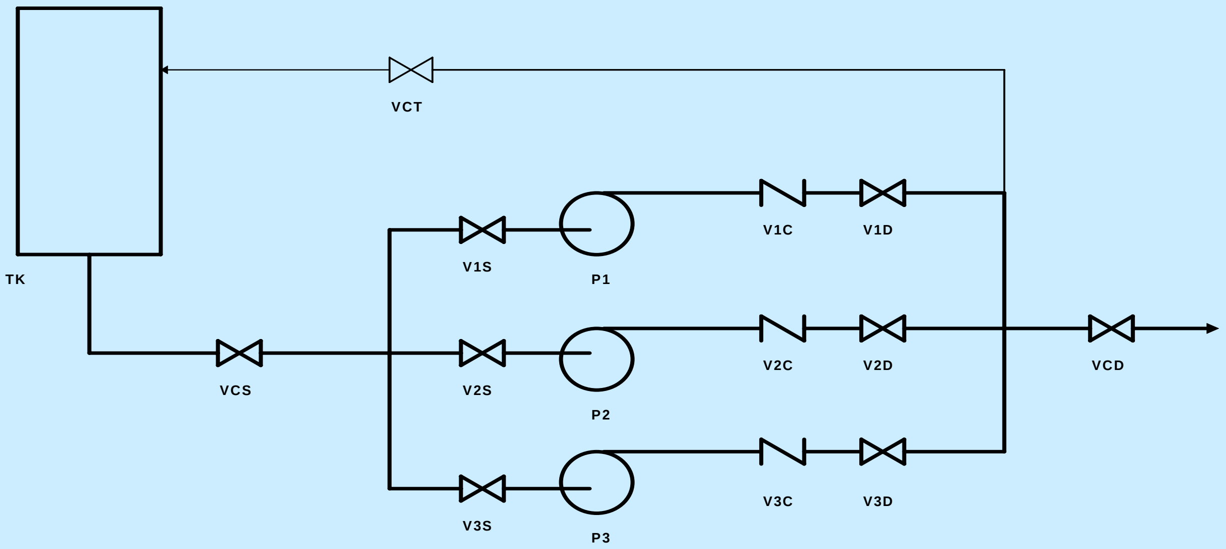
Basic Level 1. PSA course for analysts

System Analysis

Content

- System analysis of an example system
  - NORMALLY-OPERATING / STANDBY EQUIPMENT MODELS
  - CONSIDERED FAILURE MODES
  - MAINTENANCE UNAVAILABILITIES
  - COMMON CAUSE FAILURE MODELLING
  - PERSONNEL ERRORS
  - STANDBY FAILURES

EXAMPLE SYSTEM



EXAMPLE SYSTEM DATA

Component	Failure Mode	Failure Rate
Pump	Fail to Start	2.5E-03 per demand
	Fail to Run	3.5E-05 per hour
Check Valve	Fail to Open	1.5E-04 per demand
	Fail to Close	8.0E-04 per demand
	Spurious Closure	1.0E-08 per hour
	Spurious Opening	5.5E-07 per hour
Manual Valve	Spurious Closure	4.5E-08 per hour
Tank	Rupture	3.0E-08 per hour
Pump - CCF	Fail to Start - ß	6.0E-02
	Fail to Start - γ	2.0E-01
	Fail to Run - ß	2.0E-02
	Fail to Run - γ	2.5E-01
Check Valve - CCF	Fail to Open - ß	???
	Fail to Open - γ	???
	Fail to Close - ß	???
	Fail to Close - γ	???

EXAMPLE CASES

CASE 1

- ONE PUMP NORMALLY RUNNING WITH FLOW THROUGH VALVES VCS AND VCD
- TWO PUMPS IN STANDBY
- MONTHLY ROTATION OF NORMALLY RUNNING PUMP

CASE 2

- ALL PUMPS IN STANDBY
- ONE PUMP TESTED EACH MONTH WITH FLOW THROUGH VALVE VCD

CASE 3

- ALL PUMPS IN STANDBY
- ONE PUMP TESTED EACH MONTH WITH RECIRCULATION TO TANK
- INJECTION TEST THROUGH VALVE VCD ONCE EVERY 18 MONTHS DURING SHUTDOWN

NORMALLY-OPERATING / STANDBY EQUIPMENT

CASE 1 ALIGNMENT MODELS “SPECIFIED TRAIN”

- ASSUME TRAIN 1 NORMALLY RUNNING
- REQUIRES CONSISTENT ASSUMPTIONS IN ALL MODELS
- ADVANTAGES
  - SIMPLIFIED MODELS
- DISADVANTAGES
  - INTRODUCES ARTIFICIAL ASYMMETRY IN PSA MODELS AND RESULTS
  - MAY NOT IDENTIFY REAL ASYMMETRIES IN PLANT
  - INCORRECT IMPORTANCE (NOT SYMMETRIC)
  - MORE DIFFICULT FOR APPLICATIONS

NORMALLY-OPERATING / STANDBY EQUIPMENT

CASE 1 ALIGNMENT MODELS “DISTRIBUTED TRAINS”

- ASSUME EACH TRAIN NORMALLY RUNNING 1/3 OF TIME
- REQUIRES CONSISTENT ASSUMPTIONS IN ALL MODELS
- ADVANTAGES
  - CORRECT LOGICAL COMBINATIONS
  - CORRECT IMPORTANCE (SYMMETRIC)
  - EASIER FOR APPLICATIONS
- DISADVANTAGES
  - COMPLEMENT LOGIC (“NOT” EVENTS) TO DETERMINE MUTUALLY EXCLUSIVE ALIGNMENTS
  - 0.333 MULTIPLIER FOR CORRECT TOTAL FREQUENCY

“PASSIVE” FAILURE MODES

UNAVAILABILITY - GENERAL FORM

$$Q = \lambda * (t_T / 2 + t_m)$$

where λ = **Component failure rate (failure / hour)**

t_T = **Time between functional tests (hours)**

t_m = **PSA mission time (hours)**

NOTE:

A functional test provides positive indication of the component status (e.g., flow, pressure, level, temperature, etc.).

"PASSIVE" FAILURE MODES

REFERENCE VALUES

- **PUMP COMMON CAUSE STARTING FAILURES**

$$\beta_S \gamma_S Q_S = 3.0E\text{-}05$$

- **PUMP COMMON CAUSE RUNNING FAILURES**

$$\beta_R \gamma_R Q_R (24) = 4.2E\text{-}06$$

“PASSIVE” FAILURE MODES

CASE 1

- ASSUME PUMP P1 IS RUNNING
- ASSUME ROTATION IS P1-P2-P3

Valve	t_T	t_m	Q_{MV}	Q_{CV}
VCS	0	24	1.1E-06	--
VCD	0	24	1.1E-06	--
V1S, V1C, V1D	0	24	2.2E-06	2.4E-07
V2S, V2C, V2D	1440	24	6.7E-05	2.4E-07
V3S, V3C, V3D	720	24	3.5E-05	2.4E-07

NOTES

Q_{MV} = Manual Valve Spurious Closure

Q_{CV} = Check Valve Spurious Opening (Standby)
= Check Valve Spurious Closure (Running)

"PASSIVE" FAILURE MODES

CASE 1 NOTES

- Successful operation of the normally running train confirms that check valves V2C and V3C are closed.
- On average, each train is running for 1 month and is in standby for 2 months. At the time of the "average" initiating event, one standby train has been idle for ~0.5 month, and one train has been idle for ~1.5 months. The most limiting conditions apply if the initiating event occurs just before the end of the month. These conditions are used in the table.

1 2 3 1 2 3 1

x

“PASSIVE” FAILURE MODES

CASE 2

- ASSUME TEST ROTATION IS P1-P2-P3

Valve	t_T	t_m	Q_{MV}	Q_{CV}
VCS	720	24	1.7E-05	--
VCD	720	24	1.7E-05	--
V1S, V1C, V1D	2160	24	9.9E-05	2.0E-04
V2S, V2C, V2D	1440	24	6.7E-05	2.0E-04
V3S, V3C, V3D	720	24	3.5E-05	2.0E-04

NOTES

Q_{MV} = Manual Valve Spurious Closure

Q_{CV} = Check Valve Spurious Opening (Standby)
= Check Valve Spurious Closure (Running)

"PASSIVE" FAILURE MODES

CASE 2 NOTES

- Successful performance of each test confirms that the check valves in the untested trains are closed. The functional test interval for check valve spurious opening failures is 1 month.

- On average, each train is tested once every 3 months. At the time of the "average" initiating event, one train has been idle for ~0.5 month, one train has been idle for ~1.5 months, and one train has been idle for ~2.5 months. The most limiting conditions apply if the initiating event occurs just before the end of the month. These conditions are used in the table.

1	2	3	1	2	3	1
			X			

System analysis

“PASSIVE” FAILURE MODES

CASE 3

- ASSUME TEST ROTATION IS P1-P2-P3

Valve	t_T	t_m	Q_{MV}	Q_{CV}
VCS	720	24	1.7E-05	--
VCD	12960	24	2.9E-04	--
V1S, V1C, V1D	2160	24	9.9E-05	2.0E-04
V2S, V2C, V2D	1440	24	6.7E-05	2.0E-04
V3S, V3C, V3D	720	24	3.5E-05	2.0E-04

NOTES

Q_{MV} = Manual Valve Spurious Closure

Q_{CV} = Check Valve Spurious Opening (Standby)
= Check Valve Spurious Closure (Running)

“PASSIVE” FAILURE MODES

CASE 3 NOTES

- Case 3 is similar to Case 2, except the functional test interval for valve VCD is 18 Months.

- Spurious closure of valve VCD disables the system.

MAINTENANCE

TECHNICAL SPECIFICATIONS

- **ONE TRAIN MAY BE UNAVAILABLE FOR 14 DAYS**
- **TWO TRAINS MAY BE UNAVAILABLE FOR 72 HOURS**
- **THE PLANT MUST BE SHUT DOWN IF ALL THREE TRAINS ARE UNAVAILABLE**

MAINTENANCE

MAINTENANCE MODELS

- MUST ACCOUNT FOR TWO TYPES OF MAINTENANCE
- SINGLE-TRAIN MAINTENANCE
  - APPLIES TO EACH TRAIN (1, 2, 3)
  - FREQUENCY AND DURATION
  - DATA FROM SINGLE COMPONENT MAINTENANCE RECORDS
- TWO-TRAIN MAINTENANCE
  - APPLIES TO EACH PAIR OF TRAINS (1*2, 1*3, 2*3)
  - FREQUENCY AND DURATION
  - NOT INDEPENDENT COMBINATION OF SINGLE-TRAIN DATA

MAINTENANCE

CASE 1 MAINTENANCE MODELS “GROUPED MAINTENANCE”

- MAINTENANCE BASIC EVENTS IN ONLY 2 STANDBY TRAINS
- ADVANTAGES
  - LOGICALLY CORRECT CUTSETS
  - NO SPECIAL LOGIC FOR “NORMALLY RUNNING” TRAIN
- DISADVANTAGES
  - REQUIRES MAINTENANCE DATA MANIPULATION FOR CORRECT UNAVAILABILITIES
  - INCORRECT IMPORTANCE (NOT SYMMETRIC)
  - MORE DIFFICULT FOR APPLICATIONS

MAINTENANCE

CASE 1 MAINTENANCE MODELS “DISTRIBUTED MAINTENANCE”

- MAINTENANCE BASIC EVENTS IN ALL THREE TRAINS
- ADVANTAGES
  - DIRECT QUANTIFICATION OF MAINTENANCE DATA
  - CORRECT IMPORTANCE (SYMMETRIC)
  - EASIER FOR APPLICATIONS
- DISADVANTAGES
  - SPECIAL LOGIC TO ACCOUNT FOR “NORMALLY RUNNING” TRAIN
  - INCORRECT CUTSETS (ALL THREE TRAINS)

MAINTENANCE

CASE 2 MAINTENANCE MODELS

- LESS COMPLICATED LOGIC
  - ALL THREE TRAINS ARE STANDBY
  - NO SPECIAL LOGIC TO ACCOUNT FOR “NORMALLY RUNNING” TRAIN
- SAME GENERAL ISSUES AS CASE 1 MODELS
- PSAs OFTEN USE “DISTRIBUTED MAINTENANCE” MODELS FOR STANDBY SYSTEMS
  - POST-QUANTIFICATION CUTSET EDITING
  - RETAIN CONSERVATIVE THREE-TRAIN CUTSETS

COMMON CAUSE FAILURES

TYPES OF COMPONENTS FOR COMMON CAUSE ANALYSIS

- PUMPS
  - MOTOR-DRIVEN (FAIL TO START, FAIL TO RUN)
  - TURBINE-DRIVEN (FAIL TO START, FAIL TO RUN)
  - DIESEL-DRIVEN (FAIL TO START, FAIL TO RUN)
- DIESEL GENERATORS (FAIL TO START, FAIL TO RUN)
- AIR COMPRESSORS (FAIL TO START, FAIL TO RUN)
- HVAC FANS (FAIL TO START, FAIL TO RUN)
- HVAC CHILLER UNITS (FAIL TO START, FAIL TO RUN)
- MOTOR-GENERATORS (FAIL TO START, FAIL TO RUN)

COMMON CAUSE FAILURES

TYPES OF COMPONENTS FOR COMMON CAUSE ANALYSIS

- CONTAINMENT COOLERS (FAIL TO START, FAIL TO RUN)
- VALVES
  - MOTOR-OPERATED (FAIL TO OPEN, FAIL TO CLOSE)
  - AIR-OPERATED (FAIL TO OPEN, FAIL TO CLOSE)
  - SOLENOID (FAIL TO OPEN, FAIL TO CLOSE)
  - HYDRAULIC (FAIL TO OPEN, FAIL TO CLOSE)
  - MAIN STEAM ISOLATION (FAIL TO CLOSE)
  - PRIMARY AND SECONDARY RELIEF (FAIL TO OPEN)
  - PRESSURIZER PORVS (FAIL TO OPEN)
  - CONDENSER STEAM DUMPS (FAIL TO OPEN)

COMMON CAUSE FAILURES

TYPES OF COMPONENTS FOR COMMON CAUSE ANALYSIS

- CIRCUIT BREAKERS (FAIL TO OPEN, FAIL TO CLOSE)
  - BUS SUPPLY CIRCUIT BREAKERS
  - AUTOMATIC TRANSFER CIRCUIT BREAKERS
  - DIESEL GENERATOR OUTPUT CIRCUIT BREAKERS
  - REACTOR TRIP BREAKERS

COMMON CAUSE FAILURES

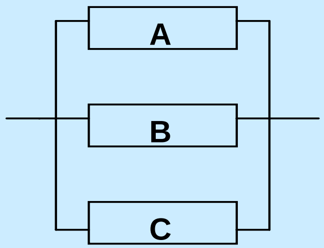
TYPES OF COMPONENTS FOR COMMON CAUSE ANALYSIS

TYPE OF COMPONENT	PSA EXPERIENCE	
	SOME MODEL COMMON CAUSE	MOST DO NOT MODEL COMMON CAUSE
CHECK VALVES	x	
SAFETY VALVES	x	
RELAYS	x	
BATTERIES	x	
TRANSFORMERS		x
BATTERY CHARGERS		x
INVERTERS		x
SIGNAL TRANSMITTERS		x
SIGNAL COMPARATORS		x
ELECTRONIC COMPONENTS		x

COMMON CAUSE FAILURES

COMMON CAUSE FAILURE LOGIC

SYSTEM

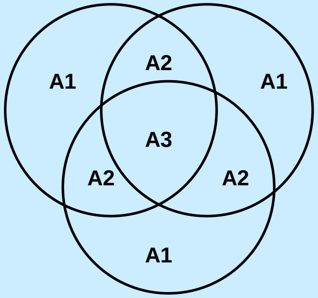


SYSTEM FAILURE CUTSETS
(PARENTHESES INDICATE
COMMON CAUSE FAILURES)

A B C
(AB) C
(AC) B
(BC) A
(AB) (BC)
(AB) (AC)
(AC) (BC)
(ABC)

COMMON CAUSE FAILURES

VENN DIAGRAM REPRESENTATION



LET	A	=	TOTAL CIRCLE
	A1	=	INDEPENDENT PORTION OF A
		=	$(1 - \beta)$ A
	A2	=	PORTION OF A THAT OCCURS WITH ONE SPECIFIC ADDITIONAL COMPONENT
		=	$(1 / 2)\ \beta\ (1 - \gamma)$ A
	A3	=	PORTION OF A THAT OCCURS WITH BOTH ADDITIONAL COMPONENTS
		=	$\gamma\beta$ A

CHECK FOR "CONSERVATION OF A"

A	=	A1 + 2*A2 + A3
	=	$(1 - \beta)$ A + 2 * [$(1 / 2)\ \beta\ (1 - \gamma)$ A] + $\gamma\beta$ A
	=	A - β A + β A - $\gamma\beta$ A + $\gamma\beta$ A
	=	A

COMMON CAUSE FAILURES

SYSTEM FAILURE EQUATION

- **FROM THE CUTSET REPRESENTATION, LET**

  A1 = A = B = C

  A2 = (AB) = (AC) = (BC)

  A3 = (ABC)

- **COMPLETE FAULT TREE SOLUTION CONTAINS 8 CUTSETS**

- **SYSTEM FAILURE IS THE SUM OF ALL COMBINATIONS**

$$Q = A1*A1*A1 + 3*A2*A1 + 3*A2*A2 + A3$$

$$= [(1-\beta)A]^3 + 3*[(1/2)\beta(1-\gamma)A]*[(1-\beta)A] + 3*[(1/2)\beta(1-\gamma)A]^2 + \gamma\beta A$$

COMMON CAUSE FAILURES

IMPORTANT FACTORS AFFECTING THE ASSESSMENT OF COMMON CAUSE PARAMETERS

- TYPE OF COMPONENT BEING MODELED
- COMPONENT APPLICATION AND OPERATING MODES IN THE PLANT BEING MODELED
  - STANDBY
  - INTERMITTENT OPERATION
  - NORMALLY RUNNING
- LEVEL OF DETAIL IN THE ANALYSIS OF SPECIFIC CAUSES FOR COMPONENT FAILURE WITHIN THE SYSTEM MODEL

COMMON CAUSE FAILURES

CASE 1 COMMON CAUSE MODELS PUMP START FAILURES

- STANDBY PUMPS

- NORMALLY RUNNING PUMP AND STANDBY PUMPS
  - RESTART AFTER LOSS OF OFFSITE POWER
  - COUPLING / DECOUPLING DEPENDS ON CIRCUIT DESIGN
  - CIRCUIT BREAKER / RELAYS FOR PUMP TRIP / START
  - CAN USUALLY JUSTIFY DECOUPLING

COMMON CAUSE FAILURES

CASE 1 COMMON CAUSE MODELS PUMP RUNNING FAILURES

- NORMALLY RUNNING PUMP AND STANDBY PUMPS
- ONE MONTH RUNNING TIME USUALLY NOT LONG ENOUGH TO DECOUPLE COMMON CAUSES FOR RUNNING FAILURES (E.G.., LONG-TERM WEAROUT)
- THREE MONTHS OR LONGER RUNNING TIME MAY JUSTIFY DECOUPLING

COMMON CAUSE FAILURES

CASE 2 COMMON CAUSE MODELS

- START FAILURES FOR ALL PUMPS
- RUNNING FAILURES FOR ALL PUMPS
- CANNOT JUSTIFY DECOUPLING
- MAY JUSTIFY SCREENING OUT SOME COMMON CAUSE FAILURE EVENTS FROM GENERIC DATA BASED ON STAGGERED TESTING
  - DIFFICULT TO DETERMINE GENERIC TESTING
  - DOCUMENT WHY STAGGERED TESTING IS ADEQUATE COMMON CAUSE DEFENSE

PERSONNEL ERRORS

UNAVAILABILITY - GENERAL FORM

$$Q = \lambda_A * Q_{HE} * T_{DET}$$

where

λ_A	=	**Frequency of activity (test, maintenance, calibration, etc.) (event / hour)**
Q_{HE}	=	**Human error rate (error / event)**
T_{DET}	=	**Error detection time (hours)**

PERSONNEL ERRORS

HUMAN ERROR DETECTION

- CONTINUOUSLY MONITORED PARAMETER (LEVEL, FLOW PRESSURE, TEMPERATURE, ETC.)
- DOCUMENTED INSPECTIONS
- PERIODIC TESTING
- ROUTINE OPERATIONS (TRANSFER OF NORMALLY OPERATING PUMPS, ETC.)
- BEWARE OF FAILURE MODE AND NORMAL INDICATION
  - CONTAINMENT PRESSURE LOW
  - TANK LEVEL HIGH

STANDBY FAILURE RATES

COMPONENT DEMAND FAILURES

- COMPONENT FAILURES ON DEMAND CAN RESULT FROM TWO TYPES OF CAUSES
  - "SHOCK" FAILURES THAT OCCUR SIMPLY BECAUSE THE COMPONENT IS DEMANDED TO CHANGE STATUS
  - "STANDBY" FAILURES THAT OCCUR FROM CAUSES THAT ACCUMULATE OVER TIME WHILE THE COMPONENT IS IDLE
- CURRENT PSA DATABASES ACCOUNT FOR THE TOTAL EFFECTS FROM BOTH TYPES OF CAUSES
- VERY LITTLE GENERIC DATA AVAILABLE TO DETERMINE ACTUAL CONTRIBUTIONS FROM "SHOCKS" AND "STANDBY" FAILURES

STANDBY FAILURE RATES

COMPONENT DEMAND FAILURES

- PLANT-SPECIFIC DATA ALLOW BETTER DETERMINATION OF CAUSES
- PSA MODELS DO NOT NEED TO SEPARATE FAILURE CAUSES FOR GOOD ESTIMATES OF COMPONENT DEMAND FAILURE RATES
- DEMAND FAILURE RATE = (NUMBER OF FAILURES) / (NUMBER OF DEMANDS)
- ESTIMATES OF “SHOCK” AND “STANDBY” FAILURE RATES ARE VERY IMPORTANT FOR APPLICATIONS THAT EXAMINE RISK IMPACTS FROM VARIATIONS IN TEST INTERVALS AND ALLOWED OUTAGE TIMES

STANDBY FAILURE RATES

SIMPLIFIED LINEAR ALGEBRAIC MODEL FOR COMPONENT DEMAND FAILURE RATE

$$Q_D = f * Q_T + (1 - f) * Q_T * (t_A / t_N)$$

where

where	Q_D	=	**Estimated component demand failure rate**
	Q_T	=	**Total observed demand failure rate**
	f	=	**Fraction of observed failures due to “shocks”**
	(1 - f)	=	**Fraction of observed failures due to “standby” causes**
	t_A	=	**Test interval to be used for the analysis**
	t_N	=	**Nominal component test interval for observed failure rate data**

NOTE:

$(1 - f) * Q_T / t_N$ = “Standby failure rate”, λ_S

STANDBY FAILURE RATES

EXAMPLE APPLICATION OF MODEL UNAVAILABILITY DUE TO TESTING

TEST:

- ISOLATE INJECTION LINE (CLOSE VALVE VCD)
- OPEN TEST LINE (OPEN VALVE VCT)
- START AND RUN PUMP ON RECIRCULATION FLOW

IMPACT:

- SYSTEM IS DISABLED DURING TEST DUE TO CLOSED INJECTION VALVE VCD

STANDBY FAILURE RATES

UNAVAILABILITY DUE TO TESTING

$$Q_{system/test} = (1 / t_A) * T_{test}$$

$$Q_{train/test} = (1 / t_A) * [f * Q_T + (1 - f) * Q_T * (t_A / t_N)] * T_R$$

where **$1 / t_A$ = Test frequency (tests / hour)**

T_{test} = Test duration (hours / test)

T_R = Component mean repair time (hours / maintenance event)

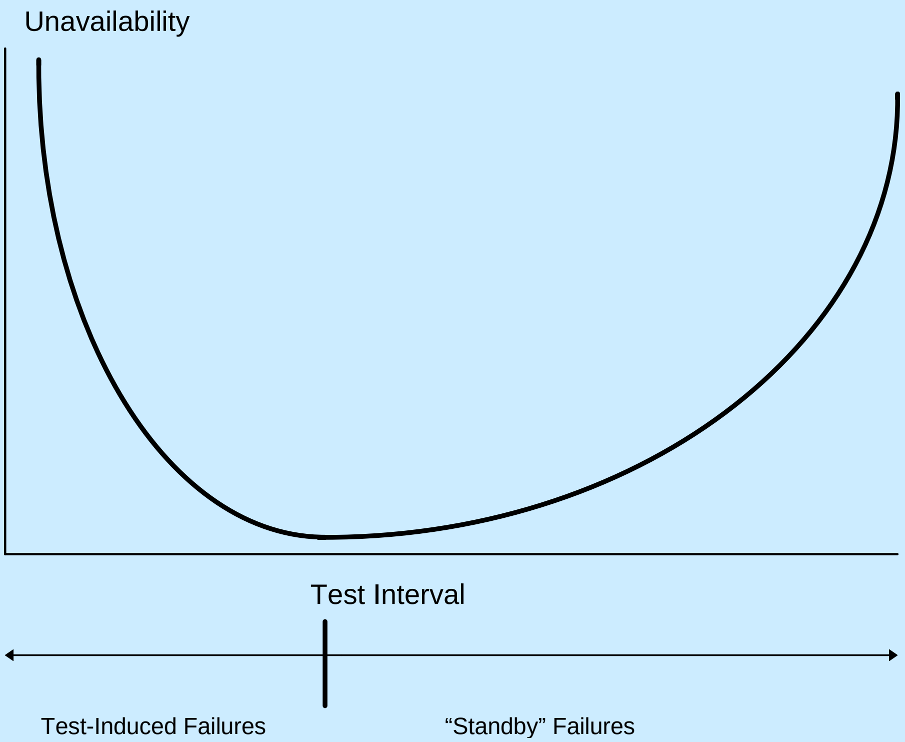
STANDBY FAILURE RATES

UNAVAILABILITY DUE TO TESTING

- FIRST TERM IS DIRECT CONTRIBUTION TO SYSTEM UNAVAILABILITY DUE TO CLOSED VALVE VCD.
- SECOND TERM ACCOUNTS FOR TEST-INDUCED FAILURES OF THE PUMP THAT REQUIRE REPAIRS.
- BOTH OF THESE EFFECTS SHOULD BE EVALUATED AS “DOWNSIDE” CONTRIBUTIONS TO UNAVAILABILITY DUE TO MORE FREQUENT TESTING.
- THESE “DOWNSIDE” CONTRIBUTIONS ARE COMPARED WITH IMPROVED COMPONENT AVAILABILITY DUE TO REDUCED EXPOSURE TIME FOR “STANDBY” FAILURES BETWEEN TESTS.

STANDBY FAILURE RATES

UNAVAILABILITY DUE TO TESTING



STANDBY FAILURE RATES

EXAMPLE APPLICATION OF MODEL UNAVAILABILITY DUE TO MAINTENANCE

CONFIGURATION:

- TWO TRAIN SYSTEM
- PERIODIC TESTING OF SECOND TRAIN IS REQUIRED WHEN FIRST TRAIN IS DISABLED FOR MAINTENANCE
- TEST IS PERFORMED WITH COMMON DISCHARGE VALVE VCD OPEN

STANDBY FAILURE RATES

SYSTEM UNAVAILABILITY DUE TO MAINTENANCE

$$Q_{maint} = 2 * (\lambda_{maint} * T_R) * [(1 / t_{t/m}) * Q_D * T_{R2}]$$

where

λ_{maint}	=	Single component maintenance frequency (maintenance event / hour)
T_R	=	Single component mean repair time (hours / maintenance event)
$1 / t_{t/m}$	=	Test frequency for second component when first component is disabled (tests / hour)
Q_D	=	Component demand failure rate (failure / test)
T_{R2}	=	Mean repair time for one component when both components are disabled (hours / maintenance event)

STANDBY FAILURE RATES

UNAVAILABILITY DUE TO MAINTENANCE

$\lambda_{maint} * T_R$	=	**Unavailability of single component due to maintenance**
$(1 / t_{t/m}) * Q_D * T_{R2}$	=	**Conditional system unavailability due to test-induced failures of second component**

Summary

- This presentation showed how to approach the system analysis performed for use in PSA
- Specific aspects of the analysis were presented using a simple example system:
  - component types
  - failure modes
  - common cause failures
  - test and maintenance