## Fault tree analysis

Fault tree analysis (FTA) was developed in 1961 at Bell Telephone Laboratories to evaluate the Minuteman Launch Control System for an unauthorized missile launch [1]. FTAs are now widely used in the electronics, nuclear and aerospace industries.

FTA is a method for analyzing causes of hazards. FTAs use Boolean logic (gates) to describe combinations of individual faults than can create a hazardous event. Each level of the tree lists the lower level events that are necessary to cause the event shown in the level above it.

The tree is written as a Boolean expression to show the specific combination of identified basic events sufficient to cause the undesired top level event. If the individual probabilities for all the basic events are known (not feasible in most abstract cases), the frequency of the top event can be calculated.

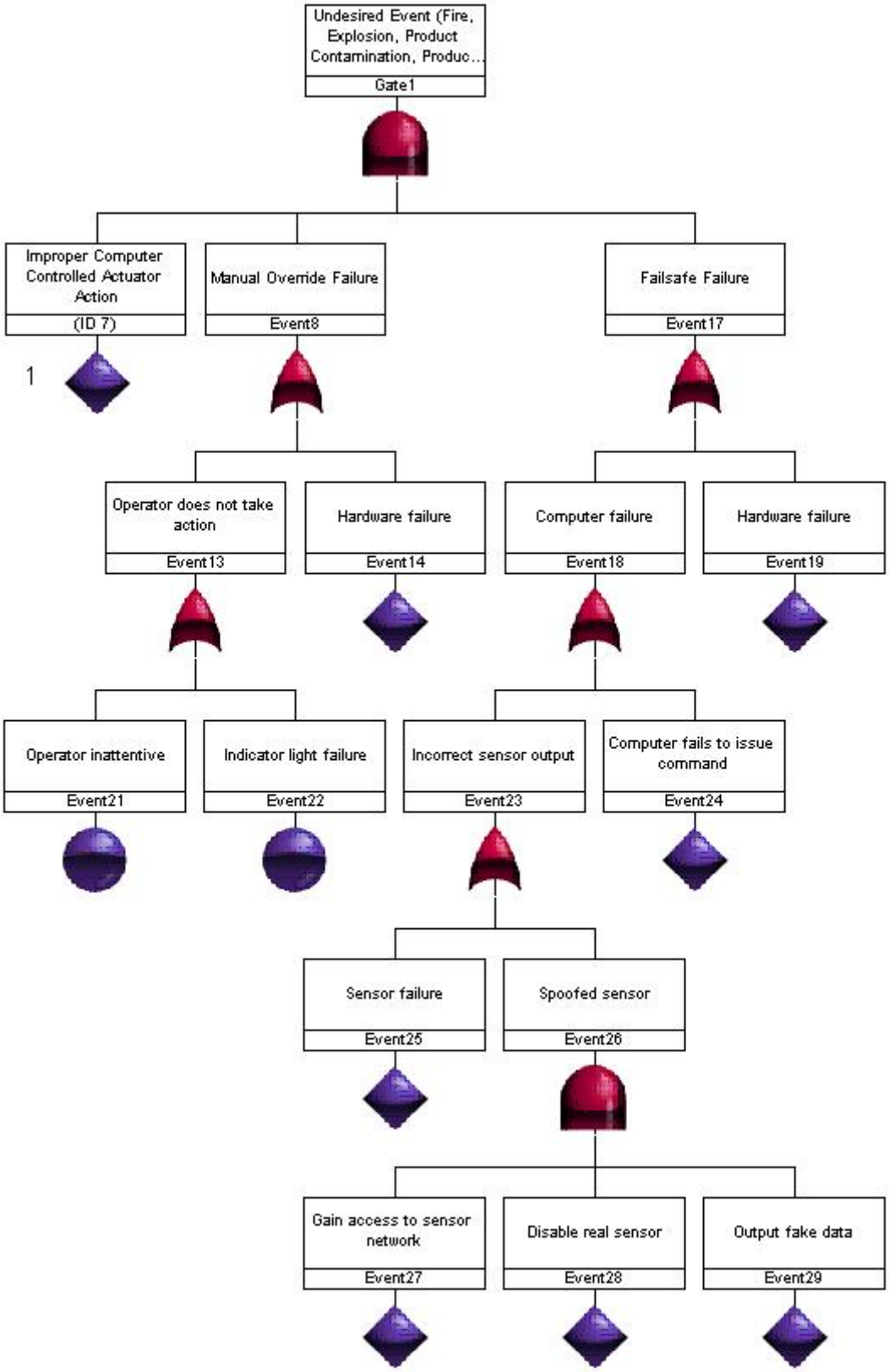
Often the most difficult part of creating a fault tree is the determination of the top level event. The selection of the top event is crucial since hazards in the system will not be comprehensive unless the fault trees are drawn for all significant top level events.

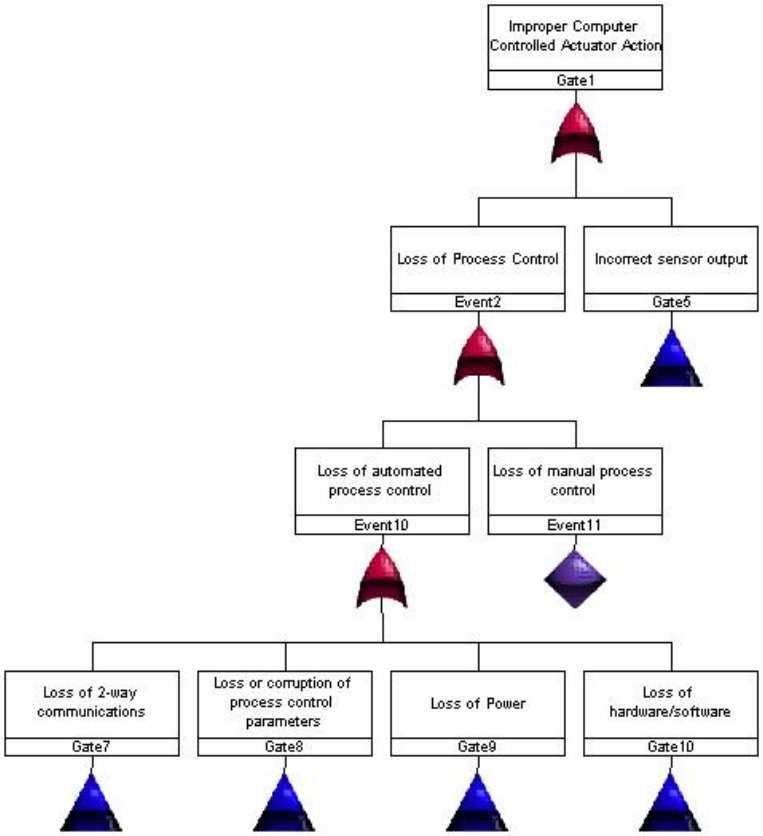
Once the top event has been defined, the next step is to determine the events related to the top event and the logical relations between them, using logic symbols to define the relations. The most frequently used symbols for fault trees are AND and OR gates. The output of an AND gate only exists if all the the input events exist (it represents combinations of events). The output of an OR gate exists provided at least one on the input events exist (it shows single events that can cause the output event). NAND and NOR gates are used primarily to define countermeasures that, if true, will allow the system to tolerate conditions that would otherwise result in safety hazards or machine failure.

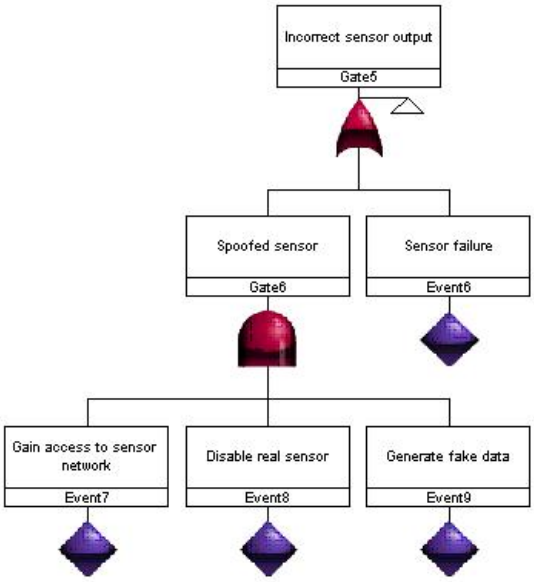
The relationships between the events shown in a fault tree are standard logical relations and can therefore be expressed using any form of Boolean algebra or truth table. The tree format, however, seems to have the advantage in readabilty.

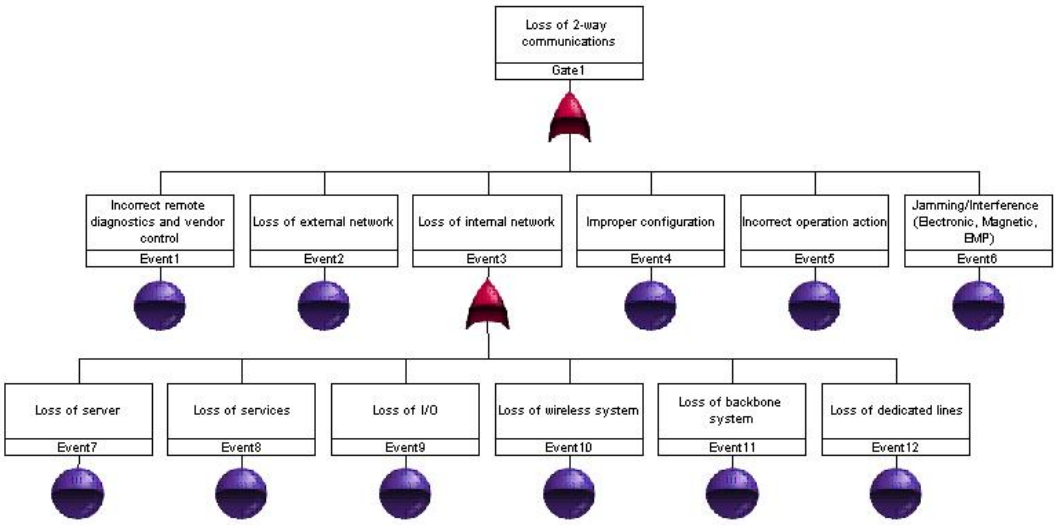
Although FTA was originally developed to calculate quantitative probabilities, it is more often used qualitatively. The graphical format provides a display of the relationships between the events and helps in understanding the system. Fault trees can help identify scenarios leading to hazards and can suggest possibilities for hazard elimination or control. This is how we are using FTA in Process Control Security.

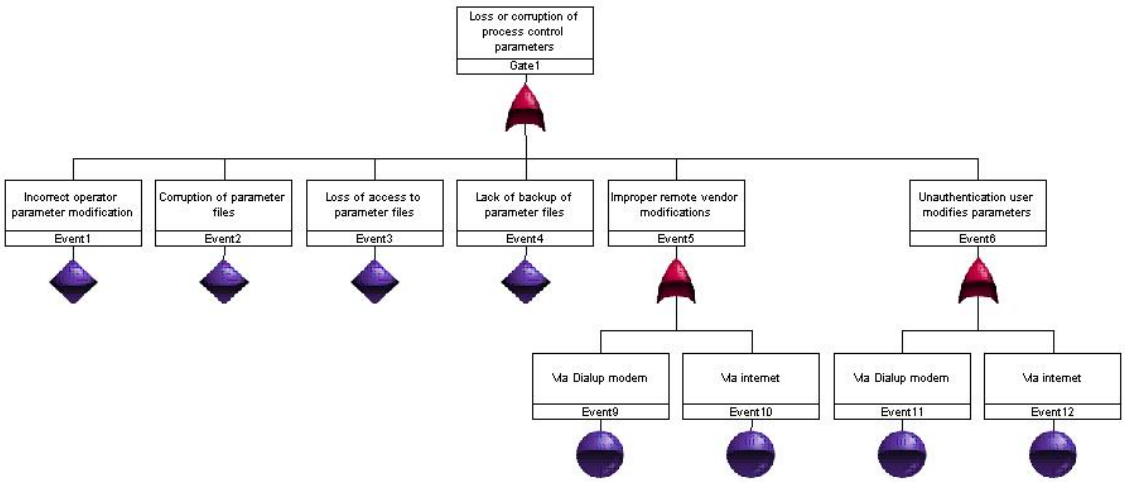
Figure 1 shows a general industrial Process Control Fault Tree. The top event in this fault tree is a list of the general undesirable events than can happen. These include: Fire, Explosion, Chemical Release, Product Contamination, Product Termination and Distribution Termination.

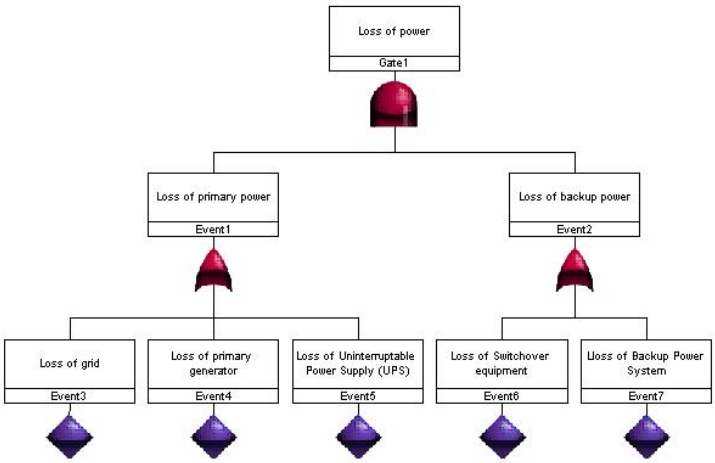

Undesired Event (Fire, Explosion, Product Contamination, Produc...
Gate1
Improper Computer Controlled Actuator Action
(ID 7)
1
Manual Override Failure
Event8
Failsafe Failure
Event17
Operator does not take action
Event13
Hardware failure
Event14
Computer failure
Event18
Hardware failure
Event19
Operator inattentive
Event21
Indicator light failure
Event22
Incorrect sensor output
Event23
Computer fails to issue command
Event24
Sensor failure
Event25
Spoofed sensor
Event26
Gain access to sensor network
Event27
Disable real sensor
Event28
Output fake data
Event29


Improper Computer Controlled Actuator Action
Gate1
Loss of Process Control
Event2
Incorrect sensor output
Gate5
Loss of automated process control
Event10
Loss of manual process control
Event11
Loss of 2-way communications
Gate7
Loss or corruption of process control parameters
Gate8
Loss of Power
Gate9
Loss of hardware/software
Gate10


Incorrect sensor output
Gate5
Spoofed sensor
Gate6
Sensor failure
Event6
Gain access to sensor network
Event7
Disable real sensor
Event8
Generate fake data
Event9


Loss of 2-way communications
Gate1
Incorrect remote diagnostics and vendor control
Event1
Loss of external network
Event2
Loss of internal network
Event3
Improper configuration
Event4
Incorrect operation action
Event5
Jamming/Interference (Electronic, Magnetic, EMP)
Event6
Loss of server
Event7
Loss of services
Event8
Loss of I/O
Event9
Loss of wireless system
Event10
Loss of backbone system
Event11
Loss of dedicated lines
Event12


Loss or corruption of process control parameters
Gate1
Incorrect operator parameter modification
Event1
Corruption of parameter files
Event2
Loss of access to parameter files
Event3
Lack of backup of parameter files
Event4
Improper remote vendor modifications
Event5
Unauthentication user modifies parameters
Event6
Via Dialup modem
Event9
Via internet
Event10
Via Dialup modem
Event11
Via internet
Event12


Loss of power
Gate1
Loss of primary power
Event1
Loss of backup power
Event2
Loss of grid
Event3
Loss of primary generator
Event4
Loss of Uninterruptable Power Supply (UPS)
Event5
Loss of Switchover equipment
Event6
Loss of Backup Power System
Event7