

# Introduction to System Reliability Modelling

## Part 2 - Basic and Mission Reliability Block Diagrams

These methods are based on MIL-HDBK-338B.

**Sentient Systems Ltd in support of  
Reliability-Advice.co.uk**



## Part 2 Contents:

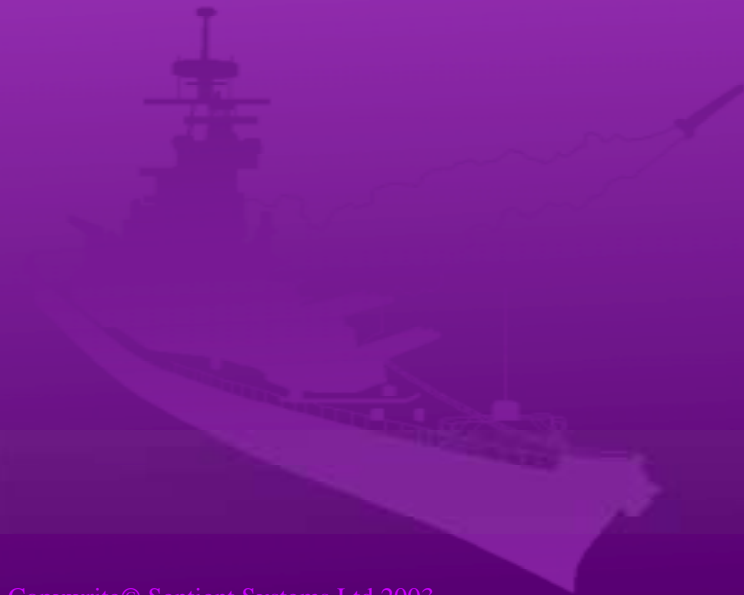
- Basic Reliability Block Diagrams
- Mission Reliability Block Diagrams

## Part 2 Prerequisites:

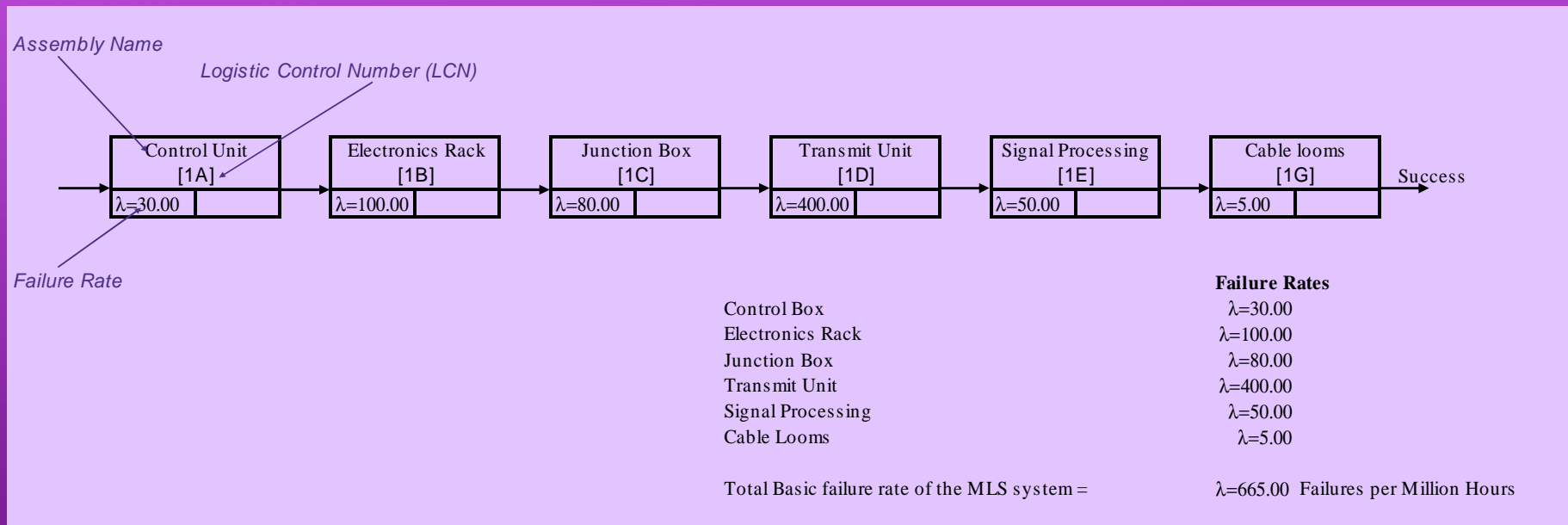
- Familiarity with the subject matter of Part 1.

## So what does the model look like?

- The Basic Reliability Block diagram -



# Basic Reliability Block Diagram for the MLS system



## MLS System?

- The example system is known as a Microwave Landing System (MLS).
- It transmits a Microwave radio signal from the flight deck of the ship which the approaching helicopter uses to navigate to the landing platform.

## Basic reliability block diagram

- The Basic reliability diagram is a **series arrangement** of blocks connected by lines. Each block would have a failure rate calculated or arrived at in some way. The total or Basic failure rate for the system is simply the addition of the failure rates of the blocks.

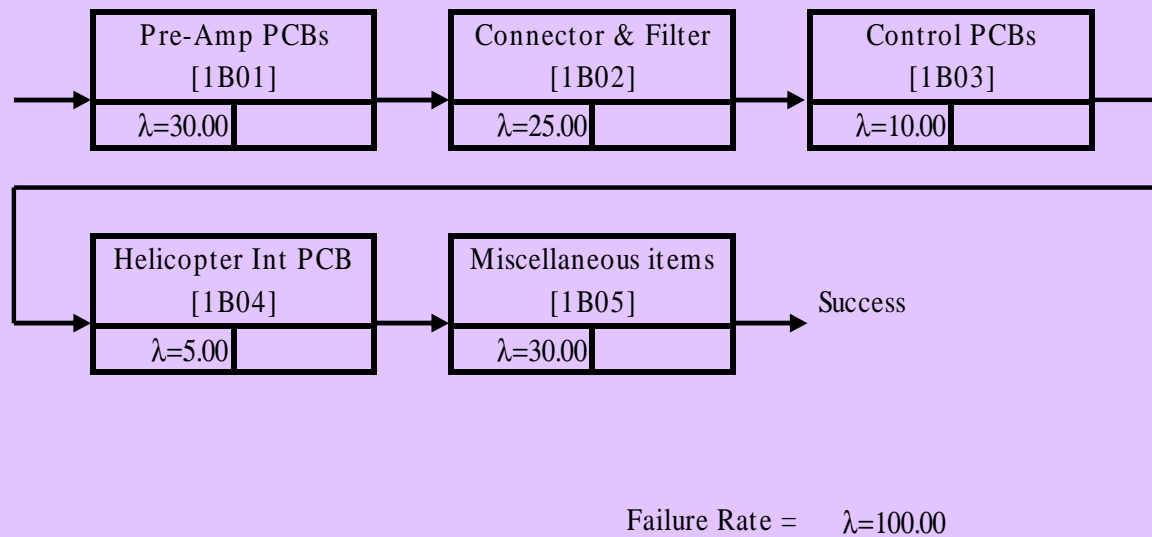
## Basic reliability block diagram

- Each block represents a part of the system. In this example there are six major sub-divisions.
- Each block is labelled and the failure rate,  $\lambda$  (lambda) is given in the block. A summary table is provided for report purposes.
- The word “Success” or “Survival” is sometimes included at the end of the chain.

## Basic reliability block diagram

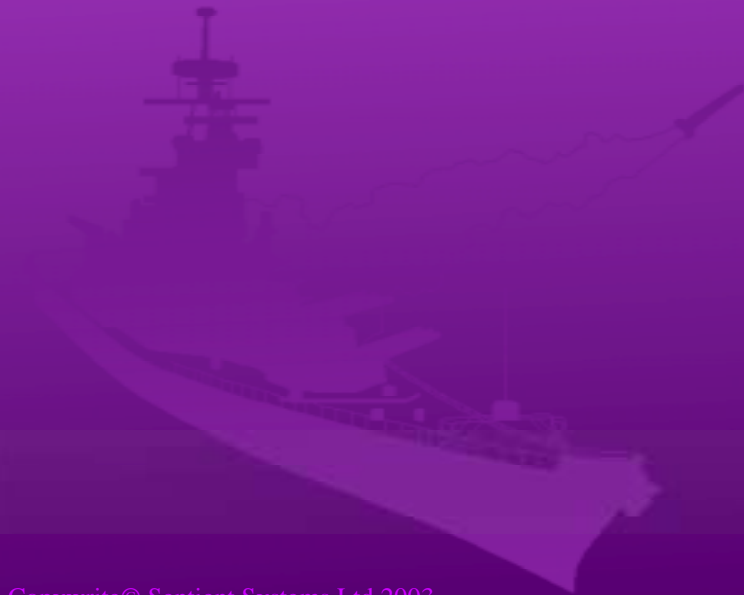
- A second example, in this case one of the blocks in the system diagram, illustrates that the chain may be folded to better occupy a page if the number of blocks necessitate this.
- This also illustrates why a hierarchical approach is more often than not used to describe complex systems reliability.

# MLS Electronics Rack



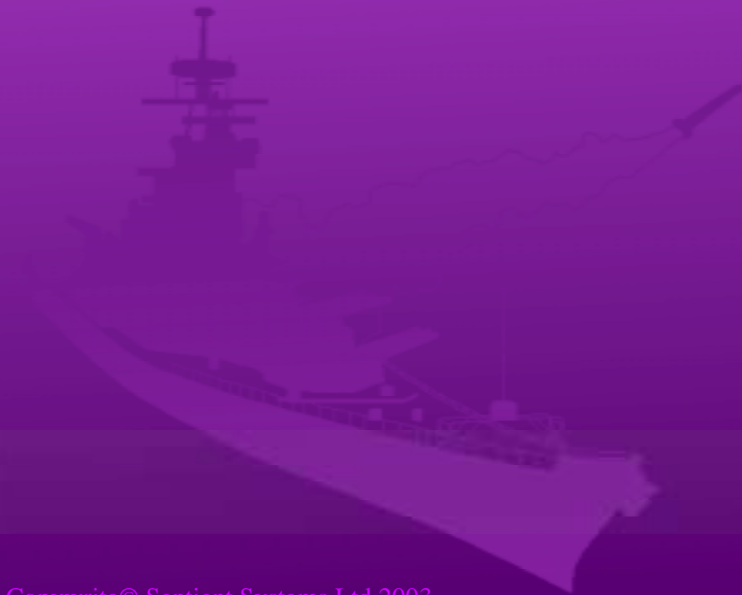
## Note:

- Although we have used  $\lambda$  and expressed reliability as a failure rate in our example this is not always preferred and it is not strictly correct. It is often expressed as a probability of survival or success,  $P_s$ .



## Will it be all right on the night?

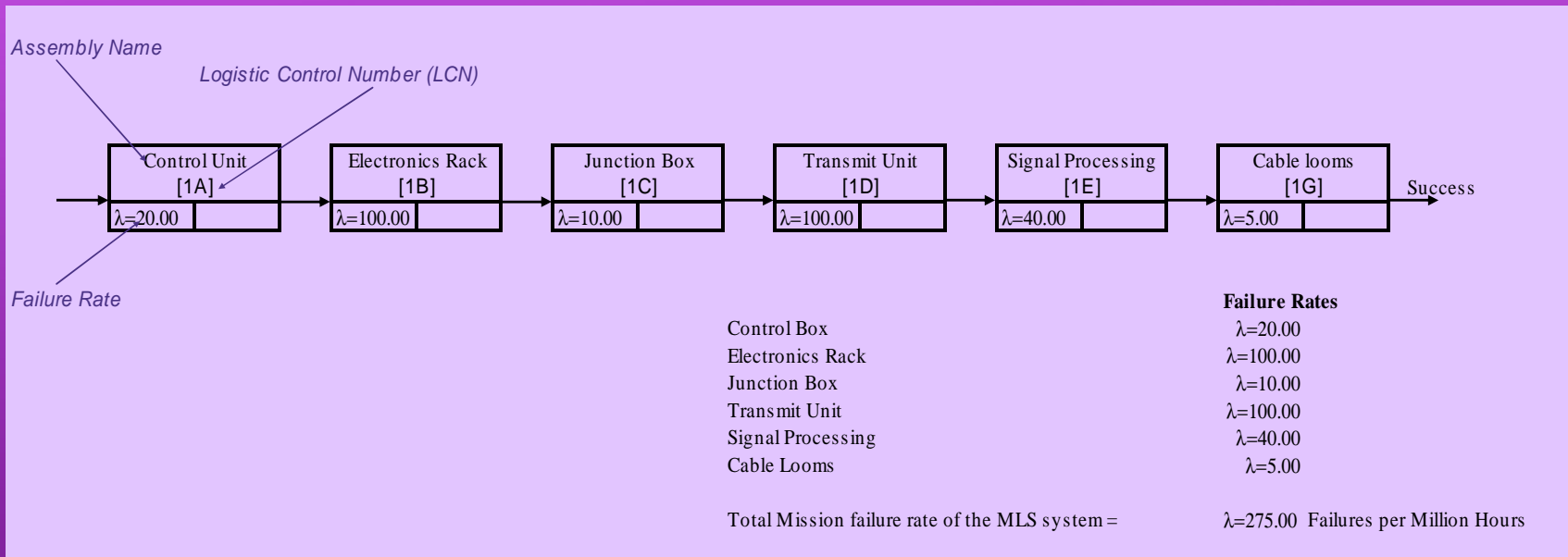
- The users of the equipment, in this case the Navy, are more concerned with “will it be all right on the night?” In other words, “what are the chances of it failing just when I need it to help land a helicopter?”



## What can fail might not matter:

- Not every possible failure in the system will cause the system to fail.
- By working to **reliability objectives** the designer would have taken steps to avoid system failure due to single causes or **single point failures**.
- Otherwise, **critical items** are identified.

# Mission Reliability Block Diagram for the MLS system



## So what's the differences?

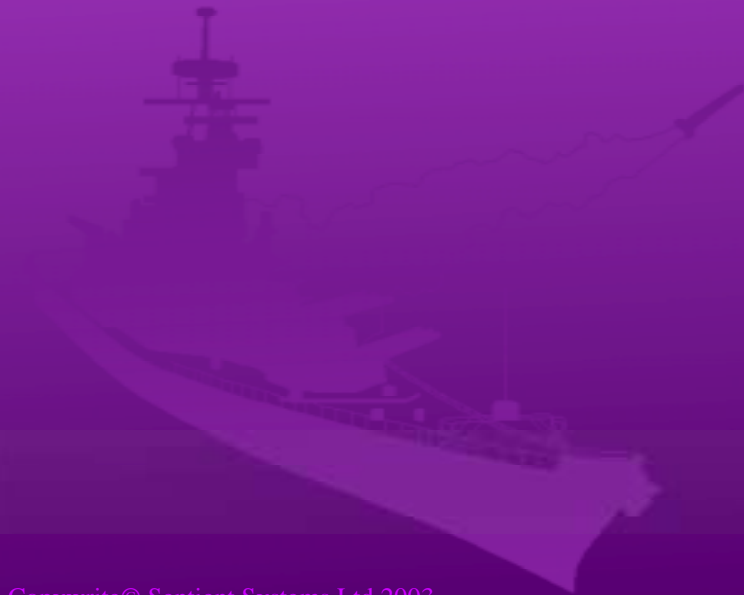
- In this example the Basic and Mission diagrams look the same but for the failure rates, but this is only our example. In lots of cases they will look quite different.
- The failure rates differ because only those that contribute to Mission failure are included and the totals are calculated according to the laws of **redundancy**.

## This is only the top level:

- Remember the model is hierarchical and the lower levels will show only those functions of the system that contribute to Mission success by eliminating those that do not contribute to success.
- As it happens, analysis of this system revealed that the Mission reliability criteria would not be realised.

## What does this tell us?

- Only a simple design approach has been taken to ensure that the Mission reliability has to meet demanding criteria.
- The model is simplified and does not account for **repair time/(down time)**.



## How well did it meet the requirement?

- It didn't.
- The analysis was conducted far too late in the development cycle in the face of an overconfident design function and over reliance on simplified reliability concepts.
- No account was taken for down time in the design!

**So what is the approach? There are several.**

- 1) The magic rule of system Mission survival or the axiom of system Mission survival - the **Reasoned approach**.
- 2) The **Boolean** approach.
- 3) **Probability Maps** approach.
- 4) **The Logical** approach.

## The magic rule : (or just gobbledygook?)

- The probability of a system surviving a mission,  $P_S$ , is equal to the probability of survival - given that a specific part or portion of the system works,  $P_{X_s}$  multiplied by the Reliability of that part of the system,  $R_X$  plus the probability of survival - given that the portion of the system fails,  $P_{X_f}$  multiplied by the Unreliability of that portion of the system  $Q_X$ !

$$P_S = P_{X_s} \cdot R_X + P_{X_f} \cdot Q_X$$

## Clear as mud?

$P_s$  = Probability of system mission survival.

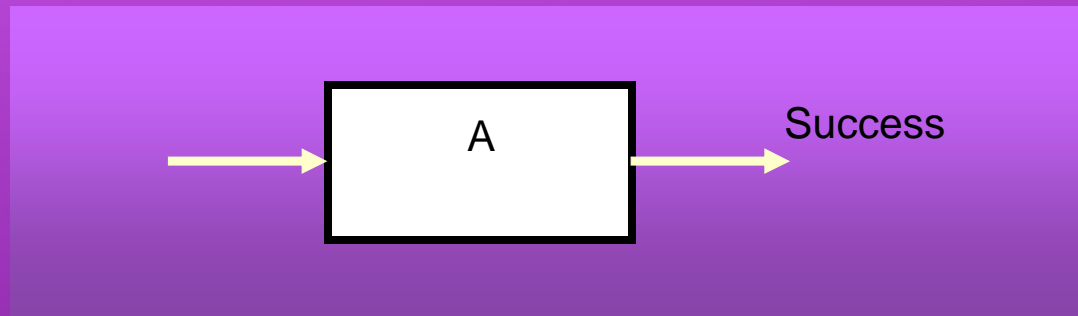
$P_{Xs}$  = Probability of system mission survival if a portion, X of the system is functional.

$P_{Xf}$  = Probability of system mission survival if a portion, X of the system is non-functional (failed).

$R_X$  = Reliability of the portion, X of the system.

$Q_X$  = Unreliability of the portion, X of the system =  $(1 - R_X)$ .

**To test the axiom on a trivial example:**



**If there is only one portion to the equipment then the Mission survival diagram looks like this.**

## To test the axiom on a trivial example:

- The probability of the survival of the equipment is obviously the same as the probability that the equipment will continue to function.
- To keep our test simple we will assume that random failure is our only concern - but in fact there are other factors, hostile action for example.

## So does the axiom say the same thing ?

$P_S$  = the probability of mission survival (given that the equipment, A works)

This bit is clearly equal to unity in our simple test

\* Reliability of A, ( $R_A$ ) +

the probability of mission survival (given that the equipment, A fails)

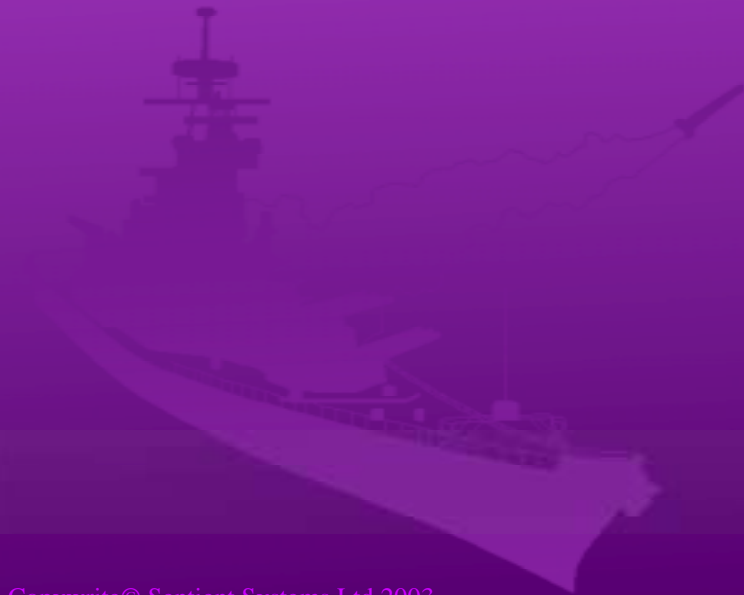
and this bit is equal to zero in our test.

\* the Unreliability of A, ( $Q_A$ )

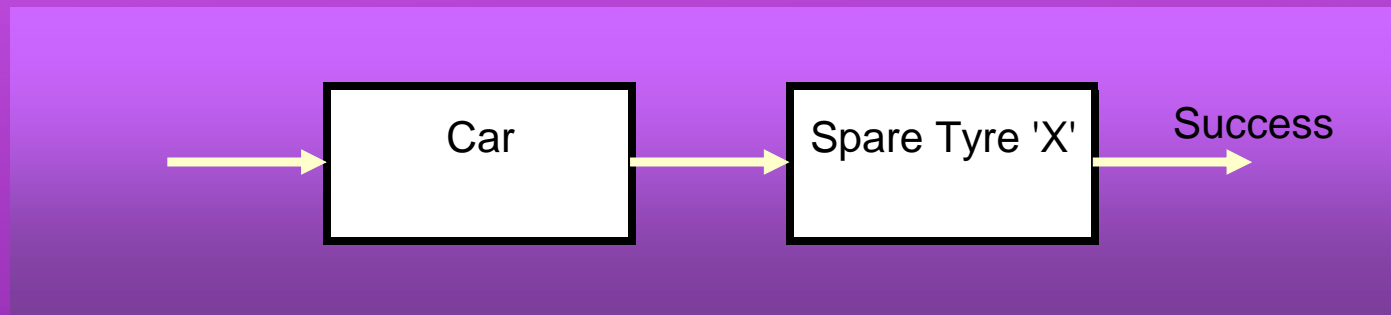
Hence,  $P_S = 1 * R_A + 0 * Q_A$ , where  $Q_A = 1 - R_A$

## Simple really!

- So in this simple case the probability of equipment survival,  $P_S$  is equal to the Reliability of the equipment,  $R_A$ .
- Remember we only considered random failure.



## 'Car Tyre' Example:



**The equipment Mission survival diagram looks like this and is meant to convey the idea that Mission survival depends on both A and B functioning. Assuming 'X' is a car tyre and that the car has 1 spare tyre. Tyre has a reliability of 0.8. The rest of the system has a probability of success of 0.4**

## Car Journey (with spare tyre):

$P_s$  = Probability of successful car journey

$P_{xs}$  = Assuming tyre 'X' is OK, Probability that the rest of the car is able to complete the journey. (0.4)

$P_{xf}$  = Given that tyre 'X' is punctured, probability that the car will still be able to complete the journey. (0.4)

$R_x$  = Reliability of the tyre (0.8)

$Q_x$  = Unreliability of the tyre (0.2)

$$P_s = P_{xs} * R_x + P_{xf} * Q_x$$

$$P_s = 0.4 * 0.8 + 0.4 * 0.2 = 0.4$$

## Car Journey (with NO spare tyre):

- If we now assume that the car has **no spare tyre**. Tyre still has a reliability of 0.8. The rest of the system has a probability of success of 0.4



## Car Journey (with NO spare tyre):

$P_s$  = Probability of successful car journey

$P_{xs}$  = Assuming tyre 'X' is OK, Probability that the rest of the car is able to complete the journey. (0.4)

$P_{xf}$  = Given that tyre 'X' is punctured, probability that the car will still be able to complete the journey. (0)

$R_x$  = Reliability of the tyre (0.8)

$Q_x$  = Unreliability of the tyre (0.2)

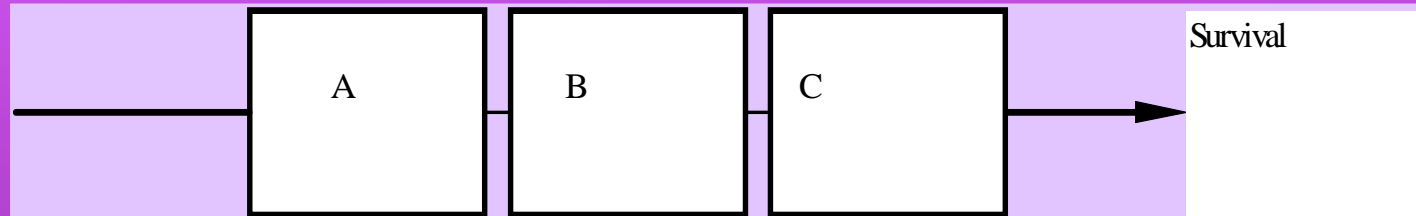
$$P_s = P_{xs} * R_x + P_{xf} * Q_x$$

$$P_s = 0.4 * 0.8 + 0 * 0.2 = 0.32$$

## Car Journey conclusions

- The Car Journey example demonstrates that the  $P_s$  equation allows the user to apply either *redundancy* (where  $P_{xf} = P_{xs}$ ) or *mission criticality* (where  $P_{xf} = 0$ ) to a particular item. As shown in the examples above, a ‘redundant’ item (car tyre with spare) means that the reliability of the tyre does not influence mission success and is therefore not factored into the Probability of mission success. Conversely, a ‘mission critical’ item (car tyre with no spare) means that the reliability of the tyre does influence mission success and needs to be factored in.

## just one more series model:



$P_S$  = the probability of mission survival (given that the equipment, A works)

*This bit is equal to unity as before but modified by the probability that equipment B and C are working.*

\* Reliability of A, ( $R_A$ ) +

the probability of mission survival (given that the equipment, A fails)

*This bit is obviously zero as before.*

\* the Unreliability of A, ( $Q_A$ )

Hence,  $P_S = R_B * R_C * R_A + 0 * Q_A$ , where  $Q_A = 1 - R_A$

$$P_S = R_B * R_C * R_A$$

**and so on for any series arrangement.**

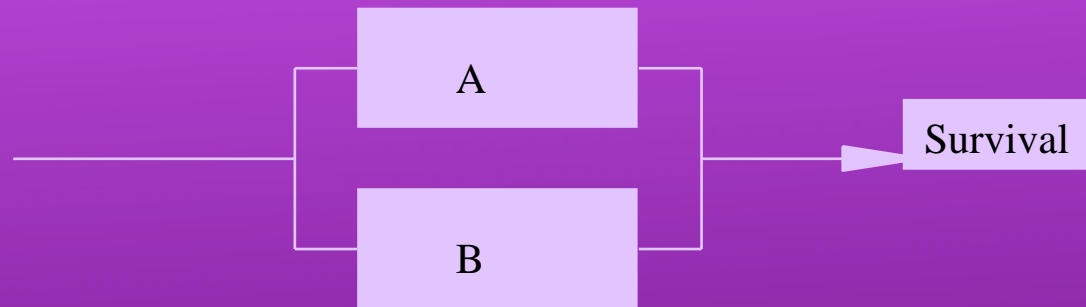
$$P_s = \prod_{i=1}^n R_i$$

- Where  $R_i$  is the reliability of the  $i$ th item of equipment in the system and  $n$  is the number of items.

## Redundancy:

- a **redundant** configuration increases the probability of mission survival
- but at a cost. The overall reliability (Basic) goes down.
- Redundancy is probably the simplest of several techniques for increasing Mission reliability.

## example of active redundancy:



- The Mission survival diagram looks like this and is meant to represent the idea that mission survival depends on either A or B functioning.

## Beware:

- Remember, the magic rule only works if the probability of failure of each part is unaffected by that of another part.



## Active redundancy?

- The two parts, A and B are functional and independent. Either can perform the function of the other.
- This is easily stated but very difficult in anything other than the most basic elements.
- Standby, switched standby, auto-reconfiguration are some of the other options.

## Here's the statement:

$P_S$  = the probability of mission survival (given that the equipment, A works) \* Reliability of A, ( $R_A$ ) +

This bit is equal to unity as before but it is not affected by the probability that equipment B is functional.

the probability of mission survival (given that the equipment, A fails) \* the unreliability of A, ( $Q_A$ )

This would be zero if it only depended on A but it must be equal to the probability that B is functional, i.e the Reliability of B,  $R_B$ .

## and here's the algebra:

Hence,  $P_S = 1 * R_A + R_B * Q_A$ , where  $Q_A = 1 - R_A$

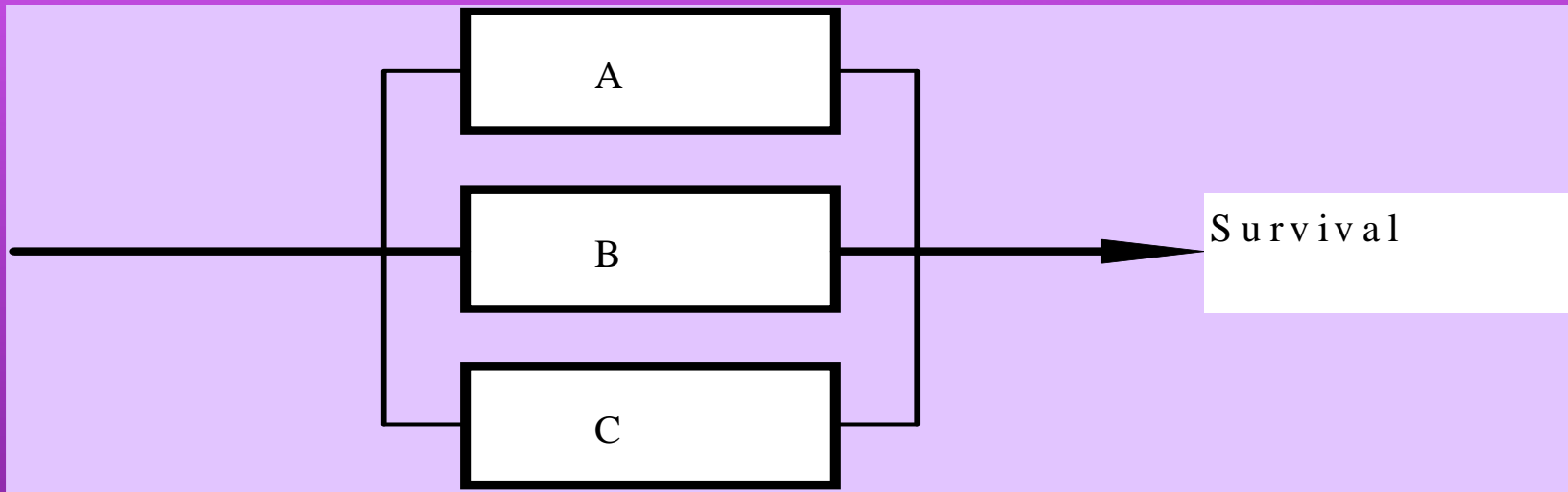
$$P_S = R_A + R_B(1 - R_A)$$

$$P_S = R_A + R_B - R_A R_B$$

and if A and B are identical (but s independent):

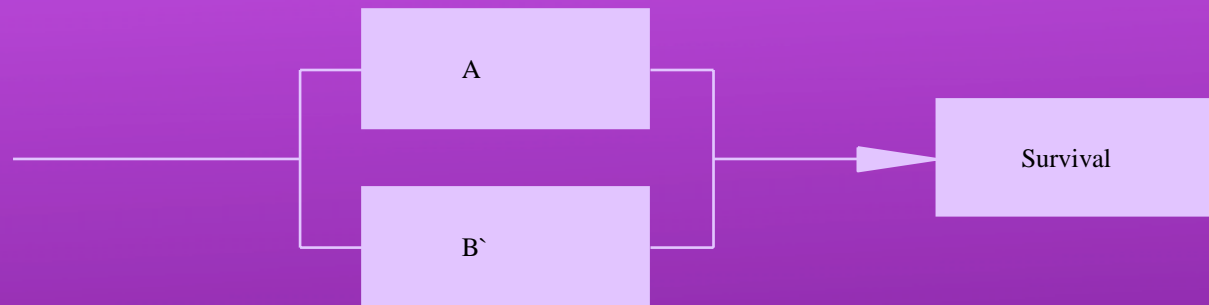
$$P_S = 2 * R_A - R_{A^2}$$

## More redundancy:



- ▼ Mission survival depends on either A or B or C functioning.
- ▼ The survival equation can be derived from the dual redundant arrangement in the last example. Consider that equipment B and C are combined as in the last example as  $B'$ :

**simplified:**



$$PS = RA + RB - RARB$$

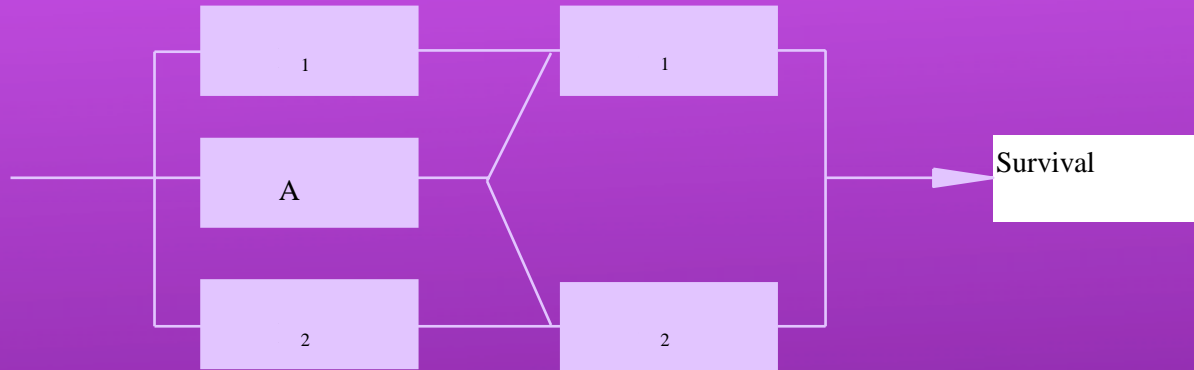
$$RB' = PB' = 1 * RB + RC * QB, \text{ where } QB = 1 - RB$$

$$PB' = RB + RC(1 - RB)$$

$$PB' = RB + RC - RBRC$$

$$\text{Therefore } PS = RA + RB + RC - RARB - RARC - RBRC + RARBRC$$

## a numerical example:



and let  $C2 = C1$  and  $B2 = B1$  for simplicity.

## a numerical example (cont):

$P_S$  = the probability of mission survival (given that the equipment, A works) \* Reliability of A, ( $R_A$ ) +

This bit is equal to the probability that  $C_1$  or  $C_2$  is functional,  $(2 * R_C - R_C^2)$  multiplied by the probability that A is functional,  $R_A$ .

the probability of mission survival (given that the equipment, A fails) \* the unreliability of A, ( $Q_A$ )

This bit is equal to the probability that  $B_1$  and  $C_1$  or  $B_2$  and  $C_2$  are functional,  $[2 * (R_B * R_C) - (R_B * R_C)^2]$

$$\text{Therefore } P_S = (2 * R_C - R_C^2) R_A + [2 * (R_B R_C) - (R_B R_C)^2] * (1 - R_A)$$

## a numerical example (cont):

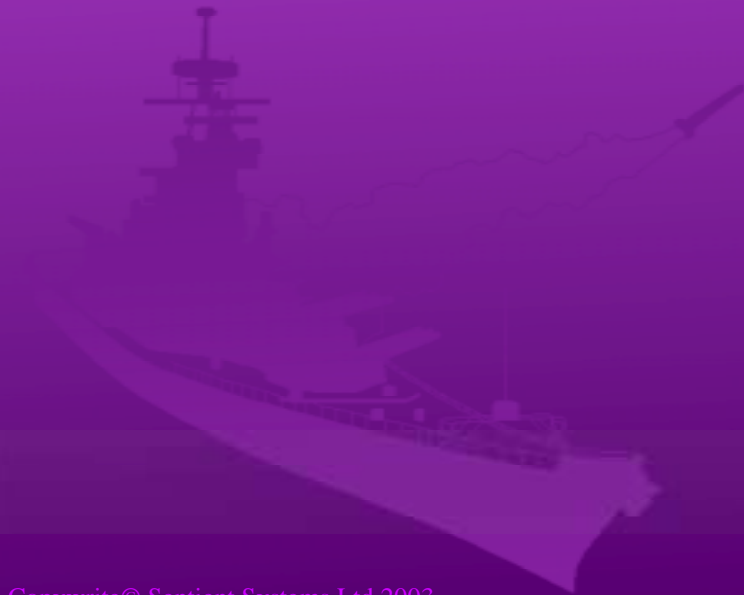
$R_A = 0.3$ ,  $R_{B1} = R_{B2} = 0.1$  and  $R_{C1} = R_{B2} = 0.2$

and therefore,

$(1 - R_A) = 0.7$ ,  $(1 - R_B) = 0.9$  and  $(1 - R_C) = 0.8$

then,  $P_S = (0.4 - 0.04) * 0.3 + (0.04 - 0.0004) * 0.7$

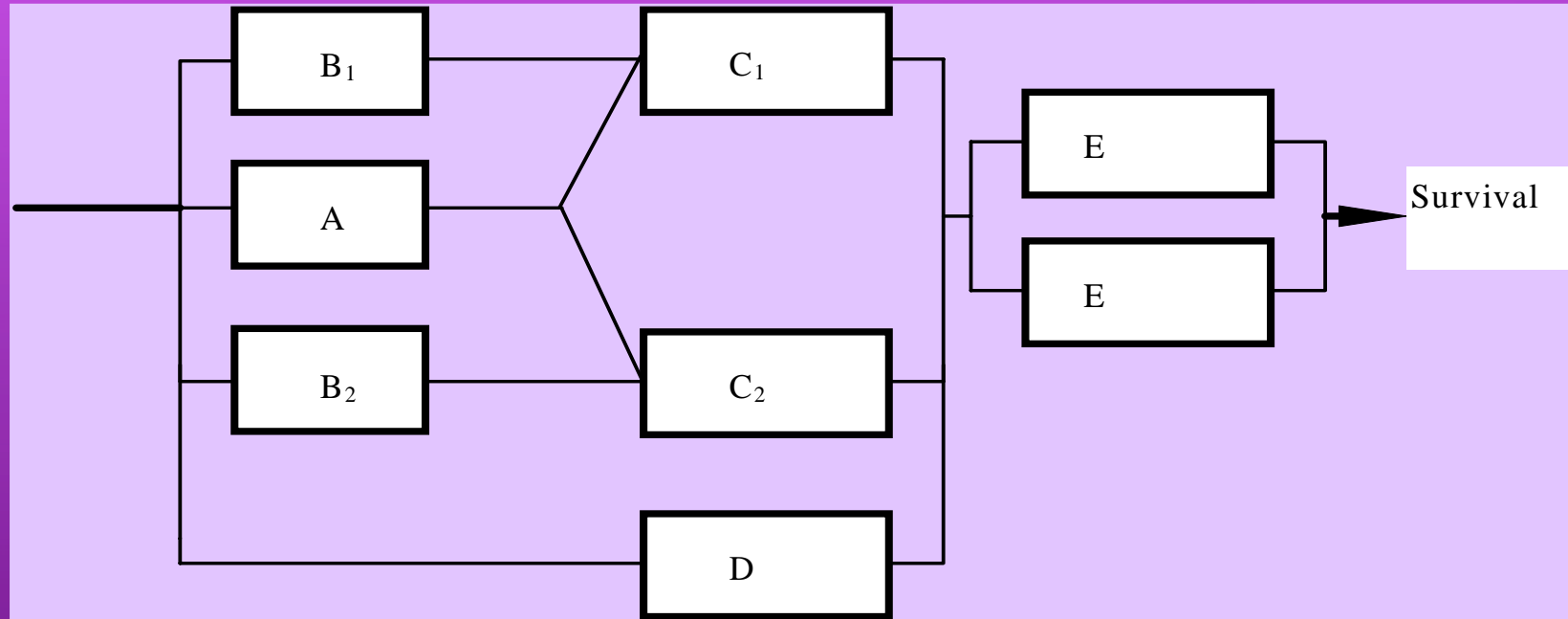
The probability of mission survival is:  $= 0.13572$



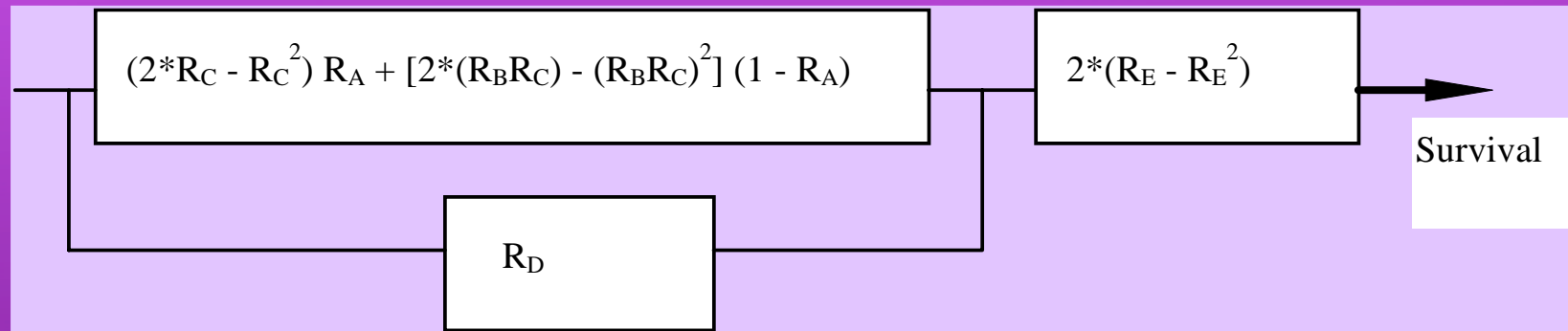
- The same procedure can be followed for any mission success diagram



## A complex example:



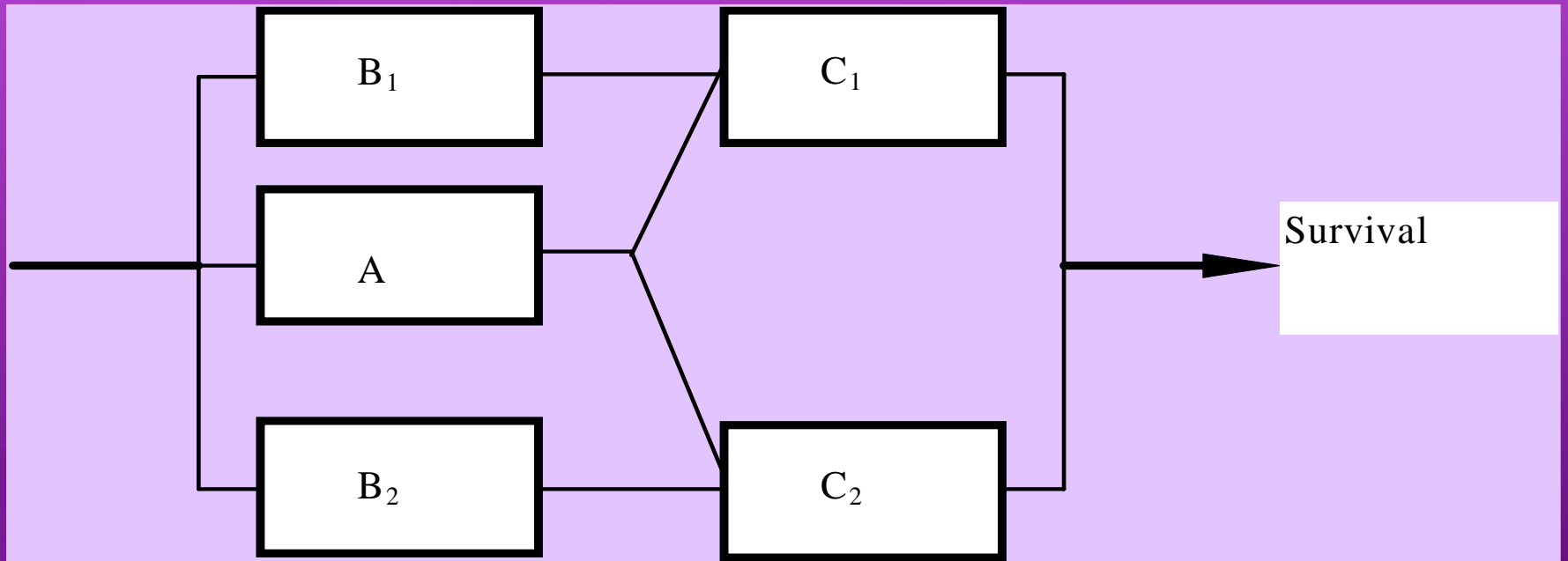
simplify:



## Method 2, Boolean Truth Table Approach:



Same model as before:



The Boolean approach lists all equipments of the system in a truth table:

Entry No	B <sub>1</sub>	B <sub>2</sub>	C <sub>1</sub>	C <sub>2</sub>	A	Success/ Failure	P <sub>s</sub>
1	0	0	0	0	0	F	0
2	0	0	0	0	1	F	0
3	0	0	0	1	0	F	0
4	0	0	0	1	1	S	0.03888
5	0	0	1	0	0	F	0
6	0	0	1	0	1	S	0.03888
7	0	0	1	1	0	F	0
8	0	0	1	1	1	S	0.00972
9	0	1	0	0	0	F	0
10	0	1	0	0	1	F	0
11	0	1	0	1	0	S	0.01008
12	0	1	0	1	1	S	0.004432
13	0	1	1	0	0	F	0
14	0	1	1	0	1	S	0.00432
15	0	1	1	1	0	S	0.00252
16	0	1	1	1	1	S	0.00108
17	1	0	0	0	0	F	0
18	1	0	0	0	1	F	0
19	1	0	0	1	0	F	0
20	1	0	0	1	1	S	0.00432
21	1	0	1	0	0	S	0.01008
22	1	0	1	0	1	S	0.00432
23	1	0	1	1	0	S	0.00252
24	1	0	1	1	1	S	0.00108
25	1	1	0	0	0	F	0
26	1	1	0	0	1	F	0
27	1	1	0	1	0	S	0.00112
28	1	1	0	1	1	S	0.00048
29	1	1	1	0	0	S	0.00112
30	1	1	1	0	1	S	0.00048
31	1	1	1	1	0	S	0.00028
32	1	1	1	1	1	S	0.00012

Σ All mission success paths = 0.13572

## The table:

- The table has  $2^n$  entries.
- The table has a 0 or 1 entry in each column indicating failure or functional respectively for each equipment.
- All possible combinations of all equipments functioning and failing are thus listed.

- From the table it is evident that nineteen of the 32 combinations result in a successful mission. The first is entry number 4 and the Probability of mission success,  $P_S$  for this case is:

$$(1 - R_{B1}) (1 - R_{B2}) (1 - R_{C1}) R_{C2} R_A$$

## Values from earlier:

If we use values from the earlier example:

$$R_A = 0.3,$$

$$R_{B1} = R_{B2} = 0.1,$$

$$R_{C1} = R_{B2} = 0.2$$

and therefore,

$$(1 - R_A) = 0.7,$$

$$(1 - R_B) = 0.9,$$

$$(1 - R_C) = 0.8$$

$$P_S = 0.9 * 0.9 * 0.8 * 0.2 * 0.3 = 0.03888$$

This number is then entered in the column  $P_S$  against entry number 4.

## For each success case:

- The process is repeated for each success case and the table completed. By summing all the success probabilities in the  $P_S$  column the total probability of mission survival is obtained as 0.13572 in this example.



# The Mission success equation:

$$\begin{aligned}
 P_S = & \bar{R}_{B1} \bar{R}_{B2} \bar{R}_{C1} R_{C2} R_A + \bar{R}_{B1} \bar{R}_{B2} R_{C1} \bar{R}_{C2} R_A + \bar{R}_{B1} \bar{R}_{B2} R_{C1} R_{C2} \bar{R}_A \\
 & + \bar{R}_{B1} R_{B2} \bar{R}_{C1} R_{C2} \bar{R}_A + \bar{R}_{B1} R_{B2} \bar{R}_{C1} R_{C2} R_A + \bar{R}_{B1} R_{B2} R_{C1} \bar{R}_{C2} R_A \\
 & + \bar{R}_{B1} R_{B2} R_{C1} R_{C2} \bar{R}_A + \bar{R}_{B1} R_{B2} R_{C1} R_{C2} R_A + R_{B1} \bar{R}_{B2} \bar{R}_{C1} R_{C2} R_A \\
 & + R_{B1} \bar{R}_{B2} R_{C1} \bar{R}_{C2} \bar{R}_A + R_{B1} \bar{R}_{B2} R_{C1} \bar{R}_{C2} R_A + R_{B1} \bar{R}_{B2} R_{C1} R_{C2} \bar{R}_A \\
 & + R_{B1} \bar{R}_{B2} R_{C1} R_{C2} R_A + R_{B1} R_{B2} \bar{R}_{C1} R_{C2} \bar{R}_A + R_{B1} R_{B2} \bar{R}_{C1} R_{C2} R_A \\
 & + R_{B1} R_{B2} R_{C1} \bar{R}_{C2} R_A + R_{B1} R_{B2} R_{C1} \bar{R}_{C2} R_A + R_{B1} R_{B2} R_{C1} R_{C2} \bar{R}_A \\
 & + R_{B1} R_{B2} R_{C1} R_{C2} R_A
 \end{aligned}$$

## Reduction:

- By a reduction technique attributed to Thomas Case the equation reduces to:

$$P_S = R_{B1}R_{C1} + \bar{R}_{B1}R_{B2}R_{C2} + R_A\bar{R}_{B1}\bar{R}_{B2}R_{C2} \\ + R_A\bar{R}_{B1}R_{C1}\bar{R}_{C2} + R_{B1}R_{B2}\bar{R}_{C1}R_{C2} + R_{B1}\bar{R}_{B2}\bar{R}_{C1}R_{C2}R_A$$

**THE END**

**FOR THE TIME BEING!**



*Sentient systems*