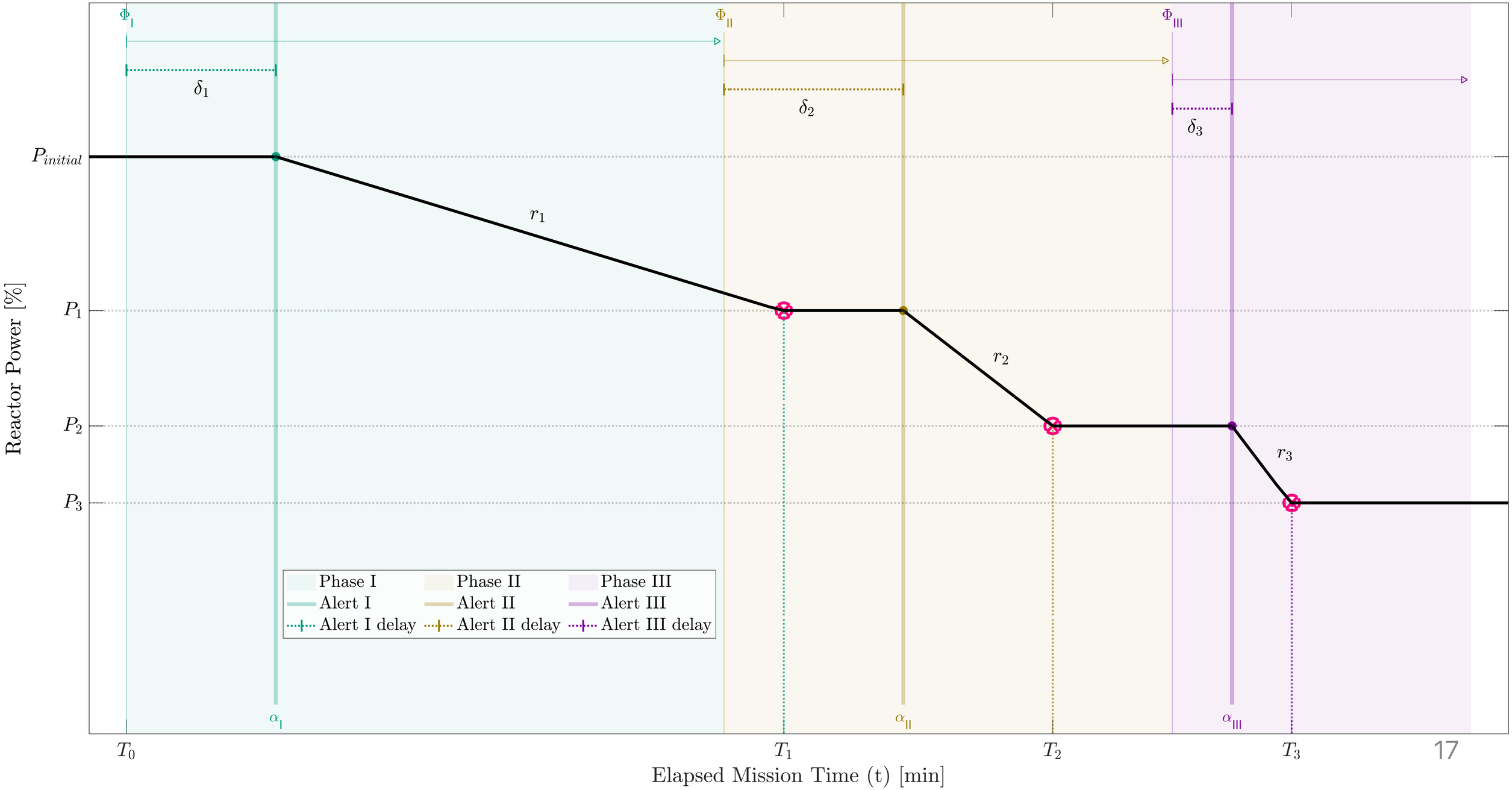
Fission Battery Response

- Graded Shutdown
- Success Criteria - Target power levels and times

Table 4.2: Success Criteria Definition for Reactor Power Level Reduction Events

Ø	Phase	Target Power $P(T_i)$ [%]	Power Reduction Rate r_i [%/time]	Time to Target Power [duration]	Elapsed Time at Target Power T_i $[min]$
I	Ignition	50%	50% *per hour*	60 *min*	$\mathcal{N}(\mu \approx 92.8\,, \sigma \approx 17.6)$
II	Propagation	20%	6% *per min*	5 *min*	$\mathcal{N}(\mu \approx 130.0, \sigma \approx 10.2)$
III	Peak	0%	1% *per sec*	20 *sec*	$\mathcal{N}(\mu \approx 130.8, \sigma \approx 11.1)$

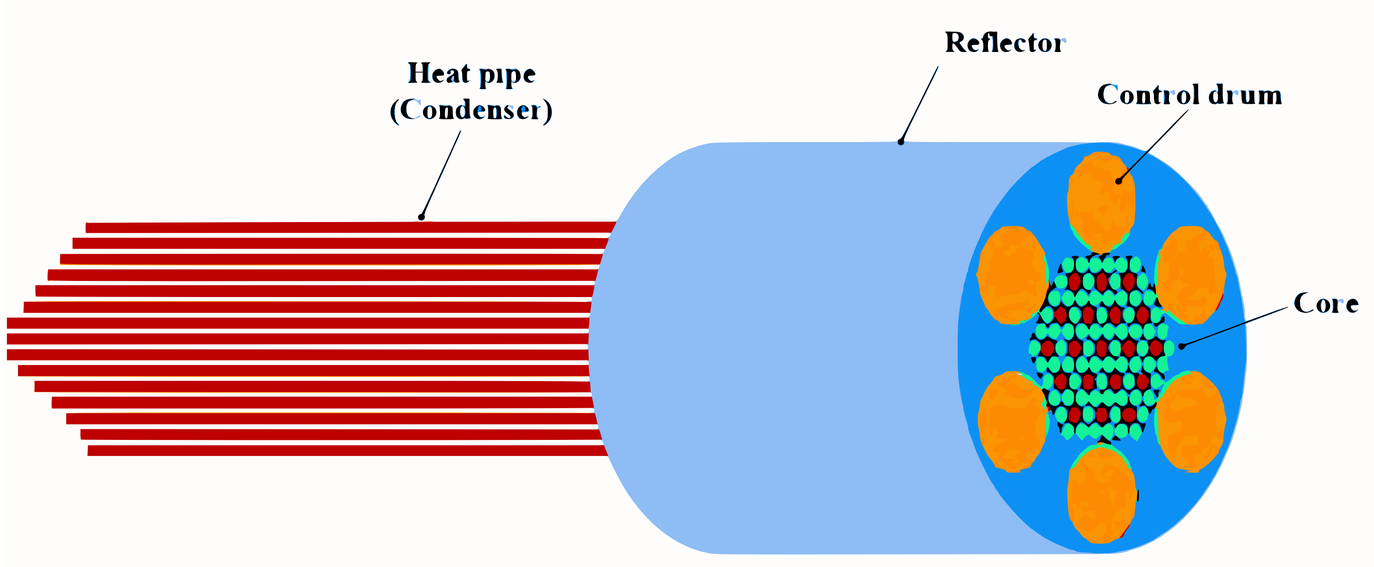
Graded Shutdown - Target Reactor Power Levels



Case Study - System Description

Reactor Control System (RCS)

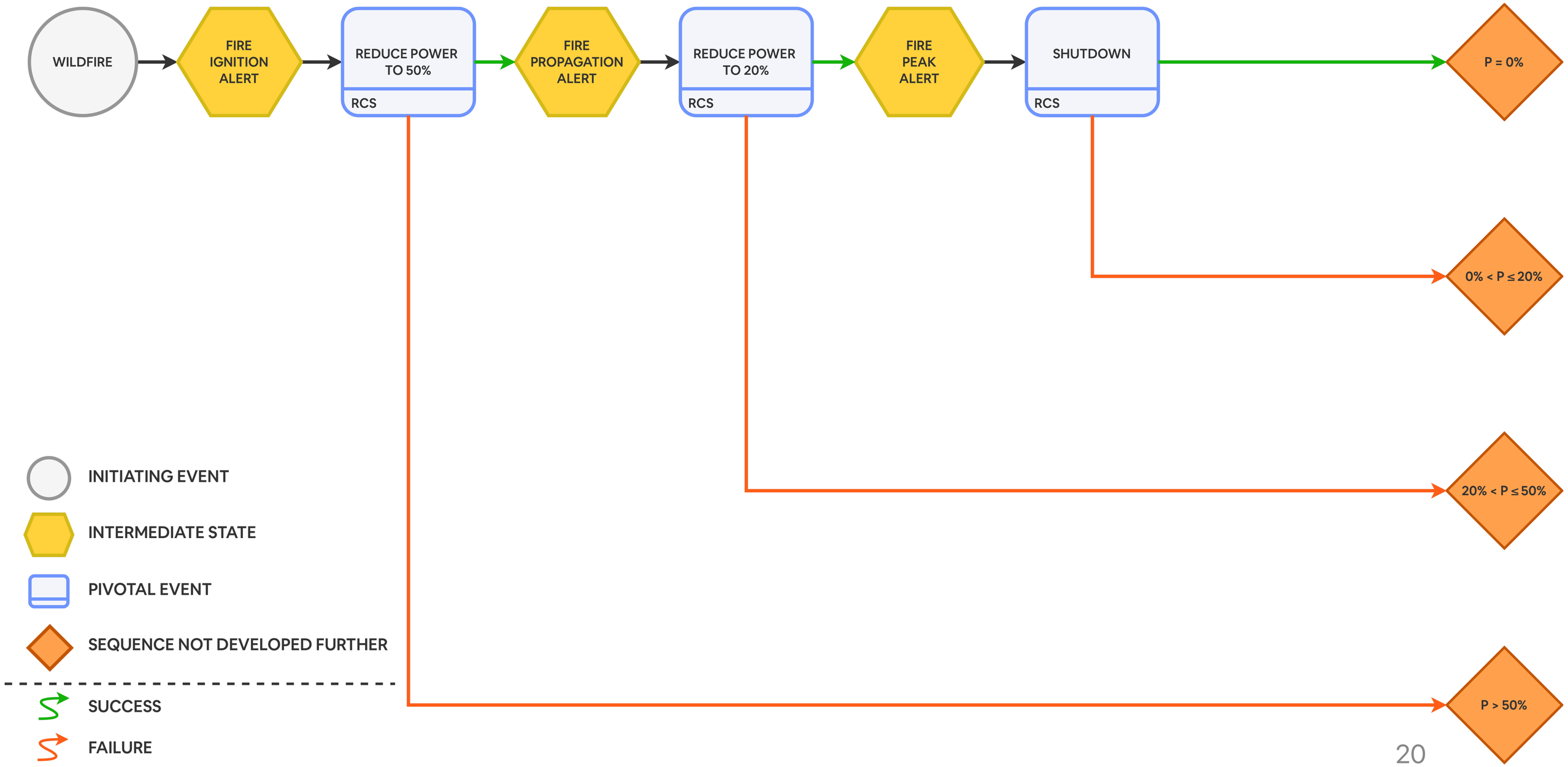
- Fully automated control
- Actuates 6 Control Drums
- Uses 3 PLCs for redundancy
- Each PLC implements a software PID loop - 6 total PID Loops



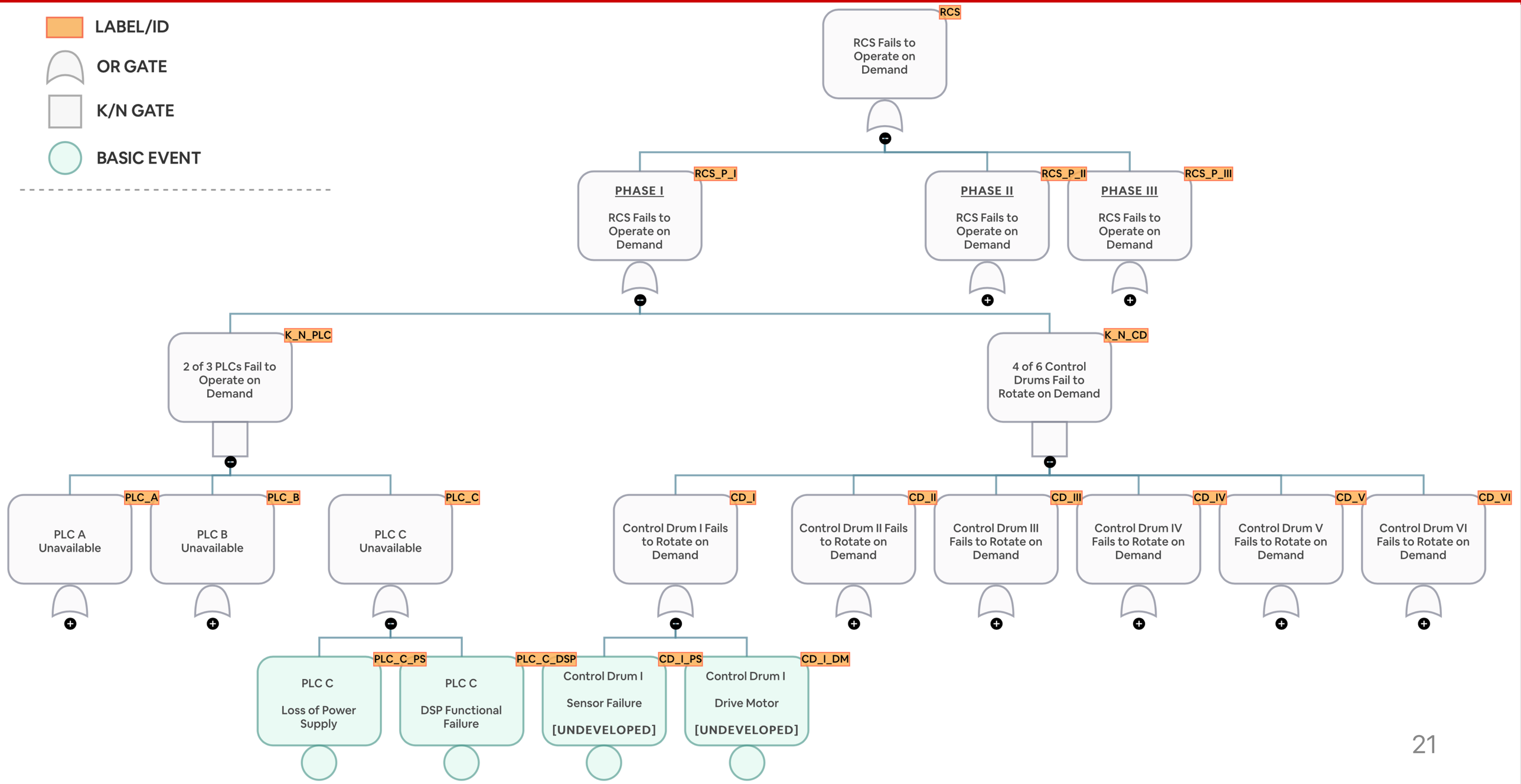
PLC: Programmable Logic Controller, PID: Proportional Integral Derivate

CASE 1: Event Sequence Diagram / Fault Tree Approach

CASE 1: RCS Power Down ESD



CASE 1: RCS Unavailability Fault Tree



CASE 1: DSP Hardware Failure Rate Estimation

#	TMS320 Variant	Failure Rate $[failures/hr]$
1	C25-GBL	1.80×10^{-9}
2	C28-343-ZFEQ	1.82×10^{-9}
3	C55-34-AZAY10	2.10×10^{-9}
4	C28-01-PZA	2.26×10^{-9}
5	C67-48-EZWT4	4.50×10^{-9}
6	C20-3PZ	5.60×10^{-9}
7	C66-78ACYP	6.55×10^{-9}
8	C20-6PZ80	14.40×10^{-9}

$$\lambda_{derated} = \mathcal{N}(\mu \approx 5.89, \sigma \approx 3.50) \times 10^{-9}$$

Arrhenius Model

$$AF_{DSP} = exp\left[\left(\frac{-E_a}{k_B}\right)\left(\frac{1}{T_{test}} - \frac{1}{T_{phase}}\right)\right]$$

$$\lambda_{DSP} = AF_{DSP} \times \lambda_{derated}$$

$$E_a = \mathcal{U}(0.45, 1.00)$$

$$T_{test} = 328.15\ K$$

CASE 1: DSP Temperate Adjusted Failure Rate

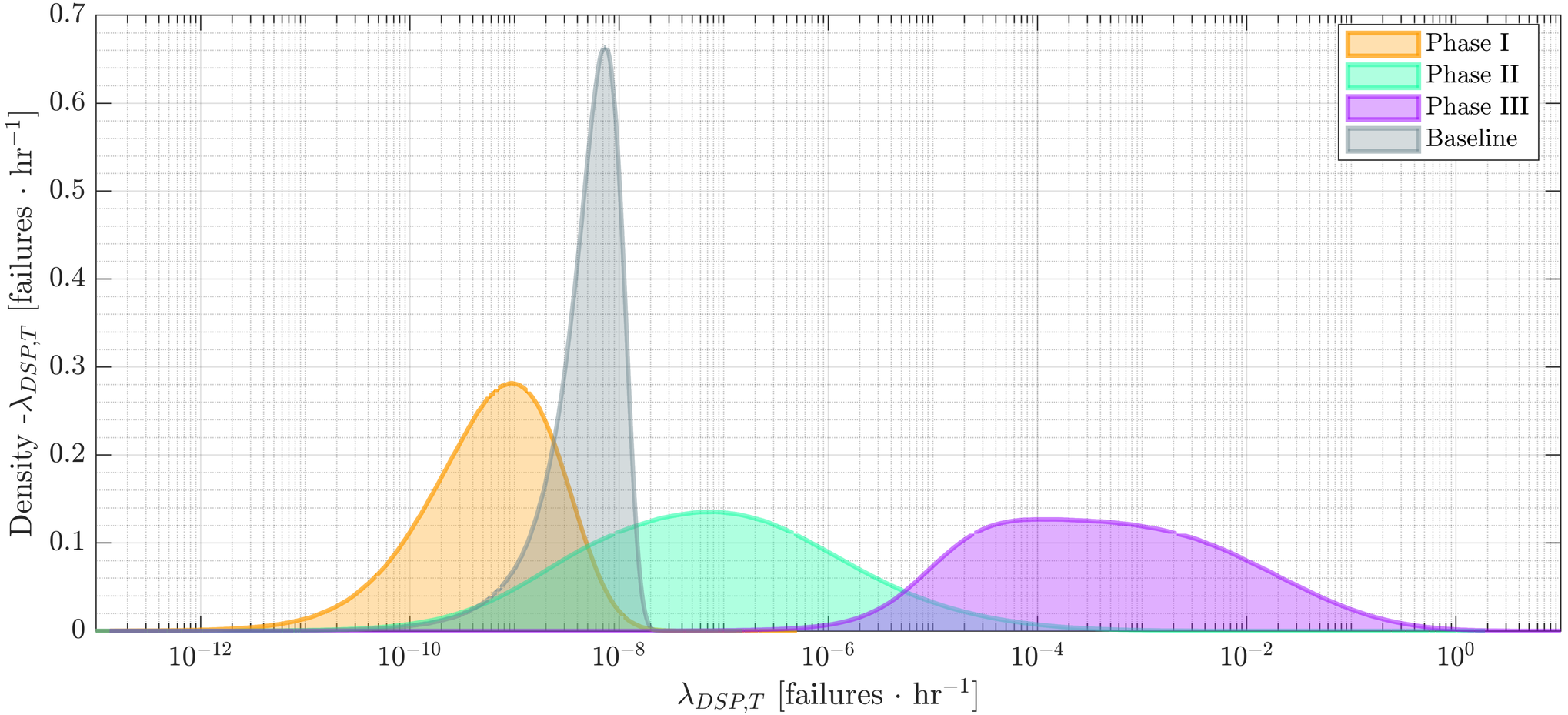


Table 4.6. Phase-dependent, temperature adjusted, digital signal processor failure rates.

Ø	Phase	Acceleration Factor AF_{DSP}	DSP failure rate λ_{DSP} $[failures/hr]$
-	Baseline	-	$\mathcal{N}(\mu \approx 5.89 \times 10^{-9}, \sigma \approx 3.50 \times 10^{-9})$
I	Ignition	$LN(\bar{m} \approx 2.57 \times 10^{-1}, EF \approx 7.36)$	$LN(\bar{m} \approx 1.74 \times 10^{-9}, EF \approx 11.9)$
II	Propagation	$LN(\bar{m} \approx 7.01 \times 10^{2}, EF \approx 90.2)$	$LN(\bar{m} \approx 4.73 \times 10^{-6}, EF \approx 114)$
III	Peak	$LN(\bar{m} \approx 2.82 \times 10^{6}, EF \approx 73.1)$	$LN(\bar{m} \approx 1.90 \times 10^{-2}, EF \approx 93.7)$

CASE 1: Temperature Dependent Hardware Failure Rates

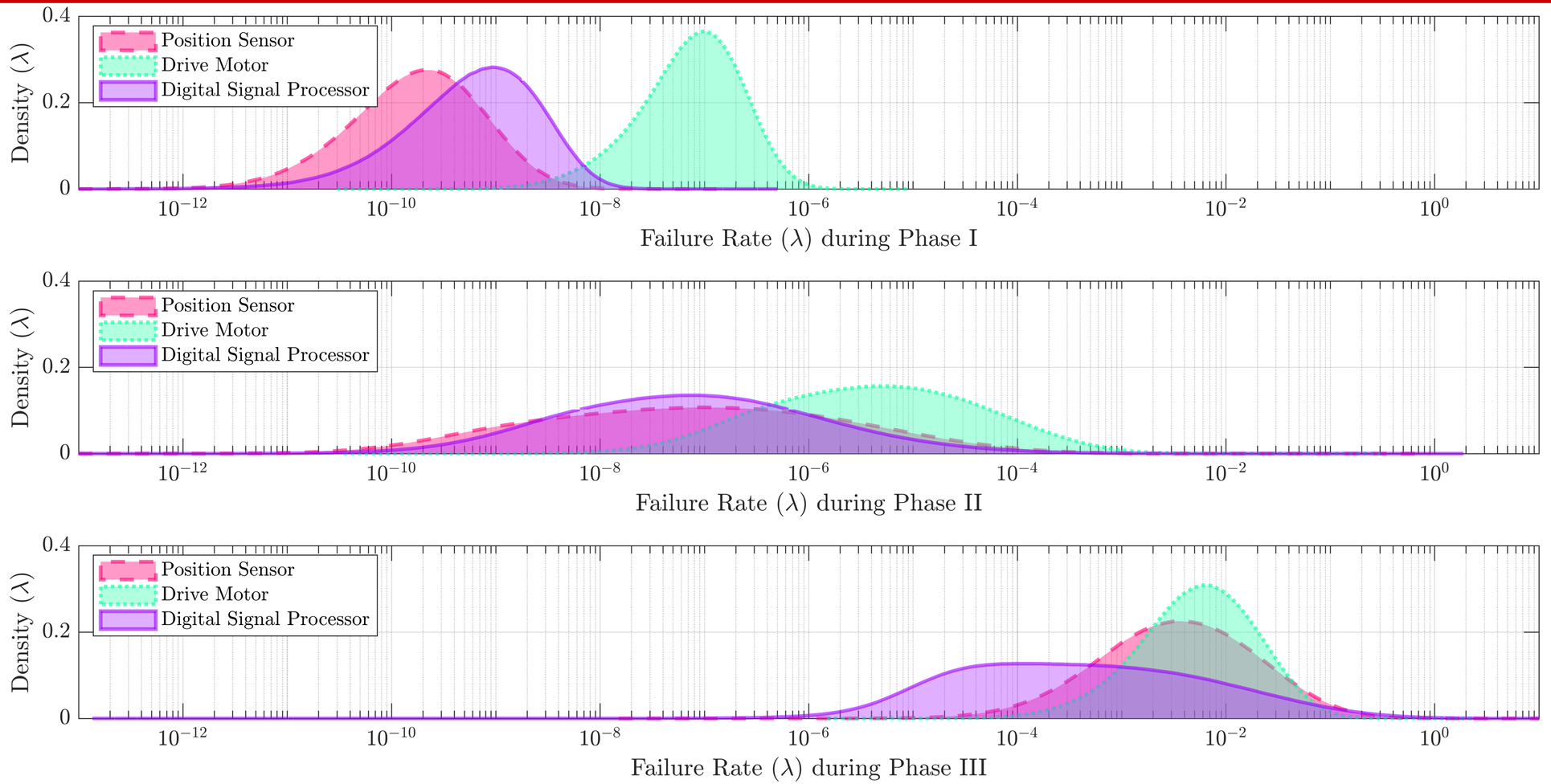


Table 4.8: Temperature Dependent Failure Rates for Programmable Logic Controller, Control Drum Failure Modes

Phase	Phase I	Phase II	Phase III
Position Sensor	$\mathcal{LN}(\bar{m} \approx 4.93 \times 10^{-10}, EF \approx 11.3)$	$\mathcal{LN}(\bar{m} \approx 2.26 \times 10^{-5}, EF \approx 262)$	$\mathcal{LN}(\bar{m} \approx 1.49 \times 10^{-2}, EF \approx 17.2)$
Drive Motor	$\mathcal{LN}(\bar{m} \approx 1.38 \times 10^{-7}, EF \approx 6.73)$	$\mathcal{LN}(\bar{m} \approx 6.31 \times 10^{-5}, EF \approx 47.0)$	$\mathcal{LN}(\bar{m} \approx 1.22 \times 10^{-2}, EF \approx 8.58)$
PLC DSP	$\mathcal{LN}(\bar{m} \approx 1.74 \times 10^{-9}, EF \approx 11.9)$	$\mathcal{LN}(\bar{m} \approx 4.73 \times 10^{-6}, EF \approx 114)$	$\mathcal{LN}(\bar{m} \approx 1.90 \times 10^{-2}, EF \approx 96.8)$

CASE 1: Temperature Dependent Hardware Failure Rates

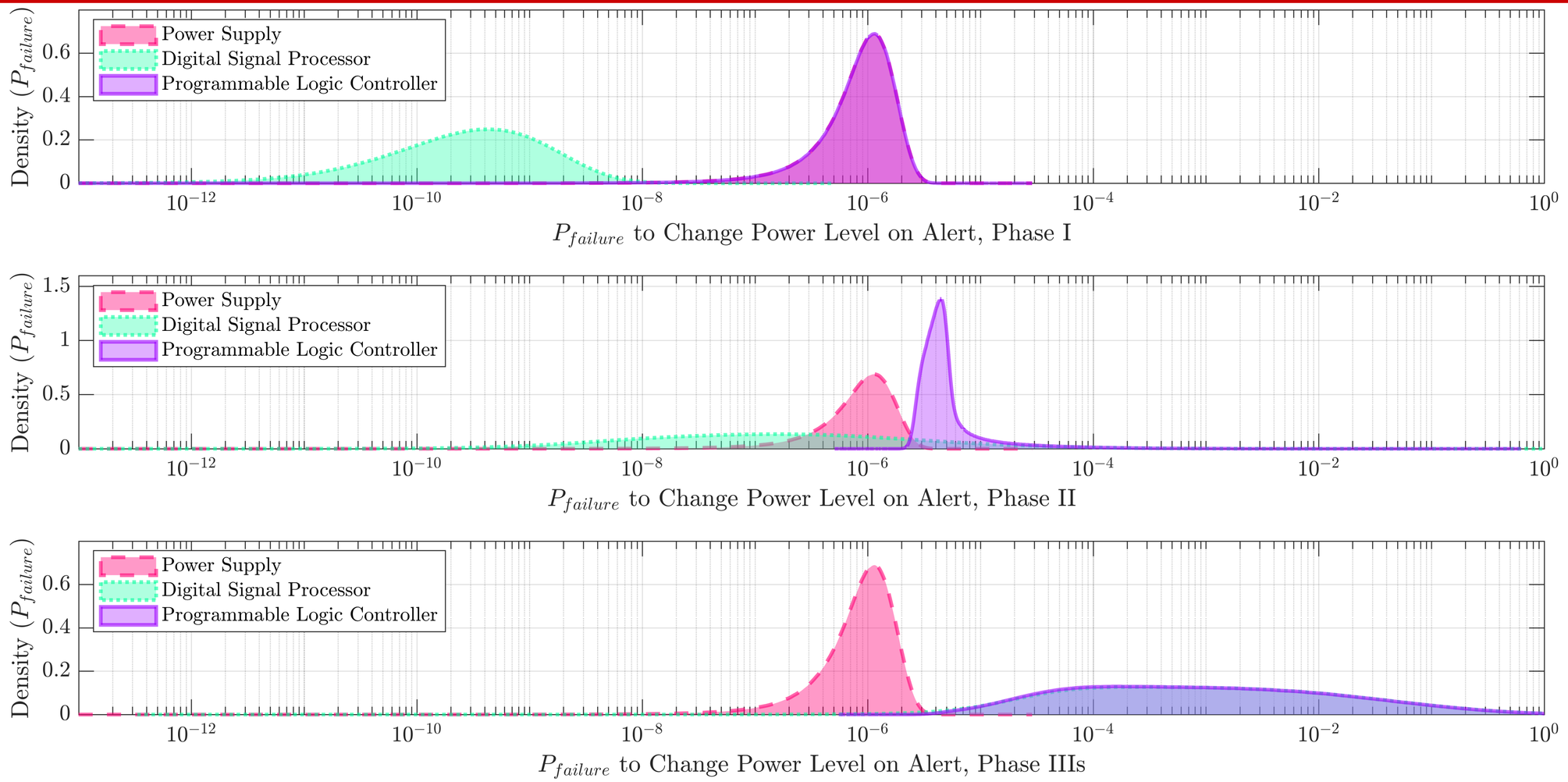


Table 4.9: Intermediate Event Probabilities, Programmable Logic Controller Failure to Change Power Level on Phase Alert

Phase	**Phase I**	**Phase II**	**Phase III**
PLC Failure	$\mathcal{LN}(\bar{m} \approx 1.10 \times 10^{-6}, EF \approx 3.90)$	$\mathcal{LN}(\bar{m} \approx 6.90 \times 10^{-6}, EF \approx 3.52)$	$\mathcal{LN}(\bar{m} \approx 3.19 \times 10^{-2}, EF \approx 78.2)$
Power Supply	$\mathcal{LN}(\bar{m} \approx 1.10 \times 10^{-6}, EF \approx 3.90)$	$\mathcal{LN}(\bar{m} \approx 3.77 \times 10^{-6}, EF \approx 1.41)$	$\mathcal{LN}(\bar{m} \approx 3.93 \times 10^{-6}, EF \approx 1.41)$
DSP Failure	$\mathcal{LN}(\bar{m} \approx 1.06 \times 10^{-9}, EF \approx 16.7)$	$\mathcal{LN}(\bar{m} \approx 9.86 \times 10^{-6}, EF \approx 115)$	$\mathcal{LN}(\bar{m} \approx 3.83 \times 10^{-2}, EF \approx 90.3)$

CASE 1: Temperature Dependent Hardware Failure Rates

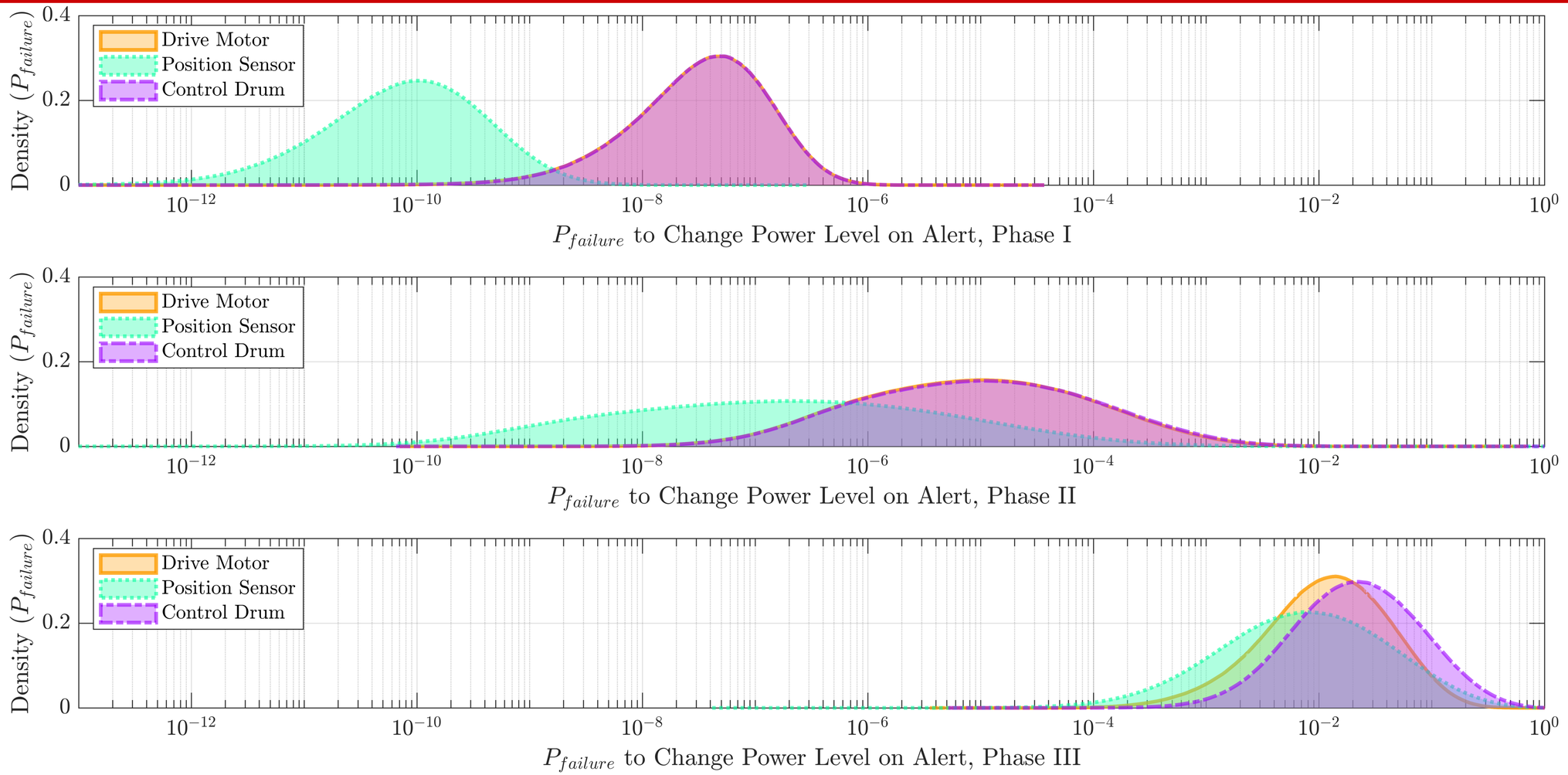


Table 4.10 Control Drum, Drive Motor, Position Sensor, failure to change power level on demand, by phase

Phase	Phase I	Phase II	Phase III
CD Failure	$\mathcal{LN}(\bar{m} \approx 8.42 \times 10^{-8}, EF \approx 10.1)$	$\mathcal{LN}(\bar{m} \approx 1.48 \times 10^{-4}, EF \approx 49.3)$	$\mathcal{LN}(\bar{m} \approx 4.95 \times 10^{-2}, EF \approx 8.48)$
Position Sensor	$\mathcal{LN}(\bar{m} \approx 3.00 \times 10^{-10}, EF \approx 15.8)$	$\mathcal{LN}(\bar{m} \approx 4.70 \times 10^{-5}, EF \approx 263)$	$\mathcal{LN}(\bar{m} \approx 3.08 \times 10^{-2}, EF \approx 16.7)$
Drive Motor	$\mathcal{LN}(\bar{m} \approx 8.41 \times 10^{-8}, EF \approx 10.2)$	$\mathcal{LN}(\bar{m} \approx 1.31 \times 10^{-4}, EF \approx 47.1)$	$\mathcal{LN}(\bar{m} \approx 2.58 \times 10^{-2}, EF \approx 8.44)$

CASE 1: RCS Unavailability Fault Tree

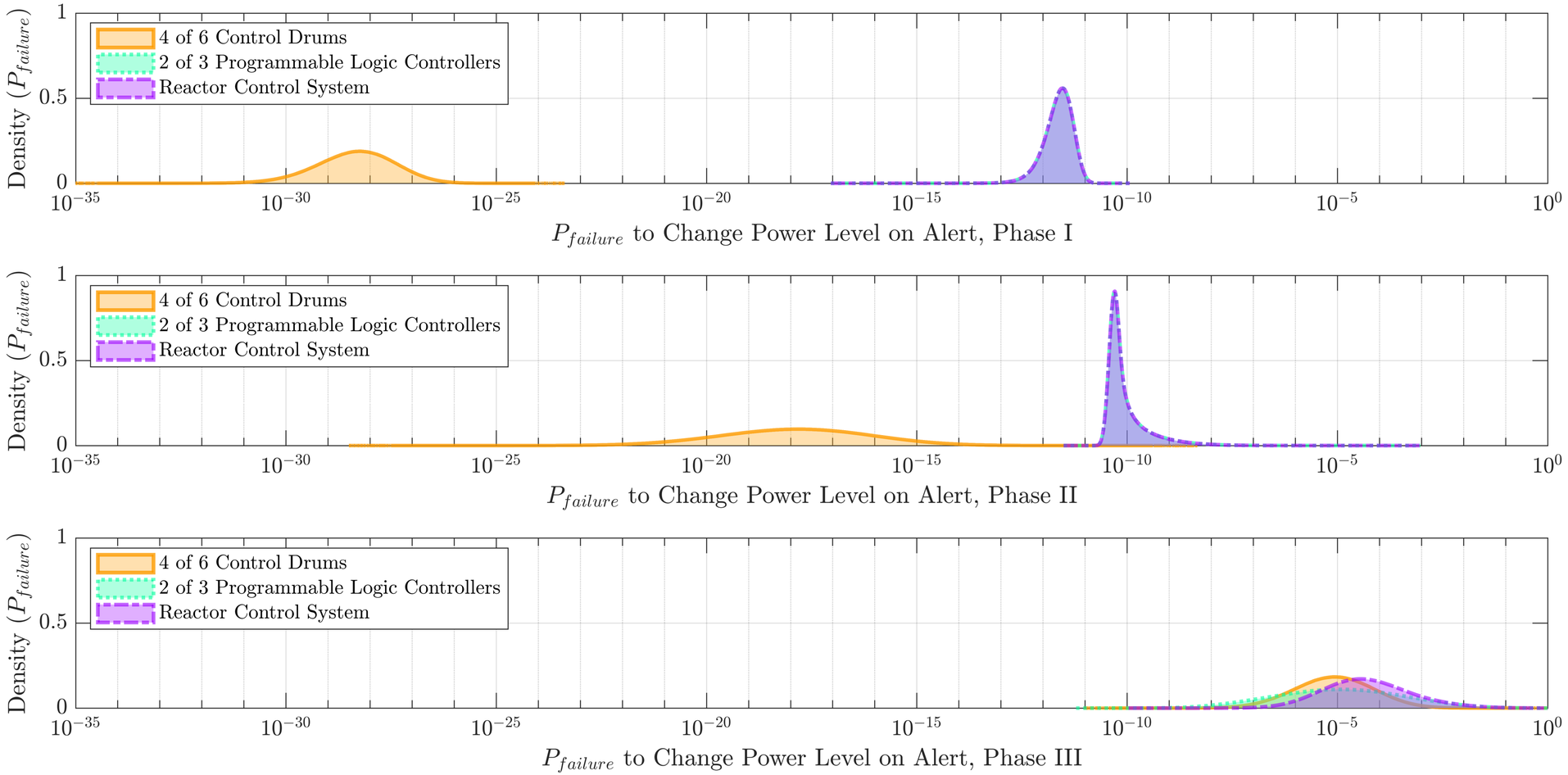


Table 4.11: Top, Intermediate Event Probabilities, Reactor Control System Failure to Change Power Level on Demand

Phase	**Phase I**	**Phase II**	**Phase III**
RCS Failure	$\mathcal{LN}(\overline{m} \approx 3.09 \times 10^{-12}, EF \approx 3.65)$	$\mathcal{LN}(\overline{m} \approx 1.68 \times 10^{-10}, EF \approx 6.20)$	$\mathcal{LN}(\overline{m} \approx 8.07 \times 10^{-4}, EF \approx 44.9)$
4 of 6 CDs Fail	$\mathcal{LN}(\overline{m} \approx 4.40 \times 10^{-28}, EF \approx 34.1)$	$\mathcal{LN}(\overline{m} \approx 5.34 \times 10^{-15}, EF \approx 831)$	$\mathcal{LN}(\overline{m} \approx 8.14 \times 10^{-5}, EF \approx 34.4)$
2 of 3 PLCs	$\mathcal{LN}(\overline{m} \approx 3.09 \times 10^{-12}, EF \approx 3.65)$	$\mathcal{LN}(\overline{m} \approx 1.68 \times 10^{-10}, EF \approx 6.20)$	$\mathcal{LN}(\overline{m} \approx 3.71 \times 10^{-3}, EF \approx 274)$

CASE 1: RCS Power Down End-State Likelihoods

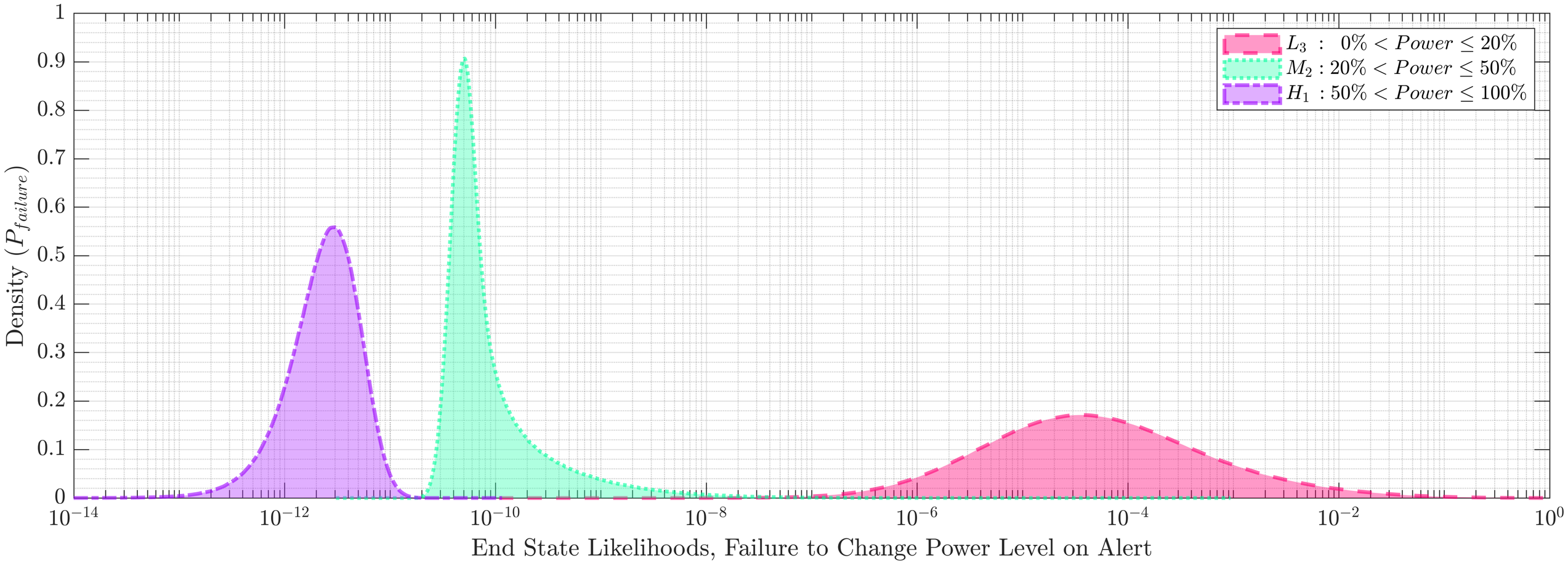
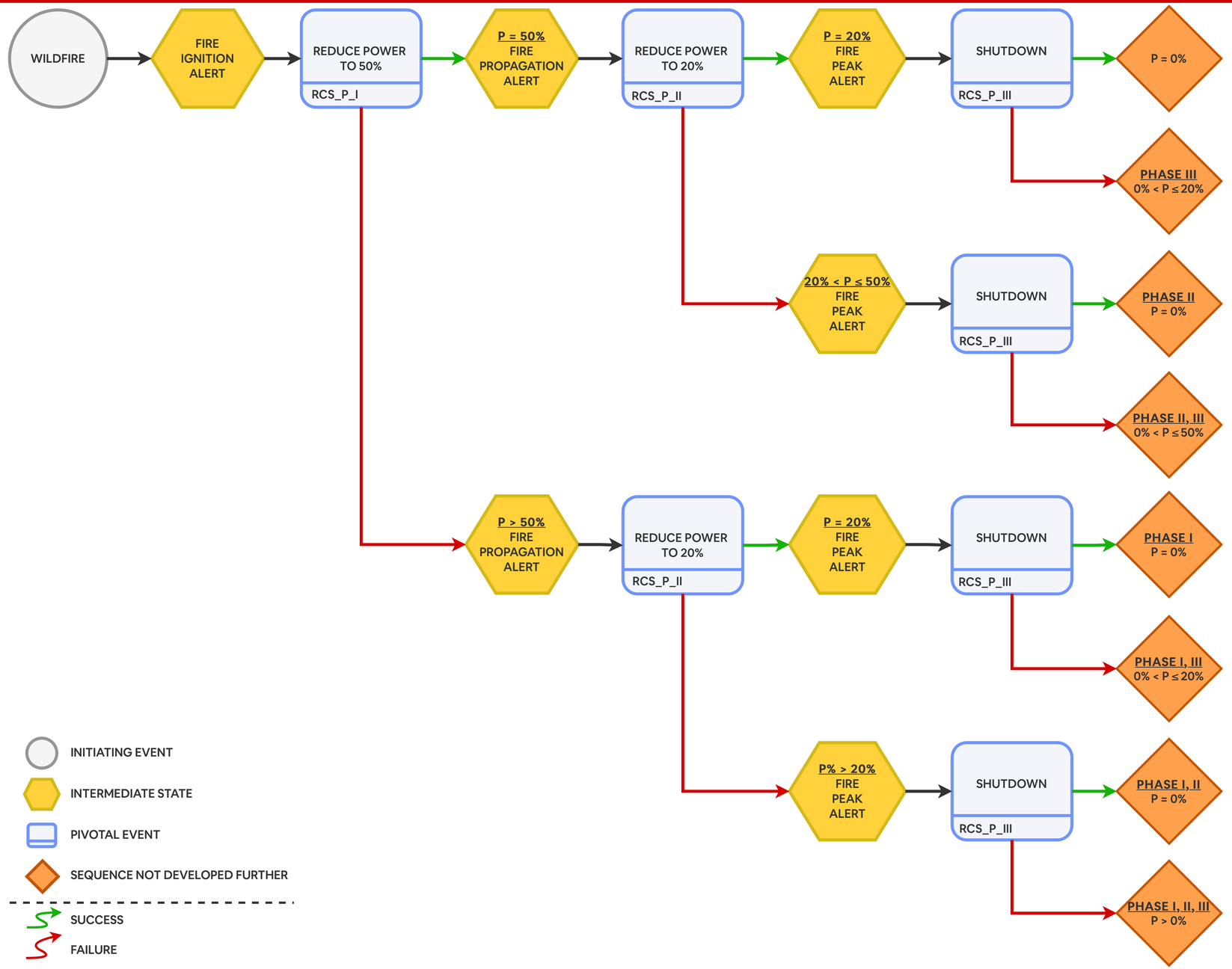


Table 4.12: Traditional PRA: Reactor power level likelihoods following shutdown, given external fire event.

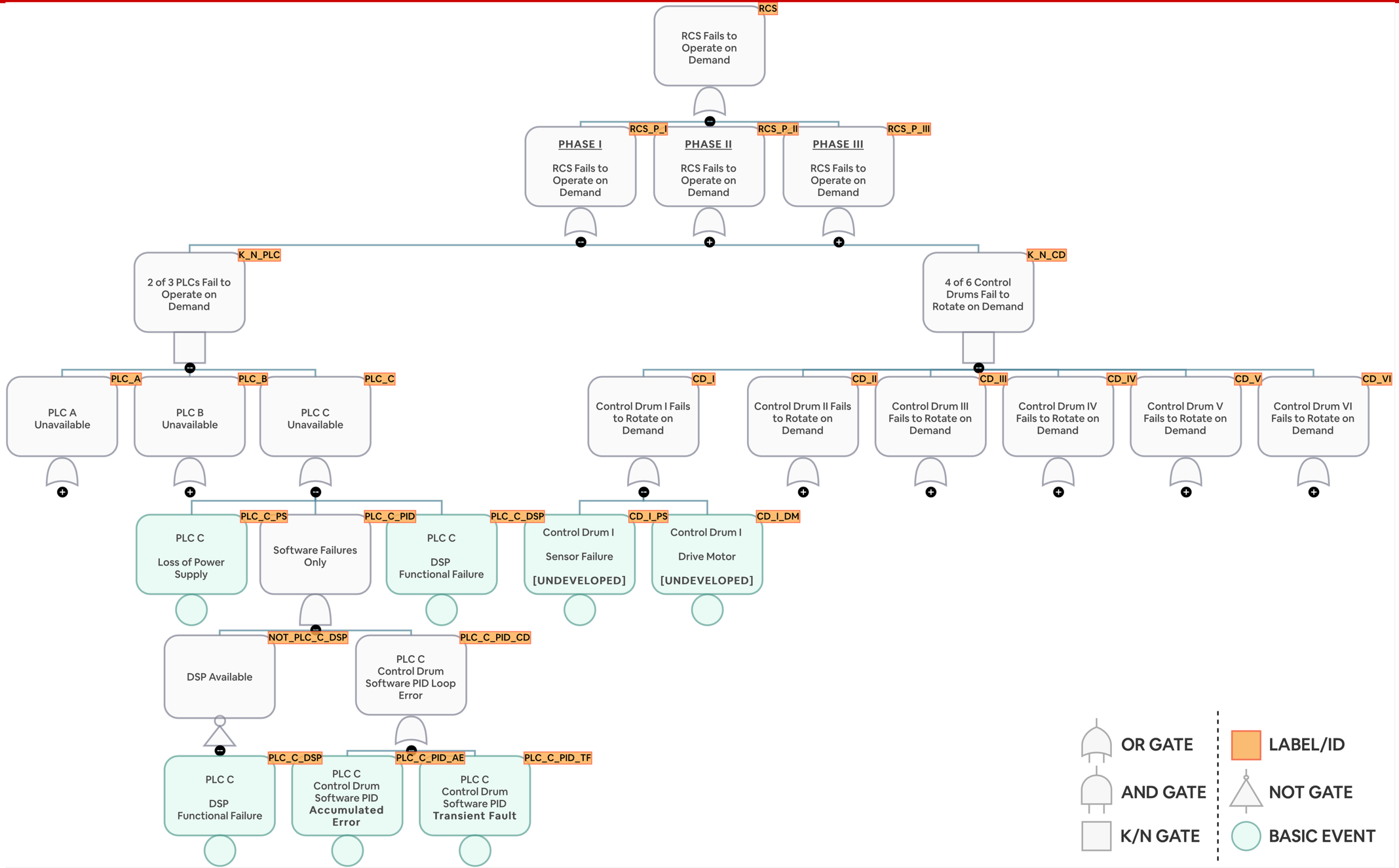
ID[5]	End State	P(End State)
S_0	Shutdown	$\mathcal{LN}(\bar{m} \approx 9.99 \times 10^{-1}, EF \approx 1.02)$
L_3	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 8.07 \times 10^{-4}, EF \approx 44.9)$
M_2	20% < Power ≤ 50%	$\mathcal{LN}(\bar{m} \approx 1.68 \times 10^{-10}, EF \approx 6.20)$
H_1	50% < Power ≤ 100%	$\mathcal{LN}(\bar{m} \approx 3.09 \times 10^{-12}, EF \approx 3.65)$

CASE 2: ESD/FT with DEPM & Recoveries

CASE 2: Reactor Control System Power Down ESD



CASE 2: RCS Unavailability Fault Tree



CASE 2: PID Software Failure Rate Estimation

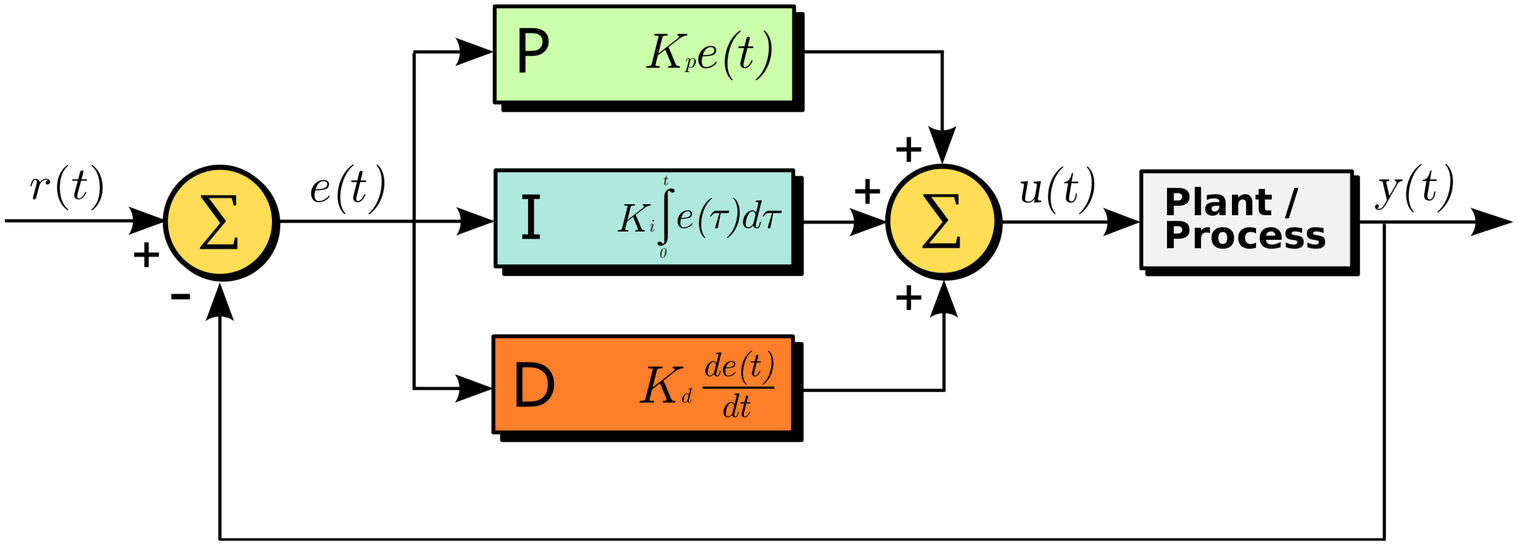


Table 4.14: Assembler code for proposed zero-order PID control algorithm.

define float @__calculate__(float %SET_POINT, %P_{VAR}, %K_p, %K_i, %K_d, %dT)		
0:	%C_{ERR}	**fsub** %SET_POINT, %P_{VAR}
1:	%P_{ERR}	load float, float* @P_{ERR}
2:	%D_{ERR}	**fsub** %C_{ERR}, %P_{ERR}
3:	%OUTPUT	**fmul** %K_d, %D_{ERR}
4:		store %C_{ERR}, float* @P_{ERR}
5:	%tmp1	**fmul** %K_p, %C_{ERR}
6:	%OUTPUT	**fadd** %OUTPUT, %tmp1
7:	%(Σ)	load float, float* @(Σ)
8:	%(Σ_{CUR})	**fmul** %dT, %C_{ERR}
9:	%(Σ)	**fadd** %(Σ), %(Σ_{CUR})
10:		store %(Σ), float* @(Σ)
11:	%(Σ)	**fmul** %K_i, %(Σ)
12:	%OUTPUT	**fadd** %(Σ), %OUTPUT
13:		return %OUTPUT

CASE 2: PID Software Failure Rate Estimation

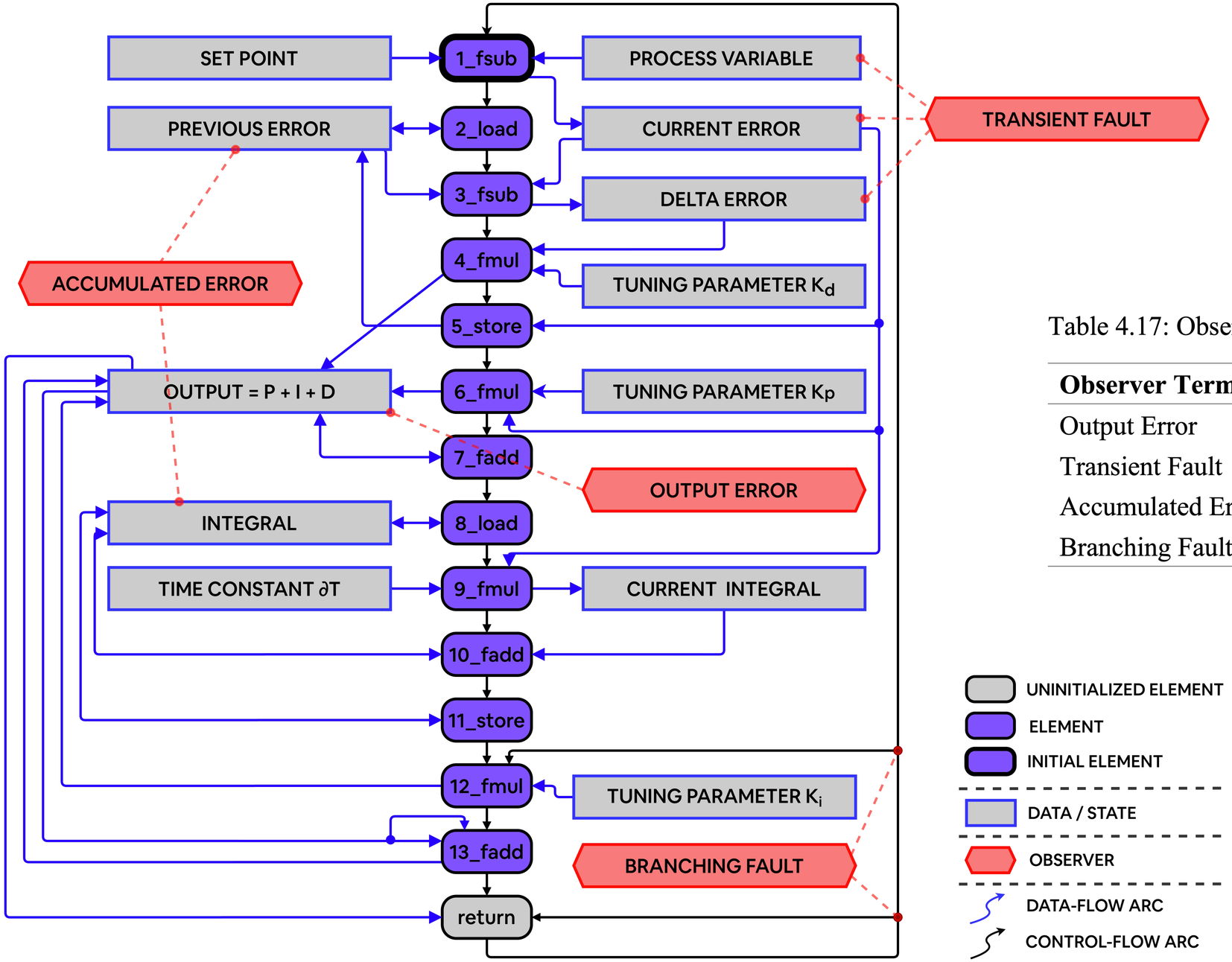


Table 4.17: Observer Terms - PID Assembler Instructions DEPM

Observer Term	Evaluated Expression
Output Error	$\sim(OUTPUT = OK)$
Transient Fault	$\sim(P_{VAR} = OK \;\&\; C_{ERR} = OK \;\&\; D_{ERR} = OK)$
Accumulated Error	$\sim(P_{ERR} = OK \;\&\; \Sigma = OK)$
Branching Fault	$(CF = return) \;\&\; \sim(CF_{next} = 1\_fsub)$

CASE 2: PID Software Failure Rate Estimation

- Calculate instruction failure rate by estimating bit error rate and adjust it for temperature dependent failure mechanisms.

$$\lambda_{BER} = AF_{DSP} \times \left(\frac{1}{2^{10}}\right)\left[\frac{\text{error}}{\text{bit}}\right] \times \left(\frac{1}{365 \times 24}\right)\left[\frac{1}{\text{hour}}\right]$$

$$\approx AF_{DSP} \times 1.12 \times 10^{-7}\left[\frac{\text{error}}{\text{bit} \times \text{hour}}\right]$$

- Since 1 SRAM bit is implemented using 6 CMOS transistors, estimate transistor use per instruction for this CPU to get instruction failure rate $\lambda_{op} = U_{op} \times \lambda_{BER}$

Table 4.16: Hardware acceleration factor adjusted instruction soft error rate [error/hour], segmented by phase.

λ_{op}	U_{op}	Instruction Soft Error Rate [error/hour]		
		Phase I	**Phase II**	**Phase III**
λ_{add}	6.12	$\mathcal{LN}(\bar{m} \approx 1.52 \times 10^{-8}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 1.48 \times 10^{-5}, EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 9.96 \times 10^{-3}, EF \approx 73.1)$
λ_{sub}	6.86	$\mathcal{LN}(\bar{m} \approx 1.71 \times 10^{-8}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 1.66 \times 10^{-5}, EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 8.93 \times 10^{-3}, EF \approx 73.1)$
λ_{mul}	11.9	$\mathcal{LN}(\bar{m} \approx 2.96 \times 10^{-8}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 2.87 \times 10^{-5} EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 1.55 \times 10^{-2}, EF \approx 73.1)$
λ_{store}	3.90	$\mathcal{LN}(\bar{m} \approx 9.71 \times 10^{-9}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 9.42 \times 10^{-6}, EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 5.07 \times 10^{-3}, EF \approx 73.1)$
λ_{load}	1.00	$\mathcal{LN}(\bar{m} \approx 2.86 \times 10^{-9}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 2.78 \times 10^{-6}, EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 1.49 \times 10^{-3}, EF \approx 73.1)$
λ_{return}	0.08	$\mathcal{LN}(\bar{m} \approx 2.86 \times 10^{-9}, EF \approx 7.36)$	$\mathcal{LN}(\bar{m} \approx 2.78 \times 10^{-6}, EF \approx 90.2)$	$\mathcal{LN}(\bar{m} \approx 1.49 \times 10^{-3}, EF \approx 73.1))$

CASE 2: PID Software Failure Likelihoods

Table 4.18: Observed Events, PID Software Failure to Change Power Level on Alert

Ø	$\textbf{alert} \Rightarrow \boldsymbol{P}_{=?}[\Diamond^{\leq \boldsymbol{T}_{alert}}$ **Transient Fault**$]^{8}$	$\textbf{alert} \Rightarrow \boldsymbol{P}_{=?}[\Diamond^{\leq \boldsymbol{T}_{alert}}$ **Accumulated Error**$]$
I	$\mathcal{LN}(\overline{m} \approx 6.93 \times 10^{-9}, EF \approx 9.19)$	$\mathcal{LN}(\overline{m} \approx 5.85 \times 10^{-9}, EF \approx 11.0)$
II	$\mathcal{LN}(\overline{m} \approx 3.69 \times 10^{-3}, EF \approx 376)$	$\mathcal{LN}(\overline{m} \approx 1.11 \times 10^{-4}, EF \approx 127)$
III	$\mathcal{LN}(\overline{m} \approx 6.67 \times 10^{-2}, EF \approx 40.9)$	$\mathcal{LN}(\overline{m} \approx 6.43 \times 10^{-4}, EF \approx 1.42)$

[8] $\Psi \Longrightarrow P_{=?}\left[\Diamond^{\leq k}\, \varphi\right]$: Once event Ψ occurs, the probability that φ is satisfied within k time units

CASE 2: DEPM - Software PID Failure Likelihoods

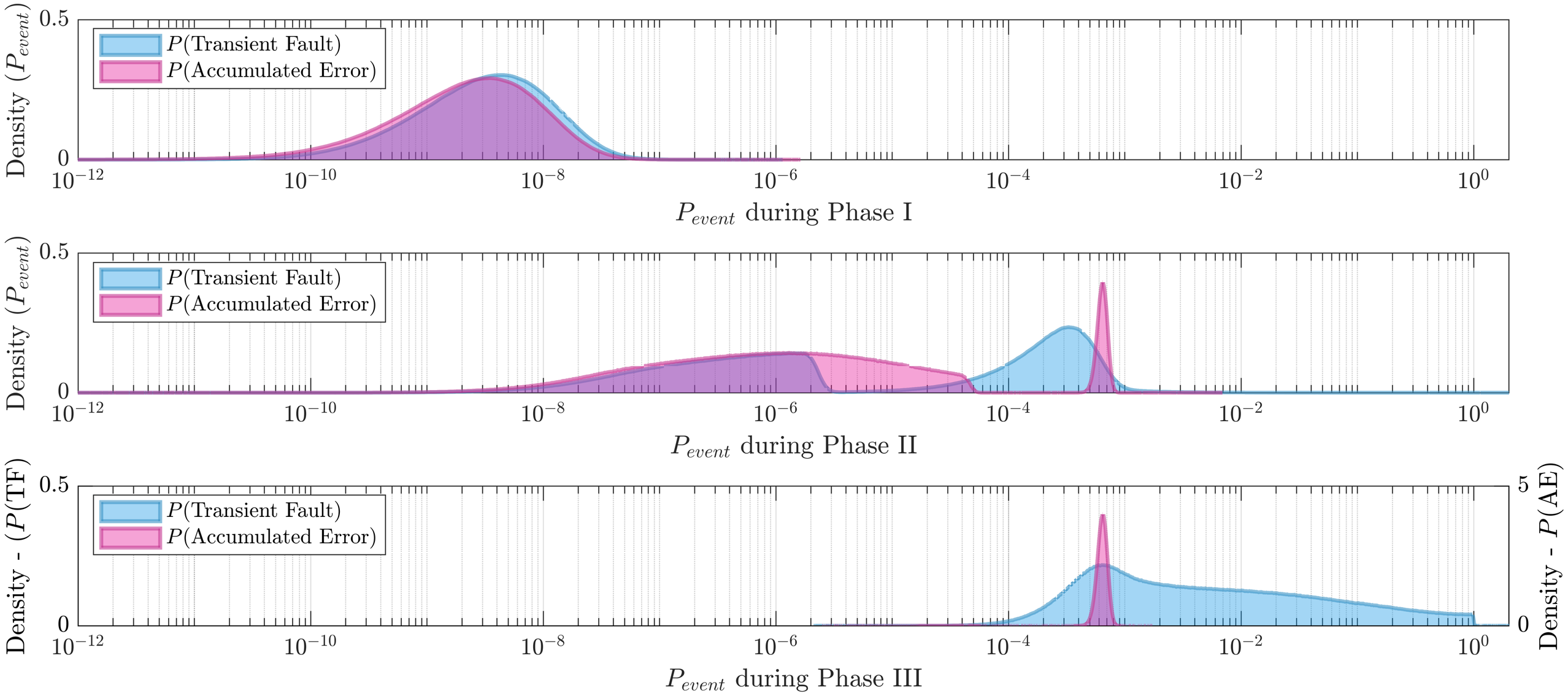


Figure 4.18: Observed Events, PID Software Failure to Change Power Level on Alert

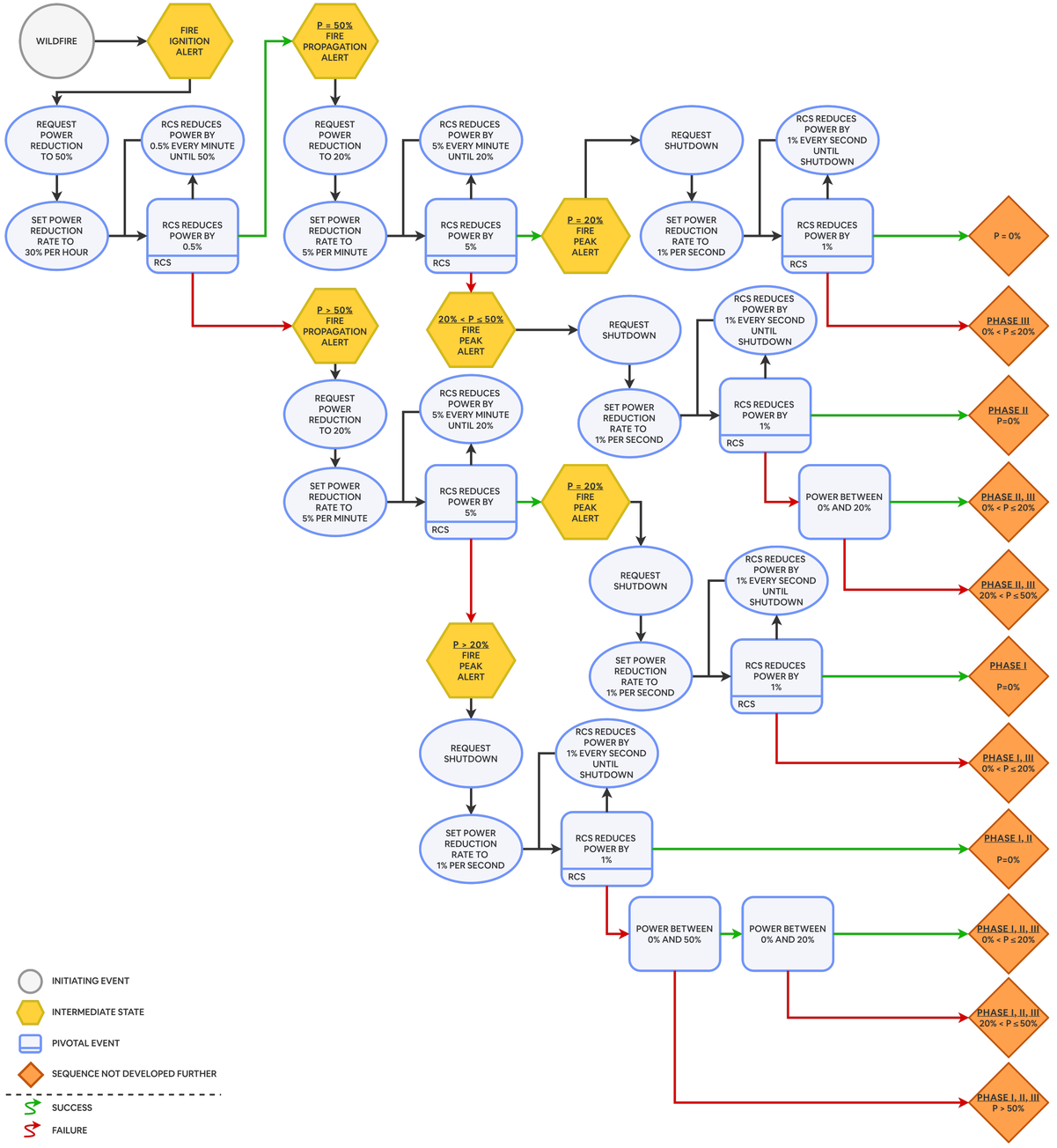
CASE 2: RCS Power Down End-State Likelihoods

Table 4.19: End State Likelihoods, Power Reduction Events for an External Fire Scenario, with Recovery

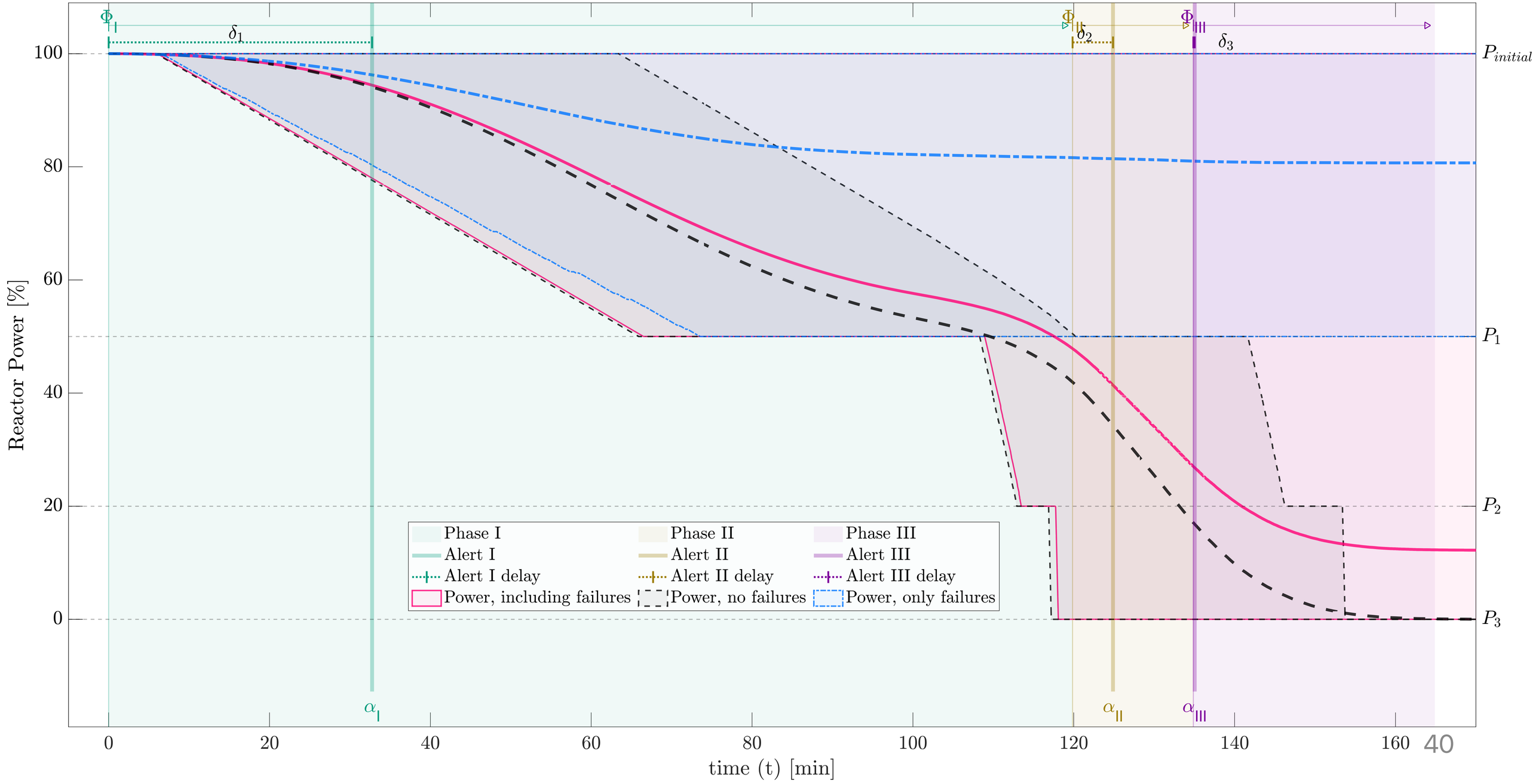
ID	Power Level	P(Power Level)	Phase I	Phase II	Phase III
S_0	Shutdown	$\mathcal{LN}(\bar{m} \approx 9.99 \times 10^{-1}, EF \approx 1.02)$	Success	Success	Success
L_3	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 7.17 \times 10^{-4}, EF \approx 26.8)$	Success	Success	Failure
S_2	Shutdown	$\mathcal{LN}(\bar{m} \approx 1.02 \times 10^{-8}, EF \approx 42.3)$	Success	Failure	Recovery
ML_{23}	0% < Power ≤ 50%	$\mathcal{LN}(\bar{m} \approx 1.05 \times 10^{-11}, EF \approx 177)$	Success	Failure	Failure
S_1	Shutdown	$\mathcal{LN}(\bar{m} \approx 3.14 \times 10^{-12}, EF \approx 3.56)$	Failure	Recovery	Success
L_{13}	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 2.26 \times 10^{-15}, EF \approx 34.0)$	Failure	Recovery	Failure
S_{12}	Shutdown	$\mathcal{LN}(\bar{m} \approx 3.20 \times 10^{-20}, EF \approx 52.2)$	Failure	Failure	Recovery
HML_{123}	Power > 0%	$\mathcal{LN}(\bar{m} \approx 3.31 \times 10^{-23}, EF \approx 207)$	Failure	Failure	Failure

CASE 3: Integrating Dual Error Propagation into Dynamic Event Trees

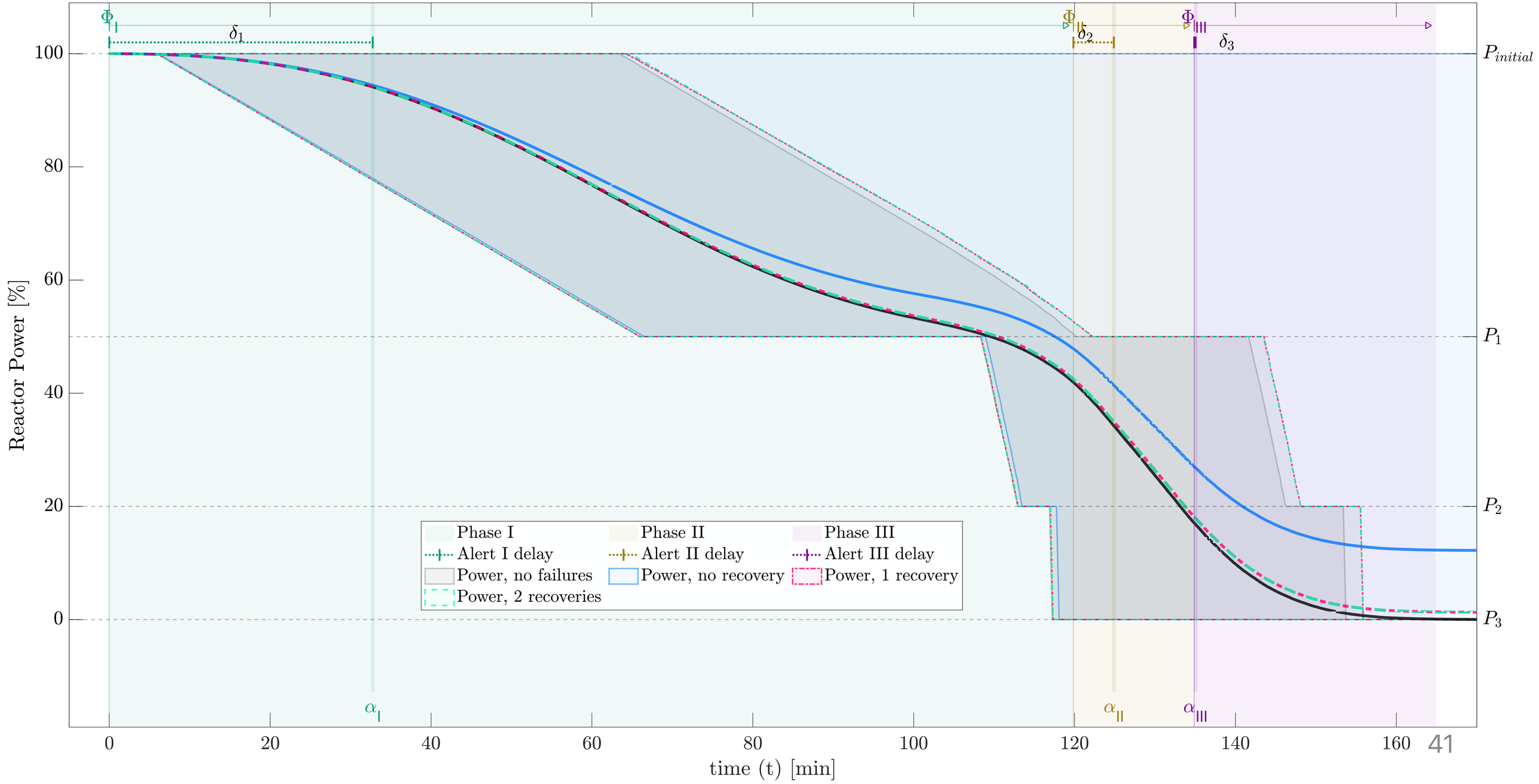
CASE 3: Reactor Control System Power Down ESD



CASE 3: Time Explicit Reactor Power Level, No Recoveries



CASE 3: Time Explicit Reactor Power Level, upto 2 Recoveries



CASE 3: RCS Power Down End-State Likelihoods

Table 4.20: End State Likelihoods, Dynamic Modeling of RCS Power Level Reduction, with Recovery

ID	Power Level	P(Power Level)	Phase I	Phase II	Phase III
S_0	Shutdown	$\mathcal{LN}(\bar{m} \approx 9.69 \times 10^{-1}, EF \approx 1.15)$	Success	Success	Success
L_3	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 2.83 \times 10^{-2}, EF \approx 2.92)$	Success	Success	Failure
S_2	Shutdown	$\mathcal{LN}(\bar{m} \approx 4.15 \times 10^{-6}, EF \approx 20.1)$	Success	Recovery	Success
L_{23}	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 1.16 \times 10^{-7}, EF \approx 24.2)$	Success	Failure	Recovery
M_{23}	20% < Power ≤ 50%	$\mathcal{LN}(\bar{m} \approx 3.15 \times 10^{-9}, EF \approx 28.8)$	Success	Failure	Recovery
S_1	Shutdown	$\mathcal{LN}(\bar{m} \approx 2.40 \times 10^{-12}, EF \approx 1.37)$	Failure	Recovery	Success
L_{13}	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 1.98 \times 10^{-13}, EF \approx 2.01)$	Failure	Recovery	Failure
S_{12}	Shutdown	$\mathcal{LN}(\bar{m} \approx 1.03 \times 10^{-17}, EF \approx 20.4)$	Failure	Failure	Recovery
L_{123}	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 1.80 \times 10^{-20}, EF \approx 6.32)$	Failure	Failure	Failure
M_{123}	20% < Power ≤ 50%	$\mathcal{LN}(\bar{m} \approx 1.64 \times 10^{-15}, EF \approx 3.58)$	Failure	Failure	Failure
H_{123}	50% < Power ≤ 100%	$\mathcal{LN}(\bar{m} \approx 1.26 \times 10^{-24}, EF \approx 79.7)$	Failure	Failure	Failure

CASE 2, CASE 3 Comparison

Table 5.1: Comparative Analysis of End-State Likelihoods for Phased Reactor Shutdown on Fire Alert

ID	Power Level	P(Power Level)	
		Traditional Analysis	Dynamic Analysis
$\boldsymbol{S_0}$	Shutdown	$\mathcal{LN}(\bar{m} \approx 9.99 \times 10^{-1}, EF \approx 1.02)$	$\mathcal{LN}(\bar{m} \approx 9.69 \times 10^{-1}, EF \approx 1.15)$
$\boldsymbol{L_3}$	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 7.17 \times 10^{-4}, EF \approx 26.8)$	$\mathcal{LN}(\bar{m} \approx 2.83 \times 10^{-2}, EF \approx 2.92)$
$\boldsymbol{S_2}$	Shutdown	$\mathcal{LN}(\bar{m} \approx 1.02 \times 10^{-8}, EF \approx 42.3)$	$\mathcal{LN}(\bar{m} \approx 4.15 \times 10^{-6}, EF \approx 20.1)$
$\boldsymbol{ML_{23}}$	0% < Power ≤ 50%	$\mathcal{LN}(\bar{m} \approx 1.05 \times 10^{-11}, EF \approx 177)$	$\mathcal{LN}(\bar{m} \approx 1.27 \times 10^{-7}, EF \approx 93.6)$
$\boldsymbol{S_1}$	Shutdown	$\mathcal{LN}(\bar{m} \approx 3.14 \times 10^{-12}, EF \approx 3.56)$	$\mathcal{LN}(\bar{m} \approx 2.40 \times 10^{-12}, EF \approx 1.37)$
$\boldsymbol{L_{13}}$	0% < Power ≤ 20%	$\mathcal{LN}(\bar{m} \approx 2.26 \times 10^{-15}, EF \approx 34.0)$	$\mathcal{LN}(\bar{m} \approx 1.98 \times 10^{-13}, EF \approx 2.01)$
$\boldsymbol{S_{12}}$	Shutdown	$\mathcal{LN}(\bar{m} \approx 3.20 \times 10^{-20}, EF \approx 52.2)$	$\mathcal{LN}(\bar{m} \approx 1.03 \times 10^{-17}, EF \approx 20.4)$
$\boldsymbol{HML_{123}}$	Power > 0%	$\mathcal{LN}(\bar{m} \approx 3.31 \times 10^{-23}, EF \approx 207)$	$\mathcal{LN}(\bar{m} \approx 1.63 \times 10^{-15}, EF \approx 3.58)$

But How Does DEPM Compare?

DEPM Comparison

- Use the ESD from CASE 1 and FT from CASE 2.
- Replace PID software failure DEPM basic event with alternative models.
- Re-run CASE 1 analysis for each model.

$$M_A := \text{No Model}$$

$$M_B := e^{(\lambda_{BER},\ t)}$$

$$M_C := e^{(AF_{DSP} \times \lambda_{BER},\ t)}$$

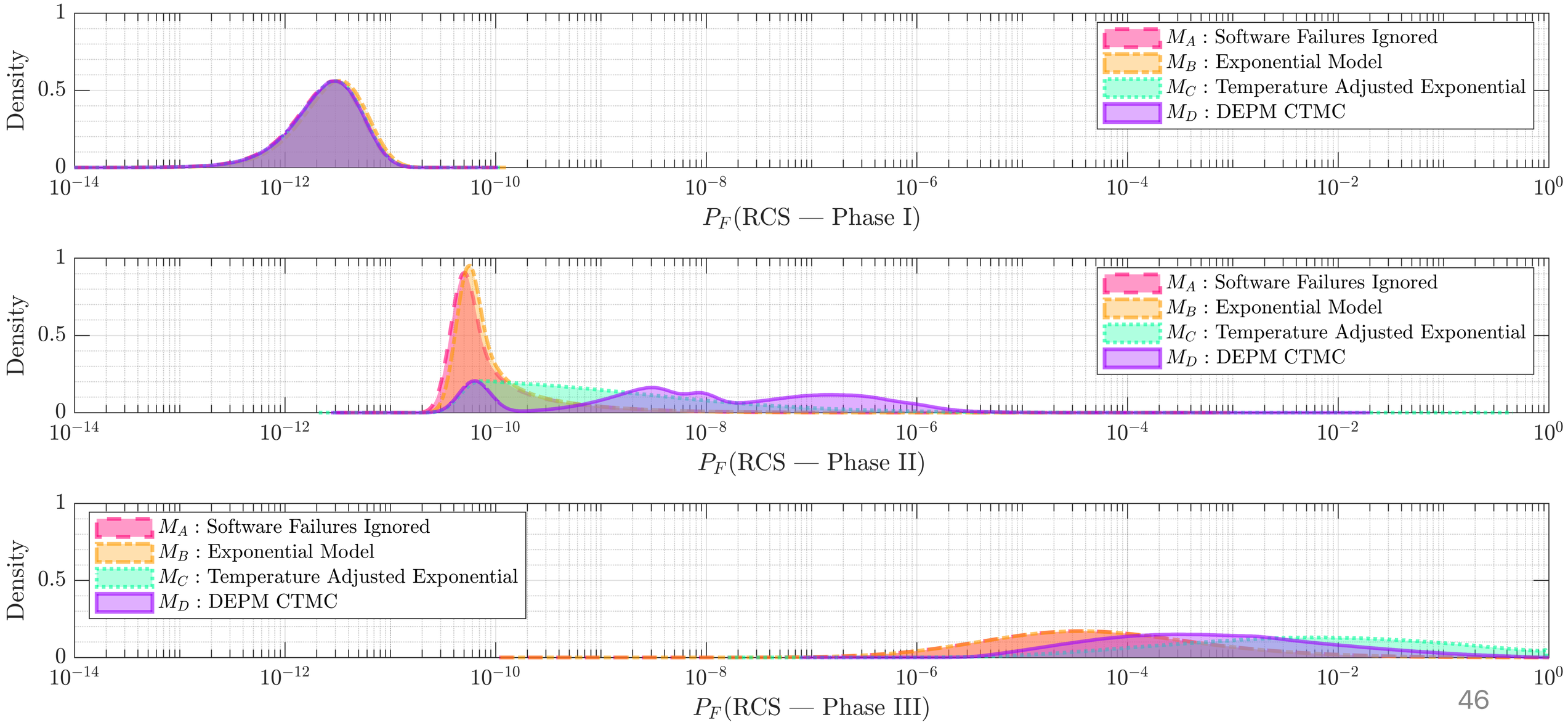
$$M_D := DEPM\ CTMC$$

Table 5.2 PLC PID software failure model contribution to Reactor Control System unavailability

Phase	Phase I	Phase II	Phase III
No Model	$\mathcal{LN}(\bar{m} \approx 3.09 \times 10^{-12}, EF \approx 3.65)$	$\mathcal{LN}(\bar{m} \approx 1.68 \times 10^{-10}, EF \approx 6.20)$	$\mathcal{LN}(\bar{m} \approx 8.07 \times 10^{-4}, EF \approx 44.9)$
$e^{(\lambda_{BER},\ t)}$	$\mathcal{LN}(\bar{m} \approx 3.48 \times 10^{-12}, EF \approx 3.63)$	$\mathcal{LN}(\bar{m} \approx 1.80 \times 10^{-10}, EF \approx 5.97)$	$\mathcal{LN}(\bar{m} \approx 8.07 \times 10^{-4}, EF \approx 44.9)$
$e^{(AF_{DSP} \times \lambda_{BER},t)}$	$\mathcal{LN}(\bar{m} \approx 3.18 \times 10^{-12}, EF \approx 3.65)$	$\mathcal{LN}(\bar{m} \approx 1.58 \times 10^{-8}, EF \approx 45.9)$	$\mathcal{LN}(\bar{m} \approx 1.99 \times 10^{-1}, EF \approx 89.3)$
DEPM CTMC	$\mathcal{LN}(\bar{m} \approx 3.14 \times 10^{-12}, EF \approx 3.56)$	$\mathcal{LN}(\bar{m} \approx 4.37 \times 10^{-7}, EF \approx 57.5)$	$\mathcal{LN}(\bar{m} \approx 1.92 \times 10^{-2}, EF \approx 38.4)$

DEPM Comparison Results

Figure 5.1 Reactor control system failure density estimates with alternative PID software failure model



Future Work

- Model Verification and Validation
- Automated Model Generation
- Incorporate Human Actions
- Expand the Case Studies
- Extend Applications

Thank You