



Y POLITECNICO DI MILANO





Prof. Enrico Zio

Politecnico di Milano Dipartimento di Energia



Fault Tree Analysis (FTA)

- Systematic and quantitative
- Deductive

AIM:

- 1. Decompose the system failure in elementary failure events of constituent components
- 2. Computation of system failure probability, from component failure probabilities







1. Define top event (system failure)

Electric power generation system



E1, E2 = engines

G1, G2, G3 = generators, each one is rated at 30 KVA

T = Failure to supply at least 60 kVA

- 1. Define top event (system failure)
- 2. Decompose top event by identifying subevents which can cause it.

At least two out of the three generators do not work



- 1. Define top event (system failure)
- 2. Decompose top event by identifying subevents which can cause it
- 3. Decompose each subevent in more elementary subevents which can cause it





- 1. Define top event (system failure)
- 2. Decompose top event by identifying subevents which can cause it
- 3. Decompose each subevent in more elementary subevents which can cause it
- 4. Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event



- 1. Define top event (system failure)
- 2. Decompose top event by identifying subevents which can cause it
- 3. Decompose each subevent in more elementary subevents which can cause it
- 4. Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event





FT event symbols



FT gate symbols

)	AND gate	Output event occurs if all input events occur simultaneously.
	OR gate	Output event occurs if any one of the input events occurs.
<u>}</u>	Inhibit gate	Input produces output when conditional event occurs.

FT gate symbols

	Priority AND Gate	Output event occurs if all input events occur in the order from left to right
	Exclusive OR Gate	Output event occurs if one, but not both, of the input events occur.
m m n input	m out of n gate (volume or sample gate)	Output event occurs if m out of n input events occur.

FT Example 1: Electric Power Generation System



Fault tree?

Prof. Enrico Zio

FT Example 2: The Shutdown System



Prof. Enrico Zio

FT Example 3: The System of Systems



Internal emergency devices:

- Power system
 Diesel Generator (DG)
- Water system
 Pipe (Pi)
 Pump (Pu)
 Pool

Interdependent CIs:

- Power system

 Generation Station (GS)
 Substation (S)
 Pole (Po)
- Water system Pipe (Pi) Pump (Pu) River
- Road transportation system Road access (R)

- Power line
- Road access

Generators (G1, G2, G3) Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14) Power delivery paths: lines (L) and buses (B).



FT Example 4: IEEE14 Bus Power Distribution System

Draw a Fault Tree (FT) for the top event "failure to supply power to bus 2" (Load2)

FT Example 4: IEEE14 Bus Power Distribution System

Draw a Fault Tree (FT) for the top event "failure to supply power to bus 4" (Load4)

FT qualitative analysis

Prof. Enrico Zio

FT qualitative analysis

Introducing:

X_i: binomial indicator variable of i-th component state (basic event)



FT = set of boolean algebraic equations (one for each gate) => structure (switching) function $\vec{\Phi}$:

$$\mathbf{X}_{\mathsf{T}} = \boldsymbol{\Phi} \left(\mathbf{X}_{\mathsf{1}}, \mathbf{X}_{\mathsf{2}}, \dots, \mathbf{X}_{\mathsf{n}} \right)$$

Fundamental Products

FT = set of boolean algebraic equations (one for each gate) => structure (switching) function *Φ*:

$$X_{T} = \Phi(X_{1}, X_{2}, ..., X_{n})$$

An important theorem states that a structure function can be written uniquely as the union of the fundamental products which correspond to the combinations of the variables which render the function true. This is called the canonical expansion or disjunctive normal form of Φ .

Fundamental Laws

- 1) Commutative Law:
 - (a) XY = YX
 - (b) X + Y = Y + X
- 2) Associative Law
 - (a) X(YZ) = (XY)Z
 - (b) X + (Y + Z) = (X + Y) + Z
- 3) Idempotent Law
 - (a) XX = X
 - (b) X + X = X
- 4) Absorption Law
 - (a) X(X + Y) = X
 - (b) X + XY = X

- 5) Distributive Law
 - (a) X(Y+Z) = XY + XZ
 - (b) (X+Y)(X+Z) = X + YZ
- 6) Complementation* (a) $X\overline{X} = \emptyset$ (b) $X + \overline{X} = \Omega$ (c) $\overline{\overline{X}} = X$
- 7) Unnamed relationships but frequently useful (a) $X + \overline{X}Y = X + Y$
 - (b) $\overline{X}(X+Y) = \overline{X}\overline{Y}$



Prof. Enrico Zio

Coherent structure functions

A physical system would be quite unusual (or perhaps poorly designed) if improving the performance of a component (that is, replacing a failed component by a functioning one) caused the system to change from the success to the failed state.

Thus, we restrict consideration to structure functions that are monotonically increasing in each input variable. These structure functions do not contain complemented variables; they are called *coherent* and can always be expressed as the union of fundamental products.

The main properties of a coherent structure function are:

- 1. $\Phi(\underline{1}) = 1$ if all the components are in their success state, the system is successful;
- 2. $\Phi(\underline{0}) = 0$ if all the components are failed, the system is failed;
- 3. $\Phi(\underline{X}) \ge \Phi(\underline{Y})$ for $\underline{X} \ge \underline{Y}$

FT qualitative analysis

Coherent structure functions can be expressed in reduced expressions in terms of minimal path or cut sets. A path set is a set \underline{X} such that $\Phi(\underline{X})=1$; a cut set is a set \underline{X} such that $\Phi(\underline{X})=0$. Physically, a path (cut) set is a set of components whose functioning (failure) ensures the functioning (failure) of the system.

- cut sets = logic combinations of primary events which render true the top event
- minimal cut sets = cut sets such that if one of the events is not verified, the top event is not verified

FT qualitative analysis

FT = set of boolean algebraic equations (one for each gate) => structure (switching) function Φ :

$$\mathbf{X}_{\mathsf{T}} = \boldsymbol{\Phi} \left(\mathbf{X}_{1}, \mathbf{X}_{2}, \dots, \mathbf{X}_{\mathsf{n}} \right)$$

Boolean algebra to solve FT equations

$$X_{T_{1}} = X_{A}X_{B} =$$

$$= (X_{E_{1}} + X_{G_{1}} - X_{E_{1}}X_{G_{1}})(X_{G_{2}} + X_{E_{1}}X_{E_{2}} - X_{E_{1}}X_{E_{2}}X_{G_{2}}) =$$

$$= X_{E_{1}}X_{G_{2}} + X_{E_{1}}X_{E_{2}} - X_{E_{1}}X_{E_{2}}X_{G_{2}} + X_{E_{1}}X_{E_{2}}X_{G_{1}} +$$

$$-X_{E_{1}}X_{E_{2}}X_{G_{1}}X_{G_{2}} - X_{E_{1}}X_{G_{1}}X_{G_{2}} - X_{E_{1}}X_{E_{2}}X_{G_{1}} + X_{E_{1}}X_{E_{2}}X_{G_{1}}X_{G_{2}} =$$

$$= X_{E_{1}}X_{G_{2}} + X_{E_{1}}X_{E_{2}} + X_{G_{1}}X_{G_{2}} - X_{E_{1}}X_{E_{2}}X_{G_{1}} + X_{E_{2}}X_{G_{2}} - X_{E_{1}}X_{G_{2}}X_{G_{2}} - X_{E_{1}}X_{G_{1}}X_{G_{2}} =$$

 E_1

 E_{2}

FT Example 1: mcs



 $X_{T_1} = X_{E_1} X_{G_2} + X_{E_1} X_{E_2} + X_{G_1} X_{G_2} - X_{E_1} X_{E_2} X_{G_2} - X_{E_1} X_{G_1} X_{G_2}$

$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2}] =$$

$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{E_1}X_{E_2}X_{E_1}X_{E_2}X_{E_1}X_{E_2} - X_{E_1}X_{E_2}X_{E_1}X_{E_2}X_{E_1}X_{E_2} - X_{E_1}X_{E_2}X_{E_1}X_{E_2} - X_{E_1}X_{E_2}X_{E_1}X_{E_2}X_{E_1}X_{E_2} - X_{E_1}X_{E_2}X_{E_1}X_{E_2} - X_{E_1}X_{E_$$

 $=1-[(1-X_{E_1}X_{G_2})(1-X_{E_1}X_{E_2})(1-X_{G_1}X_{G_2})]$



FT Example 2: The Shutdown System



Prof. Enrico Zio

FT Example 2: The Fault Tree





Generators (G1, G2, G3) Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14) Power delivery paths: lines (L) and buses (B).



FT Example 4: IEEE14 Bus Power Distribution System

Find the Mcs for the top event "failure to supply power to bus 2" (Load2)





- 1. mcs identify the component basic failure events which contribute to system failure
- 2. qualitative component criticality: those components appearing in low order mcs or in many mcs are most critical



FT quantitative analysis





FT quantitative analysis

Compute system failure probability from primary events probabilities by:

1. using the laws of probability theory at the fault tree gates

FT Example 2: The Shutdown System



FT Example 2: The Fault Tree







Compute system failure probability from primary events probabilities by:

1. using the laws of probability theory at the fault tree gates







FT quantitative analysis

Compute system failure probability from primary events probabilities by:

- 1. using the laws of probability theory at the fault tree gate
- 2. using the mcs found from the qualitative analysis

$$P[\Phi(\underline{X}) = 1] = \sum_{j=1}^{mcs} P[M_j] - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} P[M_iM_j] + \dots + (-1)^{mcs+1} P[\prod_{j=1}^{mcs} M_j]$$

It can be shown that:

$$\sum_{j=1}^{mcs} P[M_j] - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} P[M_i M_j] \le P[\Phi(\underline{X}) = 1] \le \sum_{j=1}^{mcs} P[M_j]$$

FT Example 2: The Shutdown System



Prof. Enrico Zio

FT Example 2: The Fault Tree





FT Example 2: mcs



FT Example 4: IEEE14 Bus Power Distribution System

```
Generators (G1, G2 , G3)
Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14)
Power delivery paths: lines (L) and buses (B).
```



FT Example 4: IEEE14 Bus Power Distribution System

Find the Mcs for the top event "failure to supply power to bus 2" (Load2) Compute the top event probability

FT: comments

- 1. Straightforward modelization via few, simple logic operators;
- 2. Focus on one top event of interest at a time;
- 3. Providing a graphical communication tool whose analysis is transparent;
- 4. Providing an insight into system behaviour;
- 5. Minimal cut sets are a synthetic result which identifies the critical components.

ETA+FTA

