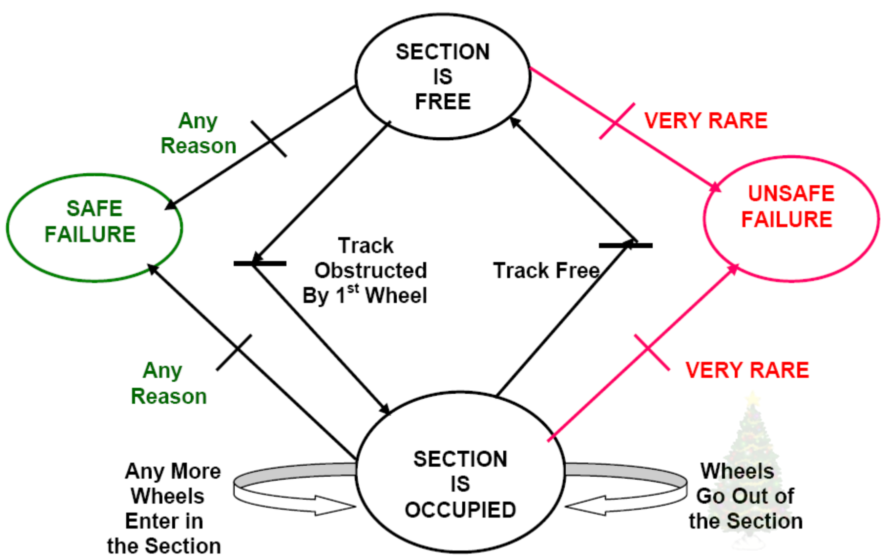
QUANTITATIVE TECHNIQUES IN SAFETY MANAGEMENT

SOMNATH PAL MIRSE, CSTM, CSQP
Asst. Prof. (Retd),
Indian Railways Instt. Of Signal Engg. & Telecommunication

Signalling branch of Railways provides the Movement Authority to the Train Drivers, where any wrong decision can result in Accidents. Railways thus have to follow a sincere **Safety Management Policy** throughout the **Life cycle of Signalling Equipment.** Hazard Identification and Risk Analysis, based on Quantitative Techniques, are to be done elaborately at the System Requirement Specification stage and be followed strictly in Design, Testing, Validation, Installation and Maintenance stages.

Establishment of a Safety Culture, along with periodical Quantitative monitoring throughout the Organization, helps in Safety Management and has thus become very vital for Signalling Department. It is also to be ensured that all staff are aware of their individual responsibilities and are proactive in their approach.

Railway Signalling Equipment can basically be defined as a **State Machine.** Normally, the Section in advance of a Signal **remains unoccupied**. As soon as the **first wheel of a Train enters the Section**, the status of the Section is set as **occupied** and this must continue, **irrespective of how many wheels enter the section**. When the full Train goes out of the Section protected by the Signal in rear, the Section goes back to **unoccupied**. The diagram below explains the State machine.



In the above State Transition Diagram, we find two extra States – **Safe Failure** and **Unsafe Failure**. **System Availability** and **Train Operation are affected** in Safe Failures. But Signal Department is **more concerned about Unsafe Failures,** since these can **cause Accidents**. This leads to the necessity to **identify any Unsafe Failure** and **adopt preventive action against its occurrence** during Design as well as Maintenance processes.

Both Safe as well as Unsafe failures can be Detected or Undetected. Undetected Failures are to be **treated as Dangerous** as we cannot take any preventive action. It is thus important to have knowledge of the **Rates, Causes and Consequences of Failures.**

Identification of the Events and **their Sequence** help in understanding the Logic and this knowledge helps in finding the Failure Modes of a System. A complicated system like Interlocking Equipment invariably contains several stages and the concept of **Reliability Block Diagram** and study of the **Influence of a particular Block on the overall System** would help in understanding the System better.

A **Hazard** is a situation in which there is an actual or potential danger to people or to the environment. In other words, **a Hazard might potentially lead to a possibly severe accident.** Associated with each Hazard is a certain Risk, related to the likelihood of the event occurring and to its likely consequences. Hazard Analysis along with **Quantification and Classification of Risks** is now Mandatory Exercises before accepting new Modern Signalling Equipment. Some of the Hazard Analysis techniques recommended are – **Fault Tree Analysis (FTA), Failure Modes, Effects and Criticality Analysis (FMECA)**, **Hazard and Operability analysis (HAZOP), Event Tree Analysis (ETA)** and **Cause and Consequence Analysis (CCA)**.

When the Level of Safety for the application has been set and the **necessary Risk Reduction estimated**, based on the results of the risk assessment process, the **Safety Integrity Level (SIL)** requirements can be derived. Safety Integrity can be viewed as a combination of **Quantifiable elements** (generally associated with Hardware, i.e. random failures) and **Non-quantifiable elements** (generally associated with systematic failures in Software, specification, documents, processes, etc.). All Interlocking Equipment are allocated specific **Safety Integrity Level** and accordingly the Tasks to be followed are classified as Mandatory, Highly Recommended and Recommended.

We shall now discuss the various topics of Quantitative Studies related to Safety Management

Formal Methods

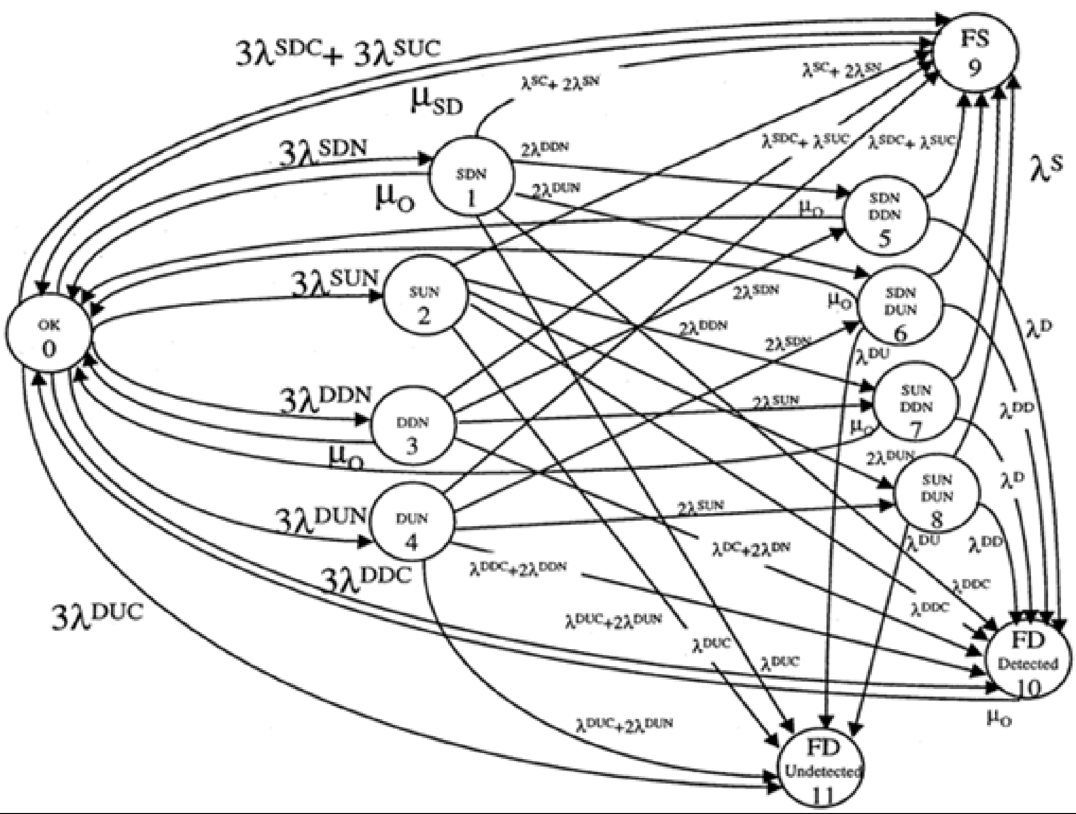
Due to **the Risks involved in Programmable Electronic based Signalling Equipment**, Engineers must themselves have a very high Level of Confidence on the System. This needs a **thorough Analysis of a Formal Model**, to start with. System Requirements are **normally written in Natural Language**. Some sentences may be **relatively ambiguous and unclear**. Quite a few Terms are often **not precisely defined**. These statements can be interpreted differently by different professionals, engaged in development of a Computer based Railway Signaling Equipment. Application of Formal methods **can reduce this problem.** It needs a thorough Analysis of a Formal Mathematical Model, to start with. **Markov Model** and **Petri Nets** are being extensively used presently to study Mathematical Modeling of Railway Signalling.

A) MARKOV Model

In Markov Model, State Diagrams are used to explain the behavior of the System under consideration. Two types of Symbols are used. A **Circle** represents a combination of Failed or Successful system Components and a **Directed Arc** represents possible **Failure and Repair Rates.** In this diagram multiple failure modes can be showed in a single drawing and the system can be represented in **Degraded Mode** also. Probabilities of operation in each State can be calculated as a function of Time, based on **Failure Rates (λ)** and **Repair Rates (μ).**

But the solution needs extensive use of **Linear Algebra**. Probability of the System being in any State is calculated by **Matrix multiplication**.

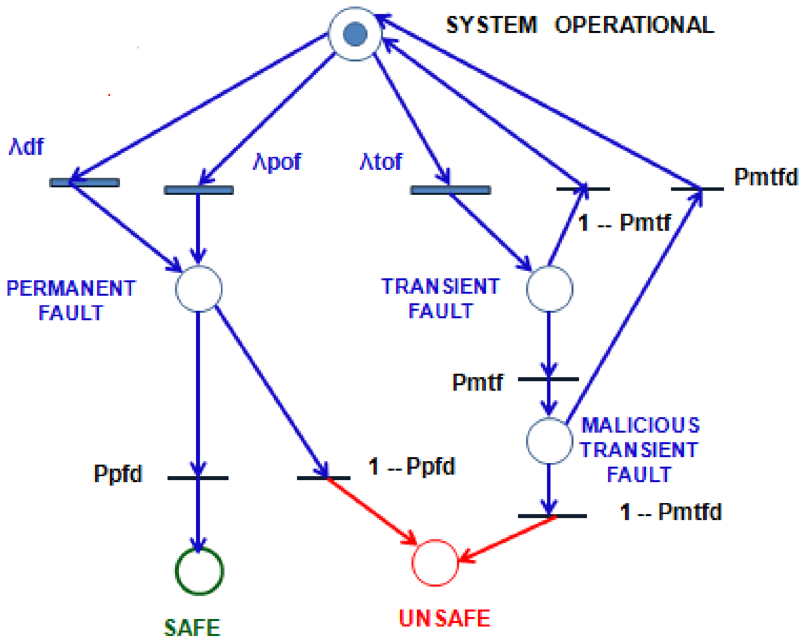
Markov Model for a 2oo3 Interlocking Equipment can be represented as below.



In this Diagram, State 0 represents the condition, where all modules are working successfully. All four normal Failure modes – Safe Detected and Undetected as well as Dangerous Detected and Undetected Failure Modes for all the Three Modules are placed as exits from State 0. And from each subsequent States, we proceed similarly considering further Module Failures. All Repair rates always have **transitions to State 0 only**.

B) PETRI NET Diagram

Petri Net diagram for Railway Signalling Equipment can be represented as shown below, where the Initial state is the **System Operational**, from which, the Token can travel to either **Permanent Fault** or **Transient Fault** States via three Timed Transients – **Design Fault Rate** (λdf), **Permanent Operational Fault Rate** (λpof) and **Transient Fault Rate** (λtof).



From Transient Fault State the Token can further proceed to **Malicious Transient Fault** State with a Probability **Pmtf** or return back to the Operational State with a Probability **(1 – Pmtf)**. From Malicious Transient Fault State the Token can return to Operational State with a Probability **Pmtfd**, if the Fault is detected. Otherwise, it goes to Unsafe State with a Probability (**1 – Pmtfd).** Similarly, from Permanent Fault State, the Token can proceed to Safe state with a Probability of **Ppfd** or can go to Unsafe State with a Probability of (**1 – Ppfd).**

Both Safe and Unsafe States are **Absorbing States** since Tokens **cannot go out from them.**

A Signalling equipment designed with Programmable Electronics depends on both Hardware as well as Software. So, if we denote **Hardware Failure Rates** as **λH** and **Software Failure Rates** as **λS,**

$$\lambda unsafe = (\lambda Hpof + \lambda Hdf + \lambda Spof + \lambda Sdf) . (1 - Ppfd) + (\lambda Htof + \lambda Stof) + \lambda Sdf. Pmtf. (1 - Pmtfd)$$

This can be further expressed as

$$\lambda unsafe = (\lambda Hpof + \lambda Hdf) . (1 - Ppfd) + \lambda Htof. Pmtf (1 - Pmtfd) + (\lambda Spof + \lambda Sdf) . (1 - Ppfd) + \lambda Stof. Pmtf. (1 - Pmtfd)$$

FAILURE RATES FOR ELECTRONIC SIGNAL EQUIPMENT

For calculating the System failure Rates, we are to consider every Module in the System individually and find their Safe and Dangerous failure rates. The Failures must be further classified into Detected and undetected failures. An example is given below.

Analog Input Circuit Failure Rate	$= \lambda_{AI}$
Number of Analog Input Circuits	$= N_{AI}$
Analog Output Circuit Failure Rate	$= \lambda_{AO}$
Number of Analog Output Circuits	$= N_{AO}$
Common Circuitry Analog I/O Module Failure Rate	$= \lambda_{A}$

Digital Input Circuit Failure Rate	$= \lambda_{DI}$
Number of Digital Input Circuits	$= N_{DI}$
Digital Output Circuit Failure Rate	$= \lambda_{DO}$
Number of Digital Output Circuits	$= N_{DO}$
Common Circuitry Digital I/O Module Failure Rate	$= \lambda_{D}$
Logic Solver Failure Rate	$= \lambda_{MP}$
Module Rack Failure Rate	$= \lambda_{R}$
Power Supply Failure Rate	$= \lambda_{PS}$

With all these parameters, we can calculate the Safe and Unsafe Failure Rates as

$$\lambda^{SD} = n_{DI}\lambda_{DI}^{SD} + n_{DO}\lambda_{DO}^{SD} + \lambda_{D}^{SD} + n_{AI}\lambda_{AI}^{SD} + n_{AO}\lambda_{AO}^{SD} + \lambda_{A}^{SD} + \lambda_{MP}^{SD} + \lambda_{R}^{SD} + \lambda_{PS}^{SD}$$

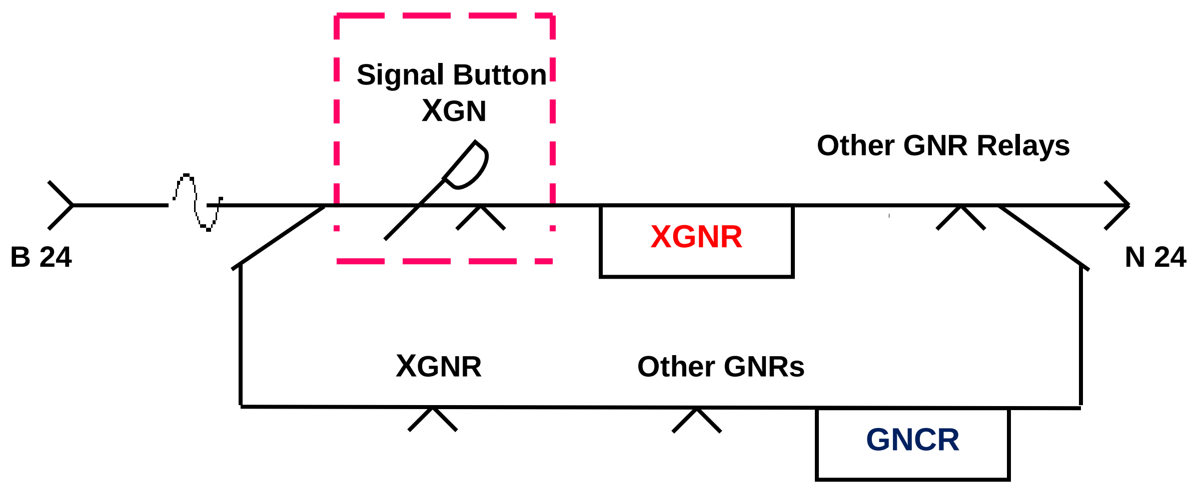
$$\lambda^{SU} = n_{DI}\lambda_{DI}^{SU} + n_{DO}\lambda_{DO}^{SU} + \lambda_{D}^{SU} + n_{AI}\lambda_{AI}^{SU} + n_{AO}\lambda_{AO}^{SU} + \lambda_{A}^{SU} + \lambda_{MP}^{SU} + \lambda_{R}^{SU} + \lambda_{PS}^{SU}$$

$$\lambda^{DD} = n_{DI}\lambda_{DI}^{DD} + n_{DO}\lambda_{DO}^{DD} + \lambda_{D}^{DD} + n_{AI}\lambda_{AI}^{DD} + n_{AO}\lambda_{AO}^{DD} + \lambda_{A}^{DD} + \lambda_{MP}^{DD} + \lambda_{R}^{DD} + \lambda_{PS}^{DD}$$

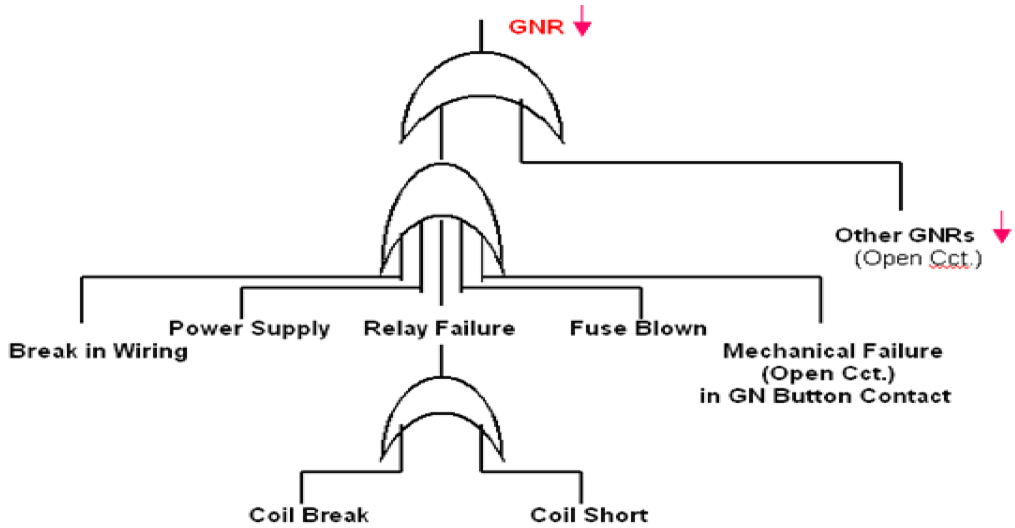
$$\lambda^{DU} = n_{DI}\lambda_{DI}^{DU} + n_{DO}\lambda_{DO}^{DU} + \lambda_{D}^{DU} + n_{AI}\lambda_{AI}^{DU} + n_{AO}\lambda_{AO}^{DU} + \lambda_{A}^{DU} + \lambda_{MP}^{DU} + \lambda_{R}^{DU} + \lambda_{PS}^{DU}$$

Failure Rate Analysis by Fault Tree.

Let us take an example from Relay based interlocking equipment. To operate any Signal, the **concerned Signal Button** is to be **pressed**. Whenever the Signal Button is pressed, the corresponding **Signal Button Relay (GNR)** will operate, provided no other Signal Button is simultaneously pressed. So, **Drop Contacts of all other GNR Relays** are proved in the operate path of **GNR Relay.** The basic Circuit Diagram is shown below:



The circuit is self-explanatory. Relay GNCR is **normally in Pick up condition**, proving that all Signal Button Relays are dropped i.e. **no Signal Button is pressed**. Now, we will prepare a **Fault Tree** to find out how the GNR Circuit can fail in a **Safe mode** (Relay does not Pick-up when Signal Button is Pressed).



The **Rate of Safe Failure**

$$\lambda \text{ safe} = \lambda_{GNR} + \lambda_{FUSE} + \lambda_{POWER} + \lambda_{WIRING} + \lambda_{CONTACT.\ FLT\ (Button)} + \lambda_{Other\ GNRs\ (13)}$$

As per ***Railtrack IRM CCA Model,***

$\lambda_{RELAY\ (open)}$ $= 0.7495 \times 10^{-6}$ / Hr., $\lambda_{RELAY\ (short)}$ $= 0.4307 \times 10^{-6}$ / Hr
$\lambda_{WIRING\ (Open)}$ $= 6.554 \times 10^{-8}$ / Hr., λ_{FUSE} $= 0.04 \times 10^{-6}$ / Hr.,
λ_{POWER} $= 0.04 \times 10^{-6}$ / Hr. and

As per ***MIL Std. 217F***

$\lambda_{CONTACT.\ FLT}$ $= 0.3468 \times 10^{-6}$ **/ Hr. (**considering **5 operations / Hr.), (for GN Button)**

Replacing these values in the equation

$$\lambda\text{safe} = (0.7495 \times 10^{-6} + 0.4307 \times 10^{-6} + 6.554 \times 10^{-8} + 2 \times 0.04 \times 10^{-6} + 0.3468 \times 10^{-6} + 13 \times 0.7495 \times 10^{-6}) / \text{Hr} = 11.416 \times 10^{-6} / \text{Hr}.$$

Effect of Ambient Temperature and Component Quality on Failure Rate

Failure Rate calculations at Stress conditions helps in the choice of components and Environment effects. Thermal and Electrical Stresses Influence the Failure rate of Electronic Components. As more and more Electronic based Equipment are being procured and Installed in railway signaling Networks, study of Impact of Stress is very important. MIL Handbook 217F provides a good Guideline for the calculations. I have calculated Failure Rates of Cards of CEL manufactured **Universal Axle Counter** for 45°C and 30°C. Calculations for a **Resistor** as per **MIL 217F item 9.1** from Amplifier – Rectifier Card is showed for example.

$$\lambda_B = 4.5 \times 10^{-9} \exp^{\{12 (T + 273) / 343\}} \exp^{\{S / 0.6) (T + 273) / 273\}}$$

Let us take an example – A Resistor of value **2.2 KΩ** of Low quality working at **45 °C** will have

$\lambda_B = 4.5 \times 10^{-9} \exp^{\{12(45+273)/343\}} \exp^{\{(0.1/0.6) \times (45+273)/273\}}$

$= 4.5 \times 10^{-9} \exp^{\{12 \times 318/343\}} \exp^{\{0.1666 \times 318/273\}}$

$= 4.5 \times 10^{-9} \exp^{(12 \times 0.92711)} \exp^{(0.1666 \times 1.16483)}$

$= 4.5 \times 10^{-9} \exp^{11.12536} \exp^{0.19406}$

$= 4.5 \times 10^{-9} \times 67870.72 \times 1.21417$

$= 370829.399 \times 10^{-9}$ **=** **<u>0.00037</u> per 10^6 Hrs.**

So, the modified Failure Rate of the Resistor $\lambda_P = \lambda_B$ **X** Π_Q **X** Π_E **X** Π_R, where Π_Q **is Quality Factor,** Π_E **is Environment Factor and** Π_R **is Resistance Value Factor.**

λ_P = 0.00037 X 15 X 3 X 1 (values taken from MIL 217F) = <u>0.016687 per 10^6 Hrs.</u>

If the working Temperature is reduced to **30 °C,** λ_B **= 0.00021583 X 10^{-9}**

Modified Failure Rate of the Resistor, $\lambda_P = \lambda_B \times \Pi_Q \times \Pi_E \times \Pi_R$

= 0.00021583 X 15 X 3 X 1 = <u>0.00972 per 10^6 Hrs,</u> an improvement of 41.7%

In addition if we now improve the Quality of the Resistor by using MIL Type**,** Π_Q **is 5 and** λ_P **will change to 0.00324 per 10^6 Hrs, an improvement by 80.6 %.**

<u>Bath Tub Curve</u>

As per the Bathtub Curve, Components can have Decreasing Failure Rate, Constant Failure Rate and Increasing Failure Rate. Reliability of Components with Decreasing Failure Rate can be improved by **Burn-In** and the Reliability of Components with Increasing Failure Rate can be improved by **Preventive Replacement / Repair**. But Reliability of Components with Constant Failure Rate **cannot be improved** by Burn-In or Preventive Replacement / Repair. We are normally **more interested with Components with Constant Failure Rate.**

Before proceeding further, we shall find the Reliability of a Component with Constant Failure Rate,

<u>Example:</u>

A Computer has a **Constant Error Rate** of 1 **Error in 17 Days** of Continuous Operation. What is the **Reliability** associated with the Computer to correctly solve a problem that requires **5 Hrs**?

<u>Answer:</u>

Mean Time To Failure = 17 Days = **408 Hrs.** λ = 1/MTTF = 1/408 = **0.0024 / Hr.**

So, $\mathbf{R_{(5)}} = e^{-\lambda t} = e^{-(0.0024 \times 5)} = e^{-0.012}$ **= 0.99**

The above example shows that Reliability is dependent on Time. So, reliability cannot remain Constant over the whole Life-time of any system. The Table below shows how **Reliability for a Constant Failure Rate Component reduces with Time.**

Constant Failure Rate / Hr	Reliability is reduced to				
	After 1 Year	After 2Years	After 3 Years	After 4 Years	After 5Years
3×10^{-7}	99.9979 %	99.9917 %	99.9829 %	99.9674 %	**99.929 %**
3×10^{-8}	99.999979 %	99.999918 %	99.999628 %	99.99917 %	**99.999945 %**

Improvement in Life-time resulting from an Initial Burn-In Period

Burn-In Testing is designed to **reduce (preferably eliminate) Infant Mortality** of a component **having a Decreasing Failure Rate,** by accumulating **Initial Operating Hours,** prior to User's Acceptance**.** It **increases** the **Mean Residual Life** (MTTF will Increase) of the components that survive Burn-In. an important consideration for performing Burn-In is the Cost Factor, which includes costs due to **Testing, Warranty**, **Components Lost during Test** and **Production Lead Time.**

Components Lost during Test must be Discarded and Replaced by a new one. Life-time without Burn-In is found from $\mathbf{R(t) = \exp [-(T/\theta)]^{\beta}}$ where, **θ is Life-time and β is Weibull Shape parameter.** Given a Reliability R_0 at time t_0, the Burn-In Period T is found from the relation $\mathbf{R(0) = \exp [-(t_0 + T)/\theta)]^{\beta} / \exp [-(T/\theta)]^{\beta}}$.

Example:

Let a component for Axle Counter Card have a **Decreasing Failure Rate** of $\mathbf{\lambda t = 0.0005\ (t/1000)^{-0.5}}$**/ Year.** Find the Influence of a Burn-in Period of **6 Months** on the Life-time of the component, considering Reliability of **0.9.**

Answer: $R_{(t)} = 0.9$, i.e. $\mathbf{\exp [-(t/1000)^{-0.5} = 0.9}$

From this, $\mathbf{t = 1000\ \{-\ln (0.9)\}^2} = 1000 \times (0.10536)^2 = 1000 \times 0.0111 =$ **11.1 Yrs**

When **a** Burn-in Period of **6 Months** (0.5 Yr) is introduced, keeping same Reliability of 0.9, $\mathbf{R_{(t|T)} = 0.9}$, i.e.

$$\mathbf{\exp [-(t + 0.5/1000)^{-0.5}] / \exp [-(0.5/1000)^{-0.5}] = 0.9}$$

So, $\mathbf{t = 1000\ \{-\ln 0.9 + (0.5/1000)^{-0.5}\}^2 - 0.5}$
$= 1000\ \{0.10536 + 0.02236\}^2 - 0.5$
$= 1000\ \{0.12772\}^2 - 0.5 = (1000 \times 0.1631) - 0.5 = 16.31 - 0.5 =$ **15.81 Yrs**

There is an **Increase of 4.71 Yrs** in the **Designed Life of the component**.

Constant Failure Rate and Preventive Replacement

It is important to make it explicitly clear that if a component has a Constant Failure Rate, then Preventive Maintenance of the Component will have **no effect** on the **Component's Failure occurrences.**

Example:

Let us consider a component with an ***MTTF* = 100 hrs,** i.e. **λ = 0.01**, and with **Preventive Replacement,** after every **50 hours**. Find the change in Reliability of the component from 0 to 60 hours in comparison with the case when no Component is Replaced.

Answer:

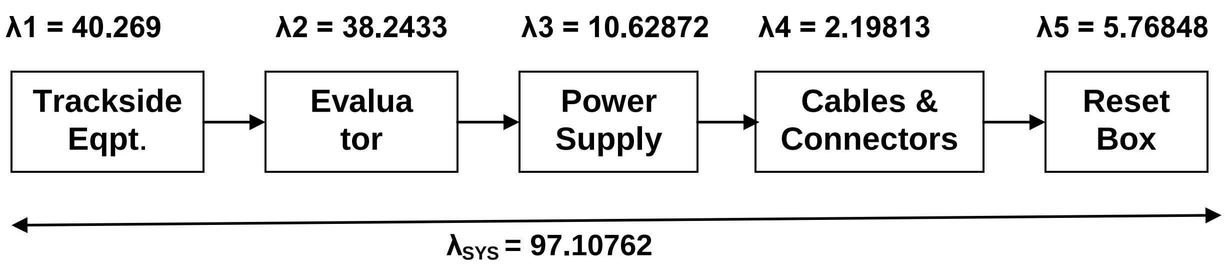
Reliability of the original component, $\mathbf{R_{original}}$ is $\mathbf{R_{50}}$ = **0.6065**
Reliability of the new component, $\mathbf{R_{new}}$ is $\mathbf{R_{10}}$ = **0.9048**
Resultant Reliability $\mathbf{R_{60}}$ will be $\mathbf{R_{60}} = \mathbf{R_{50}} \times \mathbf{R_{10}} = 0.6065 \times 0.9048 = \mathbf{0.5488.}$

Without preventive maintenance, the reliability of the same component operating for 60 hours, is R_{60} **= 0.5488.**

Thus, **Replacement of Component has no Effect on Reliability.**

Reliability Bock Diagram

Let us now consider the **Reliability Block Diagram** of **Universal Axle Counter**.



If we calculate individual Reliability values for the Units, we find

R1 = 0.99995963, R2 = 0.9999617, R3 = 0.9999894, R4 = 0.9999978 and R5 = 0.9999942

So, R_{SYS} = R1 X R2 X R3 X R4 x R5
= (0.99995963 x 0.9999617 x 0.9999894 x 0.9999978 x 0.9999942) = **0.999902865**

If we separately calculate R_{SYS} from λ_{SYS} the value is **0.999902897**

Effect of Redundancy on Reliability

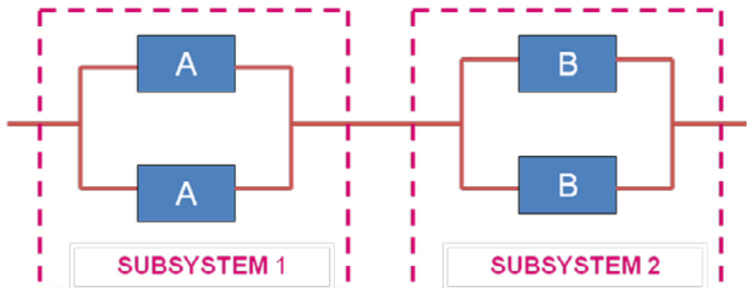
Redundancy is the existence of **more than one Way** to perform a required Function. To avoid Common Mode Failures, Redundant Elements must work Independent from each other. Redundancy can be achieved by Hardware, Software as well Time. Redundant Elements appear in **Parallel** in the Reliability Block Diagram. Redundancy can be in different Modes:

- **Active or Hot** – Failure Rate is **same in all Units**.
- **Warm or Lightly Loaded** – Failure Rate in **Redundant Unit is lower** than the Operating Unit.
- **Standby or Unloaded** -- Failure Rate in Redundant Unit is **assumed to be Zero**.

System Redundancy can be achieved in two ways. Each Component of the System may have **one or more Parallel Subsystems** or the whole System can be in **Parallel to one or more Identical Systems**. The former configuration is known as **Low Level Redundancy** and the later as **High Level Redundancy**.

Let us consider the case of an Equipment having two Units **A and B in series**. We will now study the difference between Low Level and High Level Redundancy Configurations as per their Influence on System Reliability.

<u>A) Low level Redundancy</u>

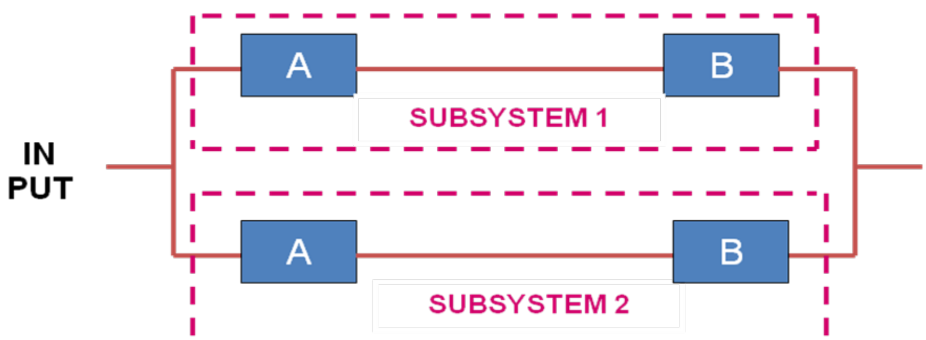


Suppose 'A' has R(a) = **0.99** and 'B' has R(b) = **0.98**

Then, subsystem 1 has $\mathbf{R_{sys1}}$ = 1 – (0.01 x 0.01) = **0.9999** and
subsystem 2 has $\mathbf{R_{sys2}}$ = 1 – (0.02 x 0.02) **= 0.9996**

Then, System Reliability will be **(R_{SYS1} X R_{SYS2}) = 0.9999 X 0.9996 = 0.9995**

<u>B) High Level Redundancy</u>



Using Reliability values R(a) = 0.99 and r(b) = 0.98, both the subsystems have **R_{sys} = 0.99 x 0.98 = 0.9702.**

System Reliability will be $\{1- (1- R_{SYS})^2\}$ = 1 – $(0.0298)^2$ = 1 – 0.000888 = 0.999112

Thus, **Reliability is more in Low level Redundancy.**

Spare Parts Provision

Depending on Failure Rate and either Repair or Replacement facilities, adequate Spare Parts must be stored. This Task is very important since Mean Time To Repair / Replacement must be reduced to improve Maintainability. Again Spare Part Logistic Support can be classified as **Centralized** and **Decentralized.**

Example:

A Component with a Constant Failure Rate **λ = 1X10^{-3} /Hr** is used Three Times in a System. Determine the **Minimum number of Spare Components** to be kept in Stores to cover a cumulative Operating Time of **10,000 Hrs**, with a Probability **γ >>0.9**?

Answer:

From table, we can find that for γ >>0.9, d = **1.28.**
Number of total **Expected Failures in the System** is (3 x 10000 X0.001) or **30.**
For components with Constant Failure Rate, **K is 1.**

So, Number of Spare Parts

$$\mathbf{n = [(k.d/2) + \sqrt{\{(k.d/2)^2 + 30\}}]^2}$$
$$= [(1X1.28)/2 + \sqrt{\{1X1.28/2)^2 + 30\}}]^2$$
$$= [0.64 + \sqrt{\{\{0.64)^2 + 30\}}]^2$$
$$= [0.64 + \sqrt{30.4096}]^2$$
$$= [0.64 + 5.51449]^2$$
$$= [6.15449]^2 = 37.8777 \text{ or } \mathbf{38}$$

Spare Parts Calculation

Let $\lambda = 1 \times 10^{-5}$ / hr. be the Constant Failure Rate of a vital spare part in a system. There are 6 systems installed and a cumulative operating time of **50,000 hrs** for each system is needed. Desired **System Reliability** is $\geq$ **0.99**. How many Spare Parts are needed?

Answer:

a) For Centralized Store

No. of Failures = 50000 / 100000 = 0.5 $\approx$ 1
Reliability of the system is = 0.99
For this value, d = 2.33 (from **Standard Normal Distribution Table**) and kd/2 = 1.165
Now $kt\lambda$ = 6x50000x0.00001 = 3

So, $n = [kd/2+ \{(kd/2)^2 + kt\lambda\}^{1/2}]^2$
$= [1.165+ \{(1.165)^2+ 3\}^{1/2}]^2$
$= [1.165 + 2.0874]^2 = (3.2524)^2 = 10.57 \approx$ **11**

b) For Decentralized Store

No. of Failures = 50000 / 100000 = 0.5 ≈ 1
Individual Reliability at each system is $(0.99)^{1/6}$ = 0.99888
For this value, d = 2.99 (from **Standard Normal Distribution Table**) and kd/2 = 1.495
Now ktλ = 50000x0.00001 = 0.5
So, $n = [kd/2+ \{(kd/2)^2 + kt\lambda\}^{1/2}]^2$
$= [1.495+ \{(1.495)^2+ 0.5\}^{1/2}]^2$
$= [1.495 + 1.6538]^2 = (3.783)^2 = 9.915 \approx \mathbf{10}$

For the System having six equipment, total spares needed will be 60. Thus, **Decentralized Stores need much more spares.**

Adequacy of Spare Parts

Example:

Suppose a Vital Component in an Interlocking Equipment has a Failure Rate of **0.000003/ Hr**. Repair Laboratory has procured **Two** Spare components if the Designed Life of the Equipment is **20 yrs**, find the Probability that the **Spares will be adequate for 10 such equipment.**

Answer:

Over the Life of the Total Network of 10 Microwave equipment, the expected number of Failures is **(10 x 0.000003 X 20 x 8760**) or **5.256**. Reliability of 2 or less failures occurring over 20 yrs is

$$R_{(20)} = \sum_{n=0}^{2}\{e^{-5.256}(5.256)^n\}/n!$$
$$= e^{-5.256}\{(5.256)^0/0! + (5.256)^1/1! + (5.256)^2/2!\}$$
$$= 0.005216\{(1 + 5.256 + (27.625536)/2\}$$
$$= 0.005216 \times 20.068768 \quad \mathbf{= 0.1046787}$$

Influence of Inspection Periodicity on Availability

Sometimes Failures remain **dormant or undetected** in a system and Availability can be influenced by the **Frequency of Inspection**, provided Replacement or Repair of any Faulty Component is done during Inspection. If λ is the Failure Rate, t1 is the Inspection Time, t2 is the Repair / Replacement time and T be the time between Inspections, then $\mathbf{[T + t1 + t2\{1-(1-e^{-\lambda T})\}}$ is the **Time from Completion of one Inspection Time to start of the next Inspection**. So, Availability $\mathbf{A_{(T)}}$ is given by

$$\mathbf{A_{(T)} = (1 - e^{-\lambda T}) / \lambda\, [\, T + t1 + t2\,(1 - e^{-\lambda T})}$$

One important point to be noted is that **inspection cannot improve Reliability** but can only **improve Availability.**

Example:

Let us consider Universal **Axle Counter** equipment having a Constant Failure Rate of **0.0000971 Failure/ 10^6 Hrs.** Any defective component would be replaced / repaired, if found defective during the Periodic Inspection. The Inspection Time is 1 Hr and Repair / Replacement takes 8 Hrs (worst case). What is the optimum time between inspections?

Answer:

We use the formula $\mathbf{A_{(T)} = (1 - e^{-\lambda T}) / \lambda\, [T + t1 + t2\, (1 - e^{-\lambda T})]}$ where,
λ = 0.0000971, t1 = 1 hr, t2 = 8 hr and **T = Inspection periodicity**.

Let us consider **168 hrs, 336 hrs, 504 hrs** and **672 hrs** as the Inspection intervals and find Availability at these Periods.

$\mathbf{A_{(168)}} = (1 - e^{-0.0000971 X 168}) / 0.0000971[168 + 1 + 8(1 - e^{-0.0000971 X 168})]$
$= (1 - e^{-0.0163128}) / 0.0000971[169 + 8(1 - e^{-0.0163128})]$
$= (1 - 0.98388195) / 0.0000971\ [169 + 8\ (1 - 0.98388195)]$
$= 0.0161804 / 0.0000971\ [169 + 8\ X(0.0161804)]$
$= 0.0161804 / 0.0000971\ X\ 169.1294432$
$= 0.0161804 / 0.01642247$
$\mathbf{= 0.9852598}$

Similarly, $\mathbf{A_{(336)}}$ **= 0.9801959,** $\mathbf{A_{(504)}}$ **= 0.9732559 and** $\mathbf{A_{(672)}}$ **= 0.9662714.**

The above calculations show that Maximum Availability is for an **Inspection interval of 168 hrs.** To have a more precise value let us now consider Inspection Periodicity of **96 hrs** and **240 hrs.**

$\mathbf{A_{(96)}}$ **= 0.98434** and $\mathbf{A_{(240)}}$ **= 0.983582**

We now find that **Availability reduces** if Inspection Period is either reduced to 96 hrs or increased to 240 hrs. So, we decide that the **Optimum Availability** will be for an **Inspection Interval of 168 hrs or once in 7 Days.**

T(Hrs)	96	**168**	240	336	504	672
$\mathbf{A_{(T)}}$	0.98434	**0.9852598**	0.983582	0.9801959	0.9732559	0.9662714

Software Metrics

Since Railway Signaling systems are Safety critical, both Static and Dynamic Testing are to be implemented during V & V task. For Static Analysis, generally **Control Flow Analysis** and **Data Flow Analysis** both are used. In Dynamic Analysis, **Equivalence Partitioning**, **Boundary Value Analysis** and **Structural Testing** are needed.

Some of the important Quantified Parameters used are:

- **No. of Statements** executed at least once,
- **No. of Decision outcomes** evaluated at least once,

- **No. of Paths** executed at least once,
- **No. of Linear Code Sequence And Jump (LCSAJ)** executed at least once
- **No. of Branch Condition operand Values** evaluated at least once,
- **No. of Branch Condition combinations** evaluated at least once and
- **No. of Boolean Operator Input conditions** evaluated at least once.

An example of quantified Software testing is showed below.

Total Statements	= **10**
Nested Levels	= **4**
Total No. of Lines	= **79**
Source Only Lines	= **21**
Source & Comments Lines	= **0**
Comments Only Lines	= **55**
Empty Lines	= **3**
Comments Lines Rate	= **69.62%**

Importance of Training in Safety Management

Signal Engineers should get exposure to Hazard Analysis, Safety & Reliability Calculations and Detailed Safety Reviews leading to preparation of Safety Case. Risk Identification Analysis and Assessment techniques e.g. Hazard Identification and Ranking, Causal Analysis, Consequence Analysis, Loss Analysis, Options Analysis and Impact Analysis are also to be discussed.

In order to overcome this problem with Modern Signalling, the building of a structure, which gives consideration to the interfacing of Human and System, is essential. A **Safety Culture i**s to be established throughout the Organization. Concept of **Safety Management** during Design, Procurement, Installation and Maintenance of the System has thus become very vital for Signalling Department. Training plays a vital role to sustain Safety-Management. **Indian Railways Institute of Signal Engineering and Telecommunications (IRISET)** has the responsibility to make the S & T Engineers of Indian Railways **conversant with the various Knowledge Domains** and **competent to face the challenges of Safety Management of Modern Signalling Equipment** thereby **playing a vital role to sustain Railway Transport.**

Quality Policy of IRISET tells that it will impart quality training in the field of Signal Engineering and Telecommunication:

- Which are **aimed at bridging Competency gap in Trainees**
- Whose **Contents are current**
- Which **builds a Curiosity among Trainees to learn more** and
- Which **are of Practical values**.

Faculty Members, both Officers and Instructors are posted **on deputation** for a tenure of 3 to 5 years, from the Zonal Railways and each of them are proven Experts in their Domain and have ample Experience. In addition, Updating Faculty knowledge is a continuous process at IRISET. **Interactions** with **Manufacturers, Universities** and **Test Centres** are regular events. **Field Experts** from Maintenance and Construction wings of Railways and Industry deliver **Guest Lectures**. Visit to Installation Sites and Industries are regularly arranged for the Trainees. In addition to these, during the course, some hours are earmarked for **screening Technical Documentaries through CDs / DVDs. Video Conference** and **E- Learning** have been recently added as supplementary teaching aids.

The Institute has **11 full-fledged Laboratories** – **Mechanical Signalling, Block Signalling, Electrical Signalling, Outdoor Electrical Signalling** and **Modern Signalling** Labs in Signal branch and **Telephony, Microprocessor & Control, Microwave & Optic Fibre, Outdoor Telecom, Computer** and **Network** Labs in Telecommunication branch. There are **12** Ergonomic **Classrooms** with LCD Projectors and Public Address system. All the Faculty members have networked PCs for preparing Course Modules. A Corporate quality **Conference Hall** is used for Faculty meetings and Classes for Higher level Executives.

Knowledge on **Fail-safe Electronics, Fail-safe Data Transmission, Solid State Interlocking, Universal Block Interfacing, Digital Axle Counter, Auxiliary Warning System, ERTMS** and **Anti Collision Device** is part of Modern Signaling curriculum. Installation and Maintenance procedures are dealt in detail. **CENELEC Standards, ALARP concept** and **Safety Integrity Levels** are compulsorily taught in all Initial Courses. Interlocking Equipment invariably contains several stages and the concept of **Reliability Block Diagram** help in understanding the System better. Trainees are also exposed to the various system dependability techniques like **Fault Avoidance, Fault Tolerance, Fault Removal** and **Fault Forecasting.**

They also learn **Logistic Engineering, Supply Chain Management, Human Interfacing, FMECA** and **Fault Injection Techniques.** They get exposure to **Hazard Analysis, Safety & Reliability Calculations** and **Detailed Safety Reviews** leading to **preparation of Safety Case.** Risk Identification Analysis and Assessment techniques e.g. **Hazard Identification** and **Ranking, Causal Analysis, Consequence Analysis, Loss Analysis, Options Analysis** and **Impact Analysis** are also discussed. They are told that **Reliability** is a **Time-dependant function.**

IRISET also includes topics like **Reliability, FMECA, and Fault Injection Techniques** in special Courses**.** Reference of **MIL Standards 217** and **338** is introduced in this connection. Since nowadays many of the Signalling Equipment are Communication Line dependent, the idea of **Fail-safe Communication** and **Behaviour of Transmission Lines in Railway Signalling** are also introduced. **ORE Standards 155.2 and 118** are referred to the Trainees of Modern Signalling Courses.

All these show that the **Training Centre is fully aware of its responsibilities** to **enhance competency** in **Modern Signalling Safety Management** and can claim to be a **Global Centre for Excellence.**

Conclusion:

This Paper brings out the importance of Quantitative Techniques in Design and Maintenance of growingly Safe but Complex Equipment and Systems used in Railway Signalling. Mathematical Calculations help in increasing our Confidence in Predicting about the Probability of Failure in Dangerous Mode and taking better decisions in Maintenance Strategy.