

- Threat Tree Analysis -
Electronic Access Control
for
Safety Systems
for
Boulder ASQ Section 1313

Ron Vidano, PhD, PE, CRE
Applied Energy Industries
Ron.Vidano@aei.com

26 May 2011

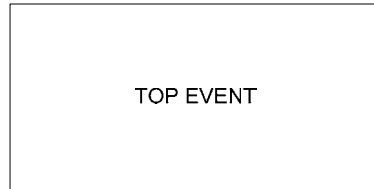
Overview

- Fault Tree Background and Principles
- Electronic Access Control for Security and Safety – Vulnerabilities and Threats
- Example of Fault Tree Analysis for Safety Threats

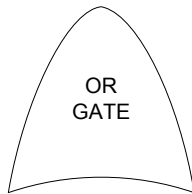
Fault Tree Background

- Fault tree analysis was developed for the US Air Force by Bell Labs
 - The technique was later adopted and applied by Boeing
 - Later, was used extensively within aerospace, nuclear power, and chemical industries
 - Today, TFA is used widely and is available within many popular reliability tools – Relex, Reliasoft, etc
- Fault tree analysis is appropriate when
 - High risk, threats of loss
 - Multi-element systems and processes
 - Already-identified undesirable events

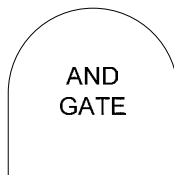
Logic Symbols



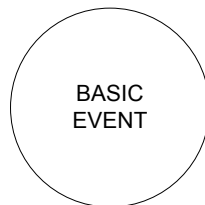
Top Event – Foreseeable, undesirable event for which all fault tree logic paths flow



OR Gate – Produces output if any input exists. Any individual input is necessary and sufficient to cause the output event



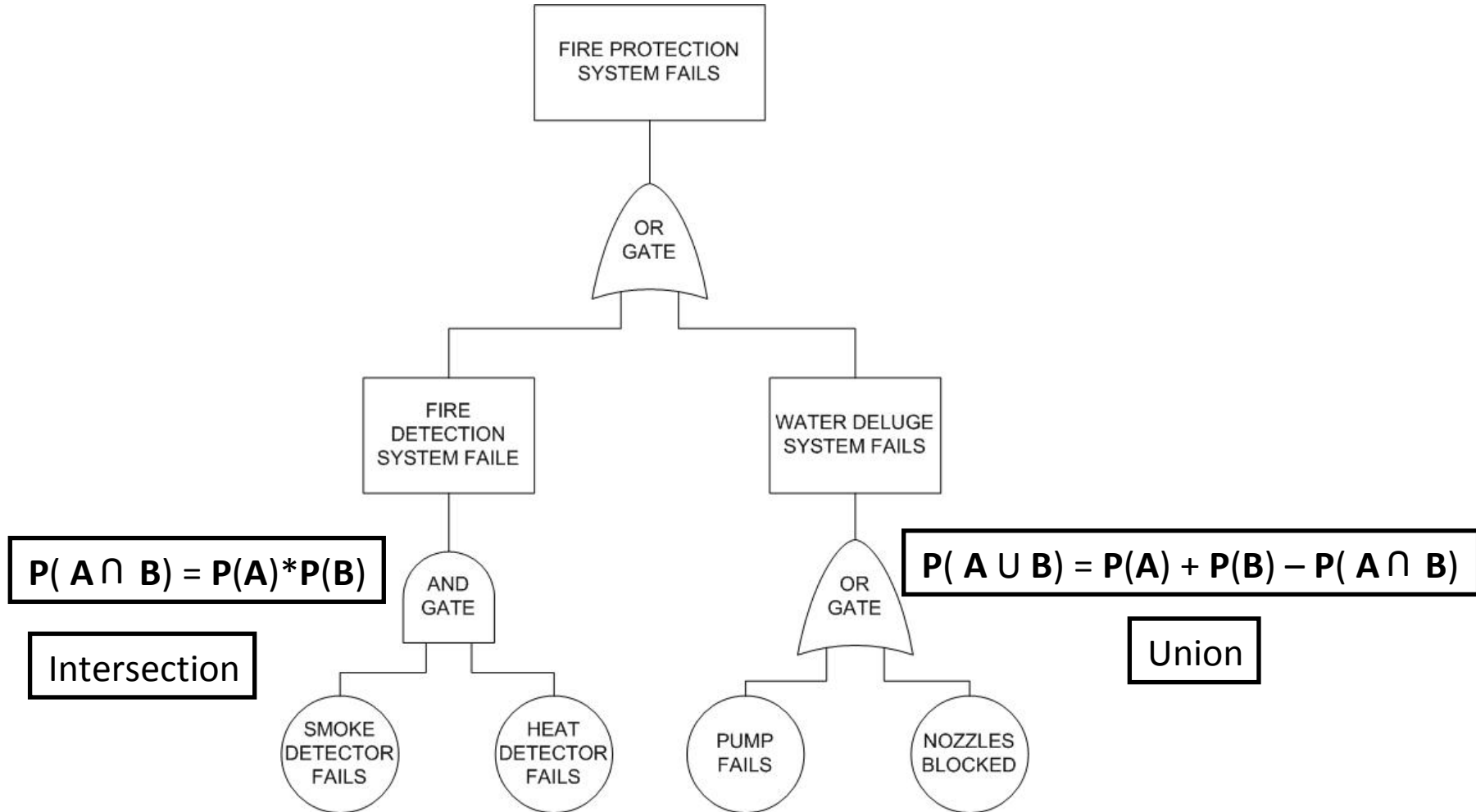
AND Gate – Produces output if all inputs co-exist. All inputs collectively must be necessary and sufficient to cause the output event



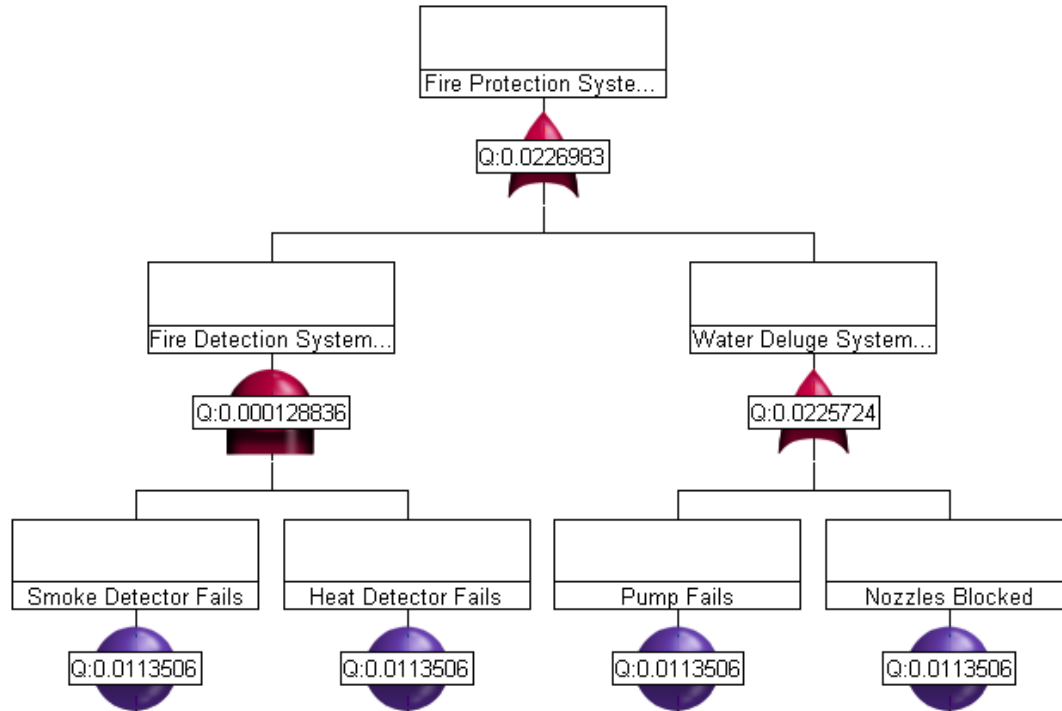
Basic Event – Initiating fault/failure

Events and gates are not component parts of the system – They are symbols representing the logic of the analysis

Simple Fault Tree Example



Probability Solution to Simple Fault Tree Example



View Calculation Results

Results for Gate: Fire Protection System Fails

Results at time 1000.00:
 Unavailability (Q): 0.02269926 Number of Failures: NA
 Unavailability (Q): 0.02269926 Frequency (F): 22.56417273

Time	Unavailability	Unreliability	Failure Frequency
0	0.000000	0.000000	22.632000
100.00	0.002282	0.002282	22.805661
200.00	0.004561	0.004561	22.779575
300.00	0.006838	0.006838	22.781143
400.00	0.009112	0.009112	22.726567
500.00	0.011383	0.011383	22.699948
600.00	0.013652	0.013652	22.672099
700.00	0.015918	0.015918	22.649990
800.00	0.018181	0.018181	22.618853
900.00	0.020441	0.020441	22.591581
1000.00	0.022699	0.022699	22.564173

Close Help

View Calculation Results

Results for Gate: Fire Protection System Fails

Results at time 1000.00:
 Unavailability (Q): 0.02269926 Number of Failures: NA
 Unavailability (Q): 0.02269926 Frequency (F): 22.56417273

Time	Unavailability	Unreliability	Failure Frequency
0	0.000000	0.000000	22.632000
1000.00	0.022699	0.022699	22.564173
8760.00	0.100691	0.100691	20.132466
17520.00	0.351718	0.351718	17.072909
26280.00	0.498070	0.498070	14.096307
35040.00	0.599625	0.599625	11.418780
43800.00	0.669092	0.669092	9.103134
52560.00	0.760136	0.760136	7.173294
61320.00	0.815912	0.815912	5.610526
70080.00	0.859209	0.859209	4.352079
78840.00	0.892924	0.892924	3.395268
87600.00	0.918781	0.918781	2.573663

Close Help

Example solved with Relx

FTA

Assume Component MTBF = 87600 hours (10 years)
 Component Failure Rate (λ) = 11.416 per million hours
 $P_f = 1 - \text{EXP}(-\lambda t)$
 Component $P_f = 0.01135$ (1000hrs); $P_f = 0.632$ (87600hrs);
 Top Event $P_f = 0.02269$; $P_f = 0.91875$ (87600hrs)
 Top Event Frequency Failure Rate= 22.564 per million hours
 for a 1000 hour mission time; Failure Rate = 2.573 per million hours for
 an 87600 mission time.

**NEXT – A DISCUSSION ABOUT ACCESS
CONTROL APPLIED TO SAFETY CRITICAL
FACILITIES**

Industrial Security & Safety Principles

Corporations – Universities – Government Facilities

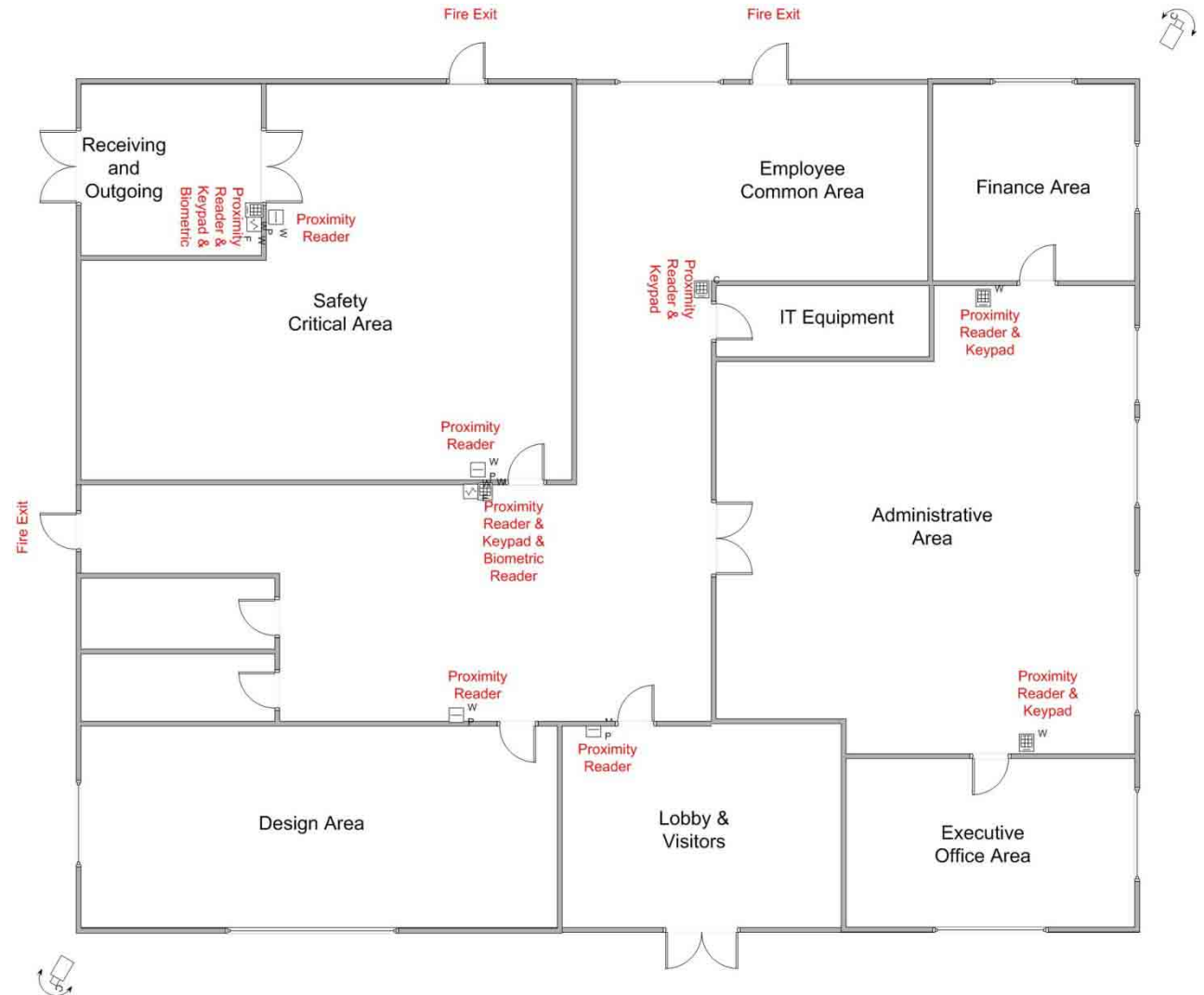
- **First Layer – Environmental**
 - Warning signs, fences, lighting, etc
- **Second Layer – Access Control**
 - Gates, doors, locks
 - Electronic Access Control (EAC) has become the dominant technology
- **Third Layer – Intrusion Detection**
 - Alarm systems
- **Fourth Layer – Video Monitoring**
 - Digital video recording with analytics is rapidly gaining acceptance

Technology is only part of the solution
The person is integrated into all of these layers

Example of Electronic Access Control

Multi-Purpose Safety Critical Facility

- Threat tree analysis is similar to fault tree methods to assess security risks
- Commonly used in Risk assessments for Probability and Severity
- Example vulnerabilities
 - Behavioral (Uncontrolled Processes)
 - Policy Misinterpretation (Poorly defined procedures)
 - Equipment or Software Problems
 - Physical (Theft, vandalism, fire)



Example - Access Control Zones

Authentication

- Single Factor – Something you have – Proximity Card
 - Building Entrance
 - Design Entrance
- Two Factor – Something you have, something you know – Proximity Card, PIN
 - Finance
 - Executive
 - IT Equipment
- Three Factor – Something you have, something you know, something you are – Proximity Card, PIN, Biometric
 - Safety Zone

Schedules – Employee, Time, Zone

- Building Entrance
 - 5/8: All Employees
 - 24/7: Certain Employees
- Design Entrance
 - 24/7: Certain Employees
- Finance, Executive, IT Equipment
 - 24/7: Certain Employees
- **Safety Zone Policy**
 - **Certified Trained Employees**
 - **Minimum Two Certified Trained Employees within Zone**
 - **Specified Time Schedules**

Example of One – Factor Authentication EAC

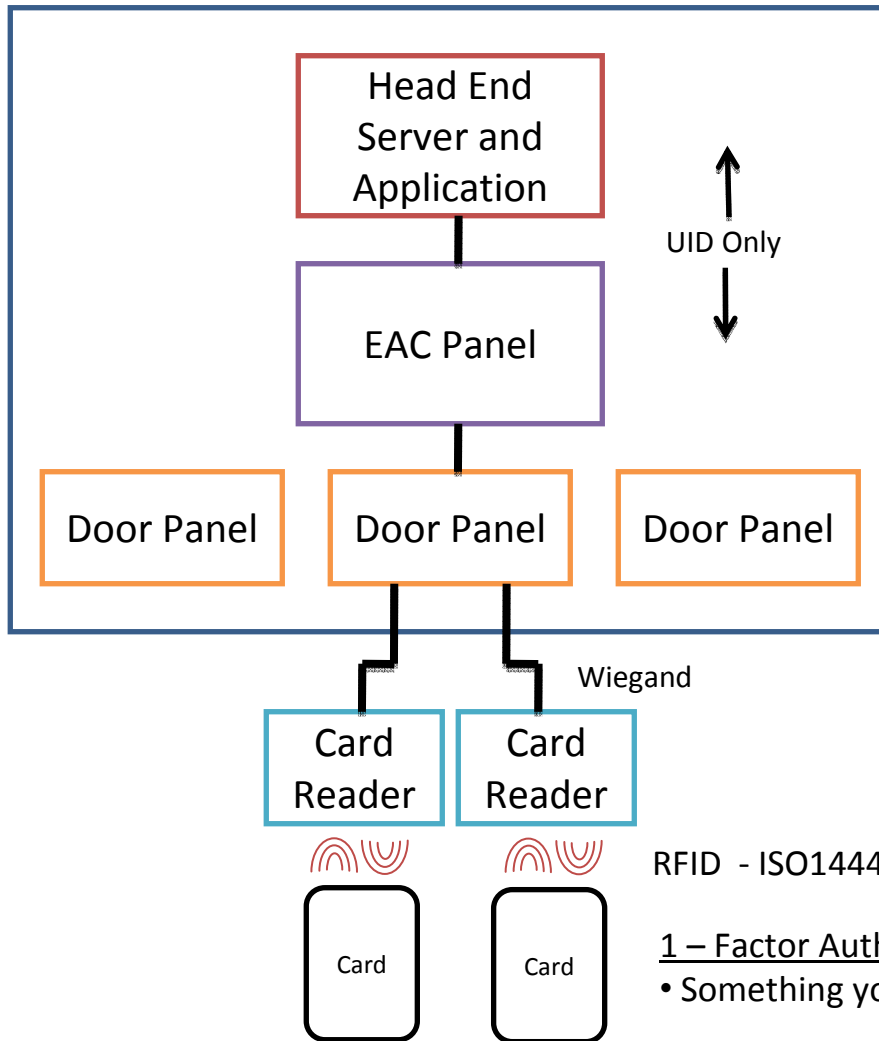
Common Problems with One-Factor EAC – Security Threats

- Piggybacking, tailgating
 - Following a legitimate user through a door.
- Levering the door open
- Lost cards – Delayed card termination

More sophisticated threats – Not necessarily more probable

- Identifier collisions
- Skimming & Sniffing
- Cloning

Therefore; Two and Three Factor Authentication EAC is used to reduce vulnerability to the threats; Particularly safety, intellectual property, and financial
(See next slide)

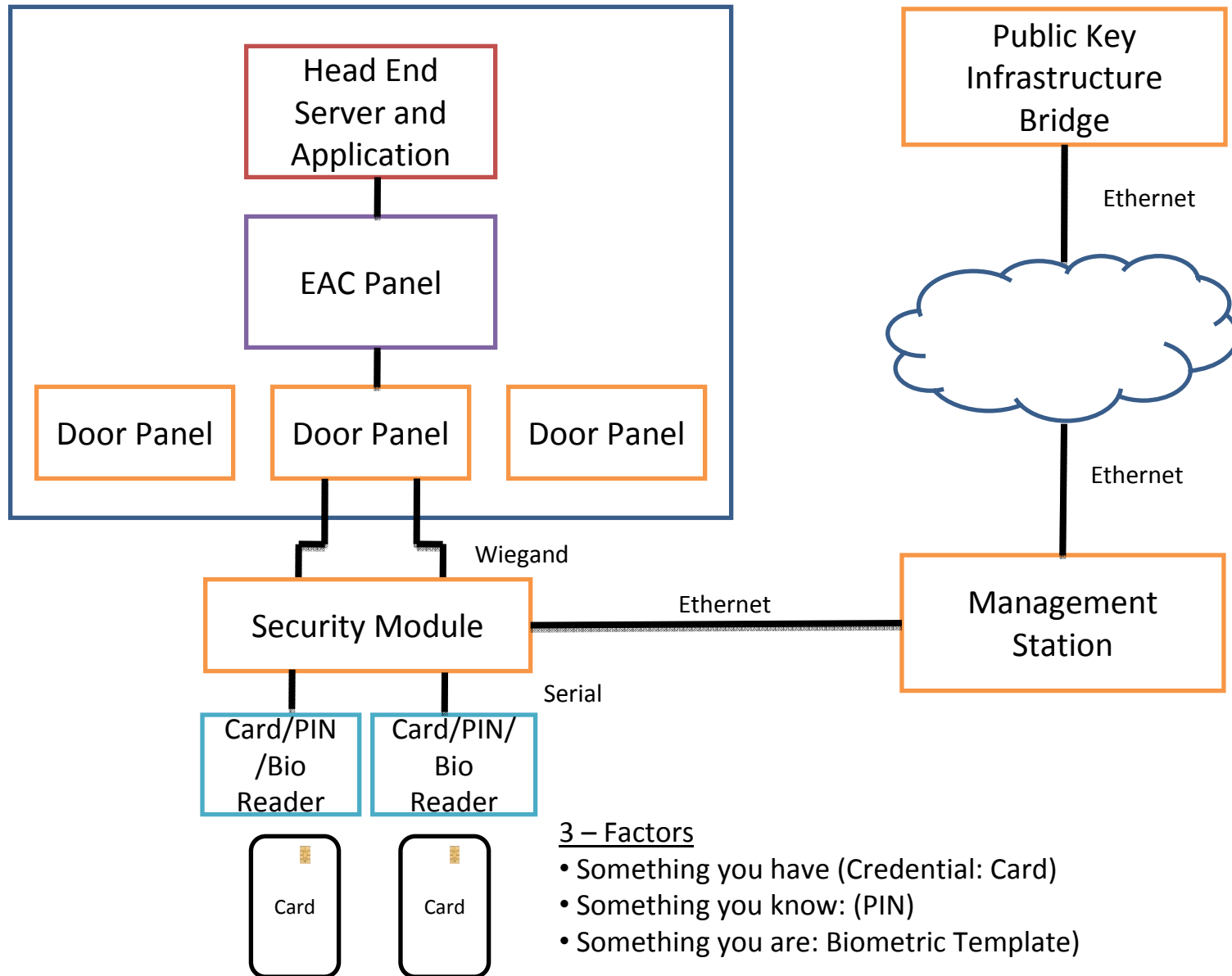


RFID - ISO14443A

1 – Factor Authentication

- Something you have

Example of Three – Factor Authentication EAC



**NEXT – A DISCUSSION ABOUT
COMPONENT PROBABILITIES
FOCUS UPON HUMAN FACTORS
AND
THREAT TO SAFETY**

Basic Event Reliability

- Electronic Failure Rates
 - Typical Overall EAC System Equipment; $\lambda = 4$ failures per million hours
- Human Error
 - General rate for errors involving high stress levels; Probability = 0.3
 - Operator fails to act correctly in the first 30 minutes of an emergency situation; Probability = 0.1
 - Carry out safety policy; Probability = 0.01
 - Error in a routine operation where care is required; Probability = 0.01
 - Human-performance limit: single operator; Probability = 0.0001
 - Human-performance limit: team of operators performing a well designed task; Probability = 0.00001

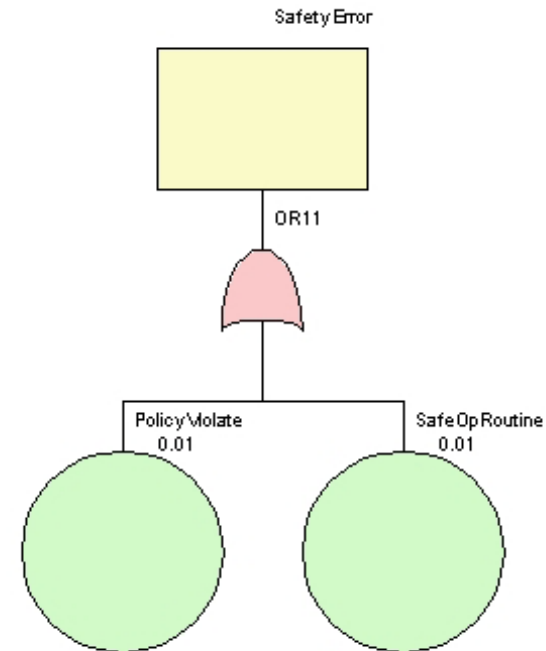
Simple Fault Tree – Safety Vulnerabilities and Threats

No Access Control System

Use Case:

- 1.No access control system in facility
- 2.Facility contains safety critical area
- 3.Policy is to have at least two trained personnel in the safety critical area
- 4.Probability of policy violation = 0.01
- 5.Probability of an error for a routine operation where care is required = 0.01

Probability of Safety Error = 0.0199



Example solved with OpenFTA

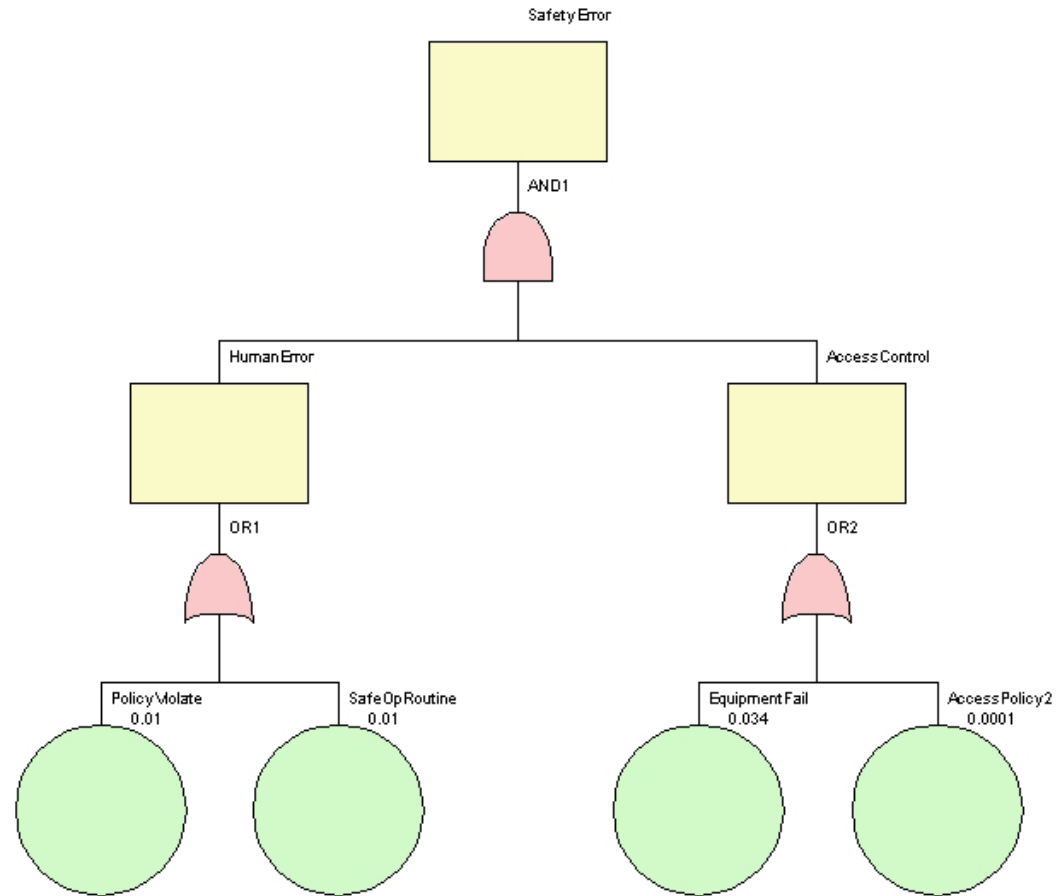
Simple Fault Tree – Safety Vulnerabilities and Threats

Three - Factor Access Control System

Use Case:

1. Two-Factor access control system in facility
2. Facility contains safety critical area
3. Policy is to have at least two trained personnel in the safety critical area
4. Probability of policy violation = 0.01
5. Probability of an error for a routine operation where care is required = 0.01
6. Probability of equipment malfunction during a year = 0.0034
7. Probability of an error for a team of operators performing well defined task = 0.0001

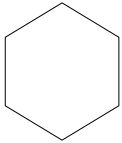
Probability of Safety Error = 0.000678



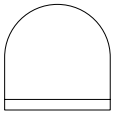
Conclusions

- Fault tree analysis forms a quantitative basis for vulnerability and threat analysis
- Electronic access control systems are a technical tool to enforce policies to provide for a safe work environment
- However; human factors are crucial

Other Logic Symbols



Inhibit Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In function. One input is a lower fault event and the other input is a conditional qualifier.



Ordered AND Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In function. Output occurs only if all inputs exist and the inputs occur in a specific order.

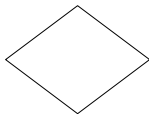


Exclusive OR Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In function. Output occurs when one, and only one, of the input events occur.

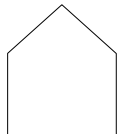


Voting OR Gate (m out of n): Output occurs when m out of n, of the input events occur.

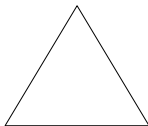
m:0:0



Undeveloped Event: Contains a failure at the lowest level of examination which can be expanded into a separate fault tree. The undeveloped event is used as an input to a logic gate.



Input Event: Contains a normal system operating input which has the capability of causing a fault to occur. The input event is used as an input to the logic gate.



Transfer Function: Signifies a connection between two or more selections of the fault tree to prevent duplicating sub-branches at multiple tree locations or to signify a location on a separate sheet of the same fault tree.



Conditioning Event: A specific condition or restriction than can apply to any logic gate.