Adversarial pathways and the use of bowties in a security world

Mel Davies
Risktec Solutions

TÜVRheinland®
Risktec

Safety and Security

- Safety and Security are now more closely linked why?

- Safety and security have a common purpose
  - *The protection of people, society and the environment.*

- The steps taken to provide protection against malicious acts incorporate specific features to ensure physical protection, but also rely on provisions that may have been installed for safety reasons.
  - *i.e a containment vessel protects against release and is made of steel and reinforced concrete which also provides an effective physical security barrier*

- **Safety evaluations focus** on risks arising from unintended events

- **Security evaluations focus** on the risks, or events, which arise from malicious acts carried out with intent.

Safety and Security

- What is a Adversarial Pathway analysis and why do we do it?

“An adversary path represents an ordered series of actions which, if undertaken completely successfully, execute an act of theft or sabotage”

From a Security perspective this considers a path taken by an adversary, their actions to overcome the Physical Protection Systems,

each action has a delay time, with a probability of detection which can occur at several locations along the path.

This assumes Physical Protection Systems are in place.

Physical Protection Systems enable the facility owners to prevent attacks through deterrence and to defeat the adversary (through, deter detect, delay and response)

What are the Targets?

- What is the target from a Safety perspective?
- These are the safety protection and control systems that are used to protect, prevent and mitigate against an unacceptable consequence. These incorporate all the components that constitutes the systems (Valves, pumps, pipes, instrumentation and controls systems, pressure vessels etc.)
  - Ie. they are attackable targets and are known as "Candidate Critical Assets"

- How does Security inform Safety?
- The security assessment may identify additional vulnerabilities of components within the plant. Designing out of such vulnerabilities may also have safety benefits, for example in consideration of internal hazards.

Adversary Pathway

- The following presents an example of a Bowtie used for an adversary pathway.

- It is a simplified illustrative tool.

- The examples shown do not incorporate aspects such as, which provide a greater depth of analysis:
  - probability of attack along a path
  - probability of interrupting the adversaries by the response force
  - probability of neutralization of the adversaries

- These aspects should be carried out using other analytical tools such as ASSESS, ATLAS etc

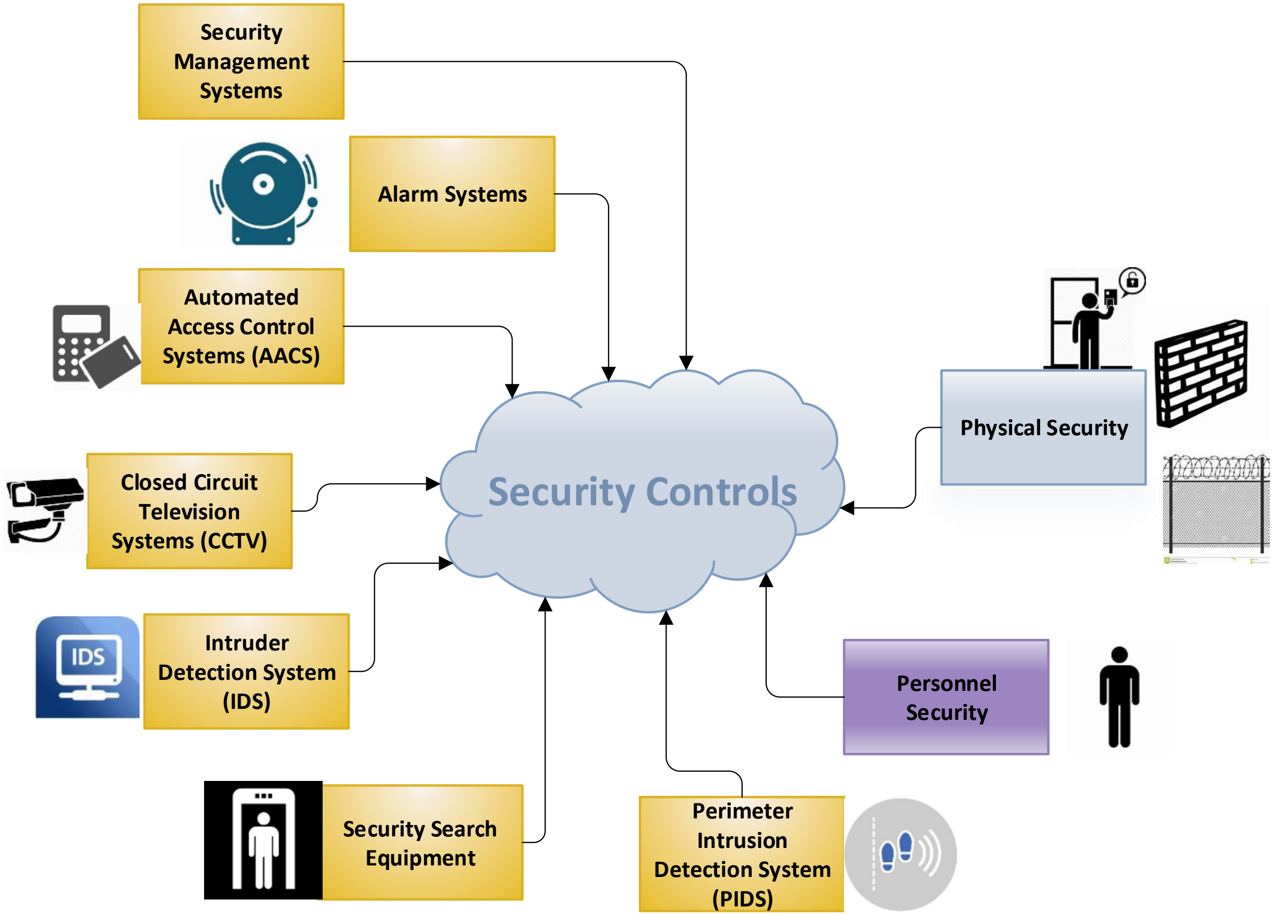
Adversary Pathway

- The Bowties presented will show:
  - Assumptions used
  - Representation of the pathway used through a building
  - Bowties diagrams showing:
    - Barriers
    - Delay Times
    - Additional Information
      - Type of Barrier
      - Control Posture
      - Barrier Quality
      - Area Zoning

- *Note: Due to the size of Bowtie that would represent the complete pathway the Bowties shown only display selected items*

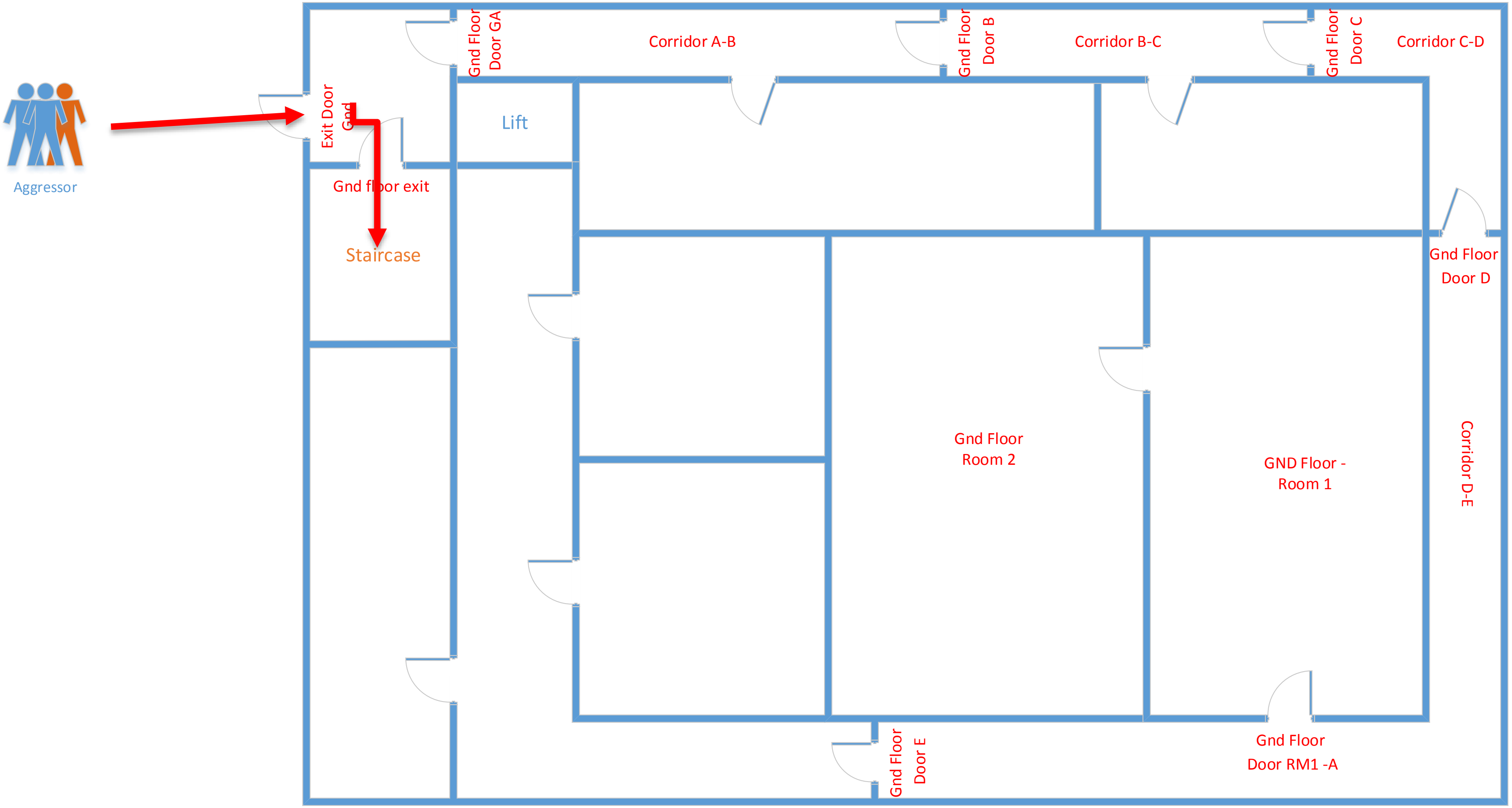
Assumptions

- Insider help available
- No Physical Protection Systems

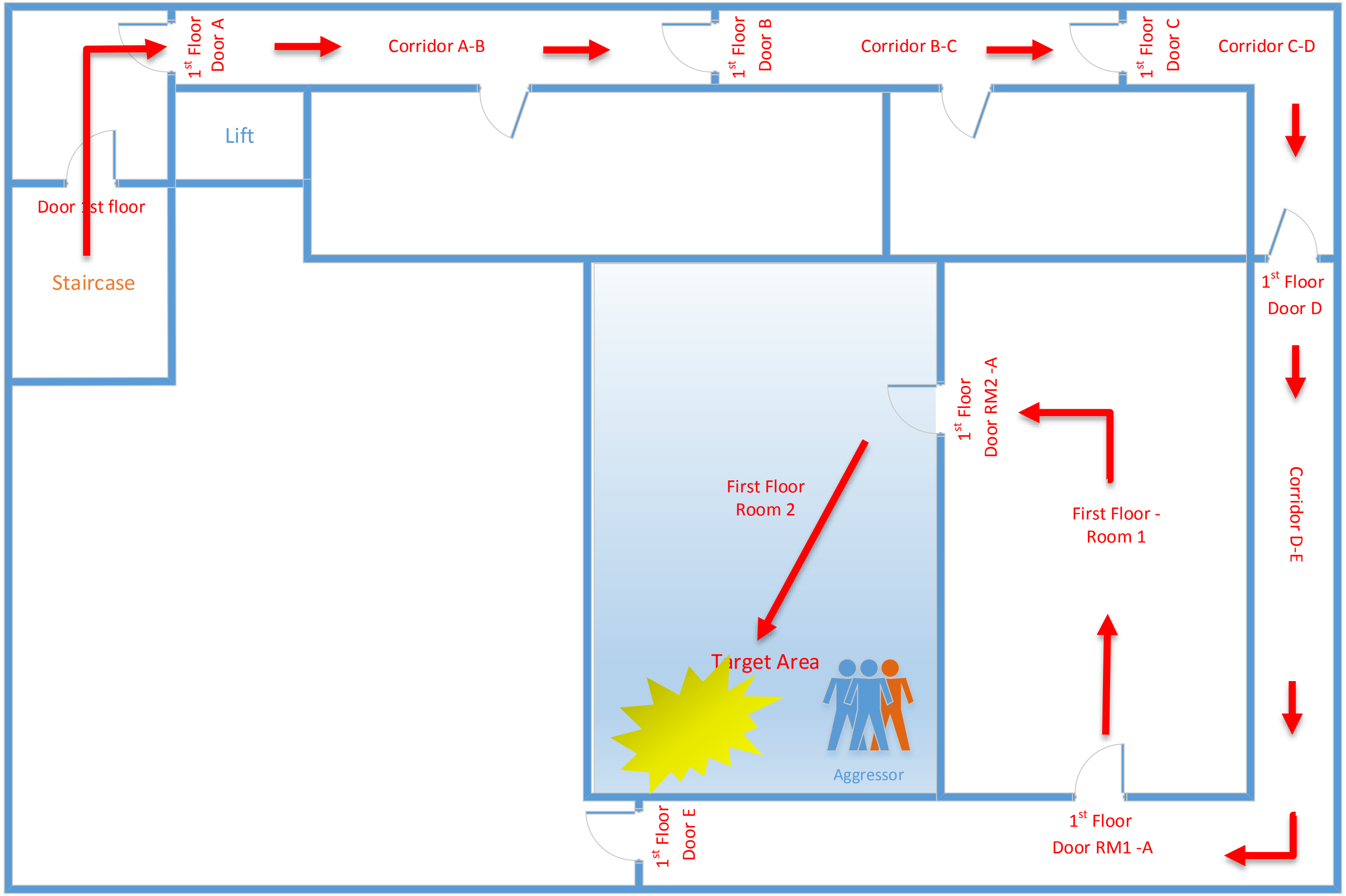

Security Management Systems
Alarm Systems
Automated Access Control Systems (AACS)
Closed Circuit Television Systems (CCTV)
Intruder Detection System (IDS)
IDS
Security Search Equipment
Perimeter Intrusion Detection System (PIDS)
Personnel Security
Physical Security
Security Controls

- Design Basis Threat – defines the resource and capability used to conduct the attacks

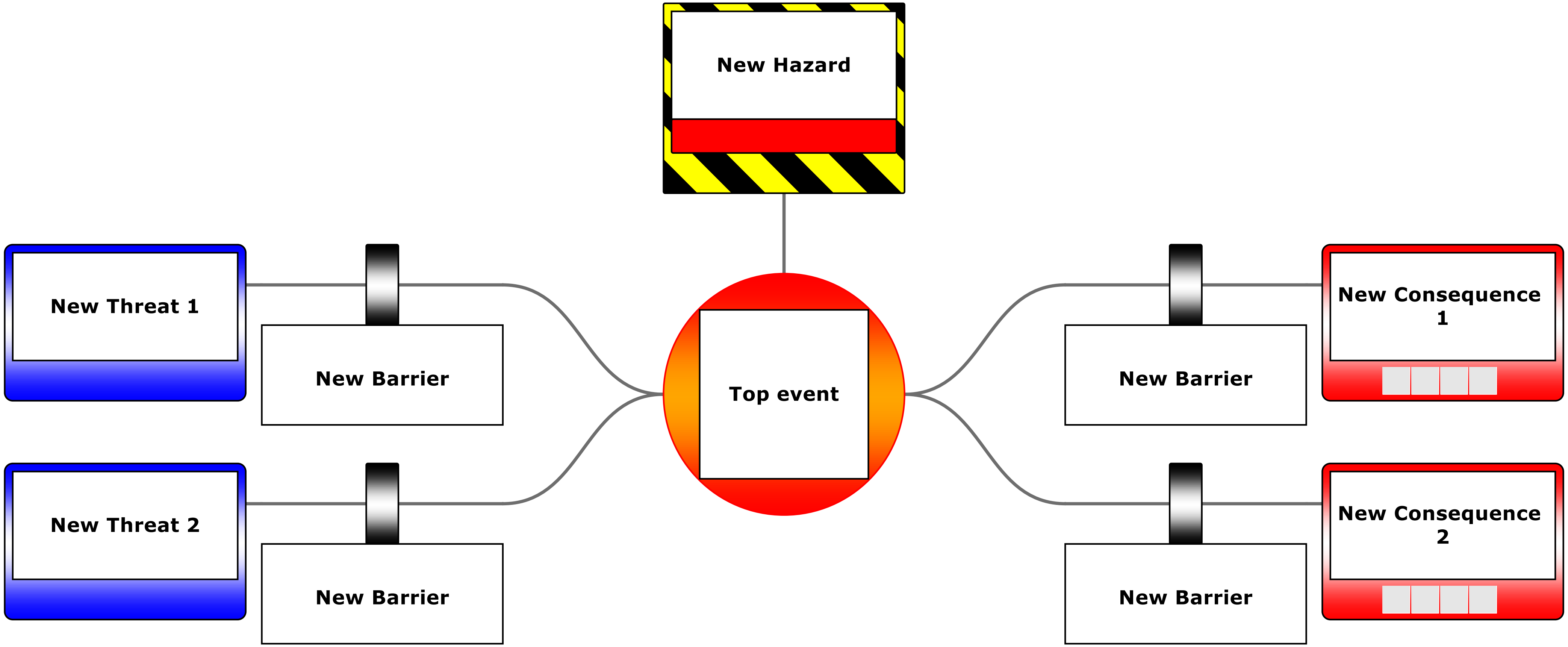
Adversary Pathway - Ground Floor



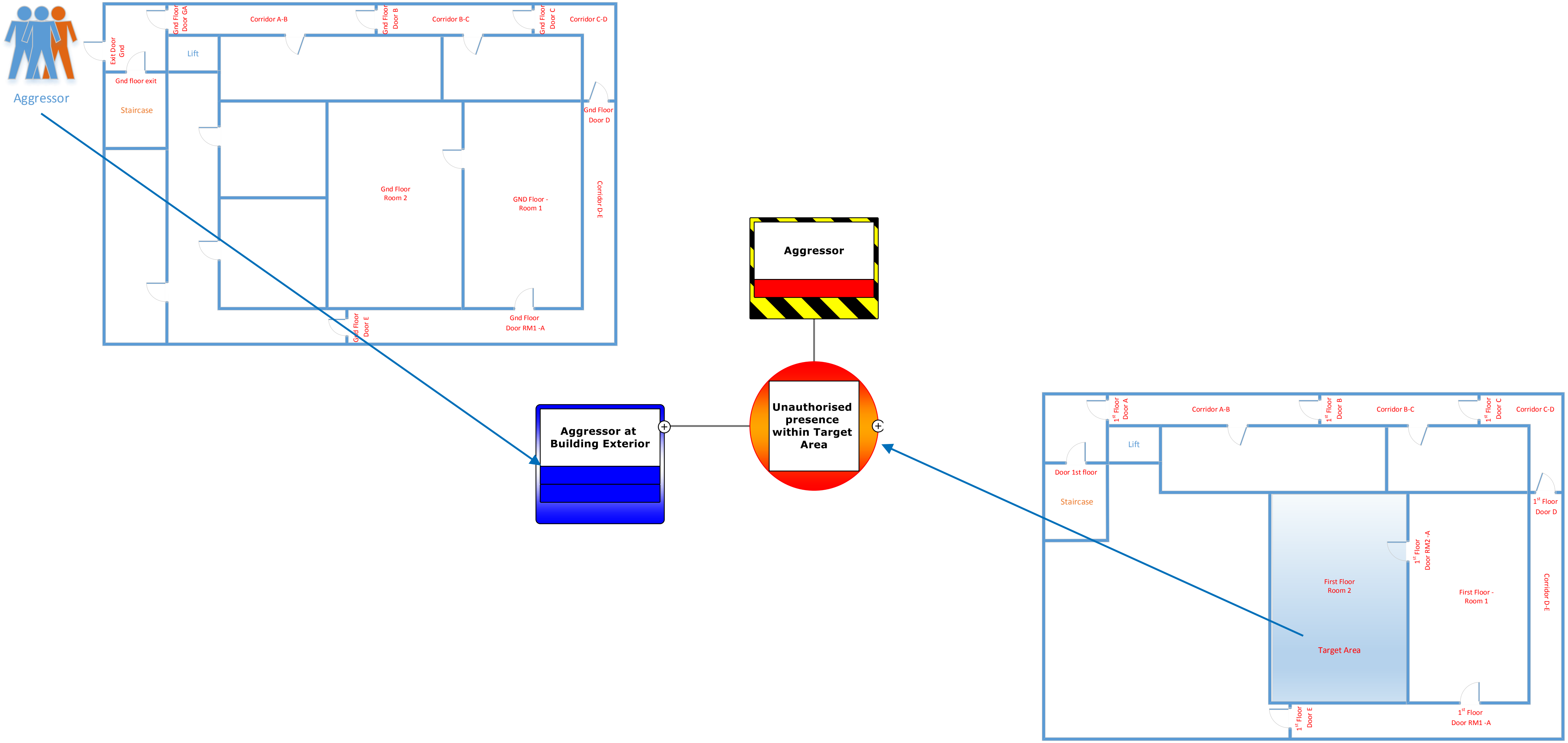
Adversary Pathway – 1st Floor



Quick overview of Bowtie



Bowtie –Adversary Pathway

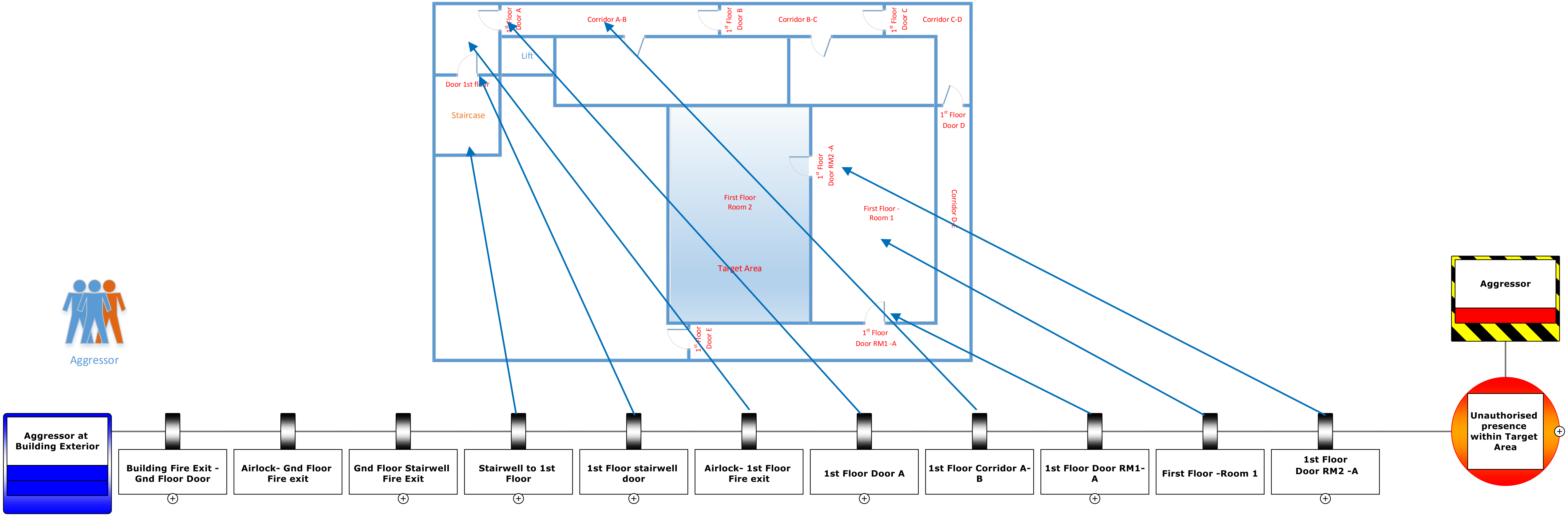


Aggressor

Aggressor at Building Exterior

Unauthorised presence within Target Area

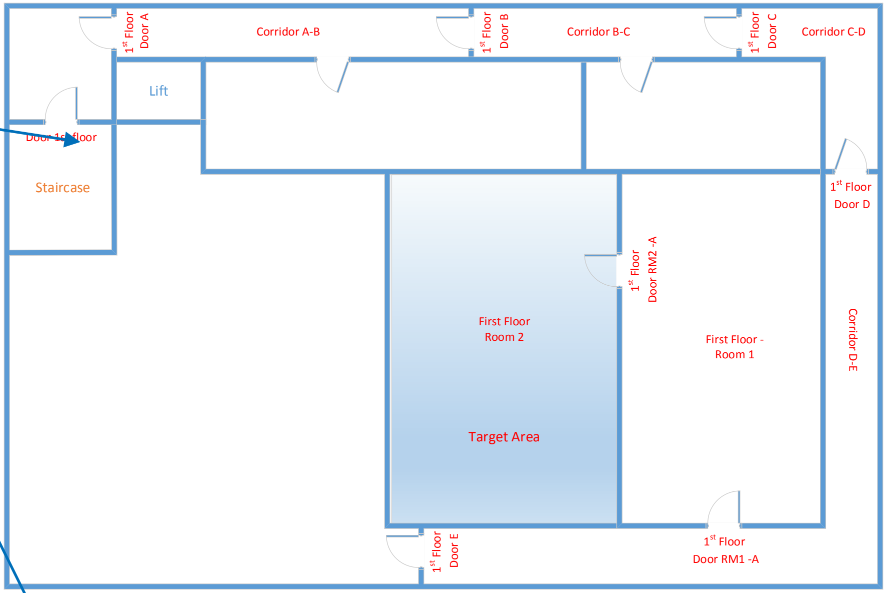
Bowtie –Adversary Pathway with building doors, corridors, rooms etc



- Each Door, Staircase, corridor is a barrier to the adversary in the pathway

Bowtie –Adversary Pathway delay times

- Each barrier has a delay time

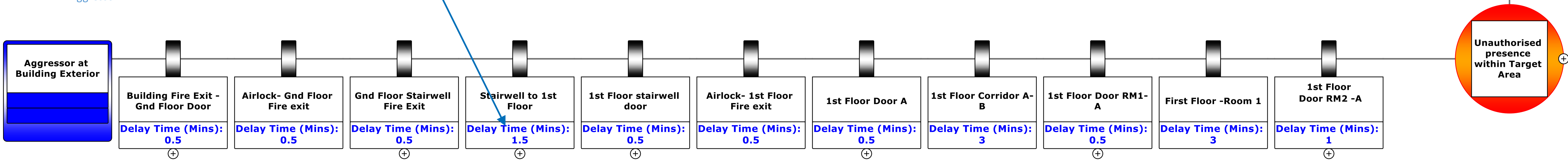


- Total time delay of all barriers

Aggressor

Aggressor

Overall Time value: 15



Aggressor at Building Exterior

Building Fire Exit - Gnd Floor Door	Airlock- Gnd Floor Fire exit	Gnd Floor Stairwell Fire Exit	Stairwell to 1st Floor	1st Floor stairwell door	Airlock- 1st Floor Fire exit	1st Floor Door A	1st Floor Corridor A-B	1st Floor Door RM1-A	First Floor -Room 1	1st Floor Door RM2 -A
Delay Time (Mins): 0.5	Delay Time (Mins): 0.5	Delay Time (Mins): 0.5	Delay Time (Mins): 1.5	Delay Time (Mins): 0.5	Delay Time (Mins): 0.5	Delay Time (Mins): 0.5	Delay Time (Mins): 3	Delay Time (Mins): 0.5	Delay Time (Mins): 3	Delay Time (Mins): 1

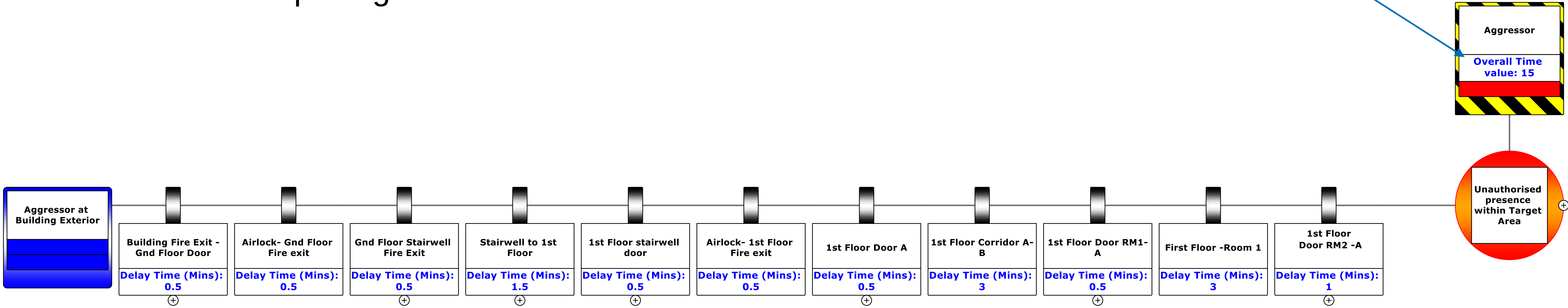
Unauthorised presence within Target Area

TÜVRheinland®
Risktec

Bowtie – Adversary Pathway response team time target

- This now provides the response time for any response team

- Delay time should be sufficient enough to allow for security personnel to respond in time to interrupt the adversary before completing their malevolent act



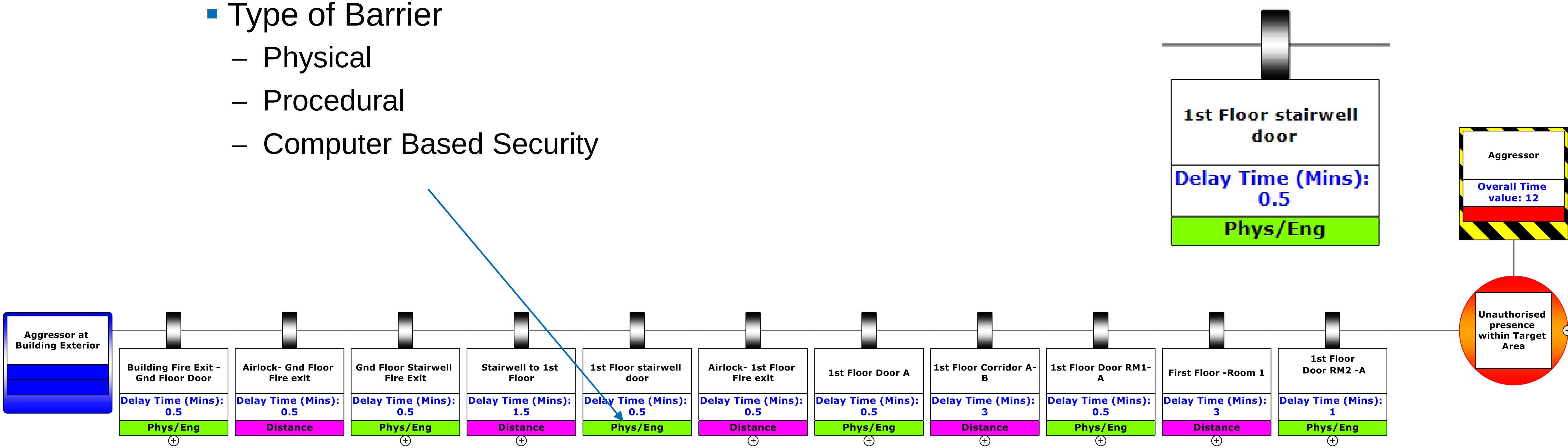
TÜVRheinland® Risktec

Delay Time Analysis?

- How can the response force response time be calculated?
  - Repeat the Bowtie for response force using their interception pathway. This will provide the response time and can be compared against the adversary pathway time to determine any differentials.
- Can multiply parallel pathways be calculated ?
  - Where multiple parallel pathways are used by a number of adversaries these can be modelled in a single Bowtie and each pathway delay time calculated.

Bowtie – Adversary Pathway additional Information

- Additional information can be added
- Type of Barrier
  - Physical
  - Procedural
  - Computer Based Security



1st Floor stairwell door
Delay Time (Mins): 0.5
Phys/Eng

Aggressor
Overall Time value: 12

Aggressor at Building Exterior

Building Fire Exit - Gnd Floor Door
Delay Time (Mins): 0.5
Phys/Eng

Airlock- Gnd Floor Fire exit
Delay Time (Mins): 0.5
Distance

Gnd Floor Stairwell Fire Exit
Delay Time (Mins): 0.5
Phys/Eng

Stairwell to 1st Floor
Delay Time (Mins): 1.5
Distance

1st Floor stairwell door
Delay Time (Mins): 0.5
Phys/Eng

Airlock- 1st Floor Fire exit
Delay Time (Mins): 0.5
Distance

1st Floor Door A
Delay Time (Mins): 0.5
Phys/Eng

1st Floor Corridor A-B
Delay Time (Mins): 3
Distance

1st Floor Door RM1-A
Delay Time (Mins): 0.5
Phys/Eng

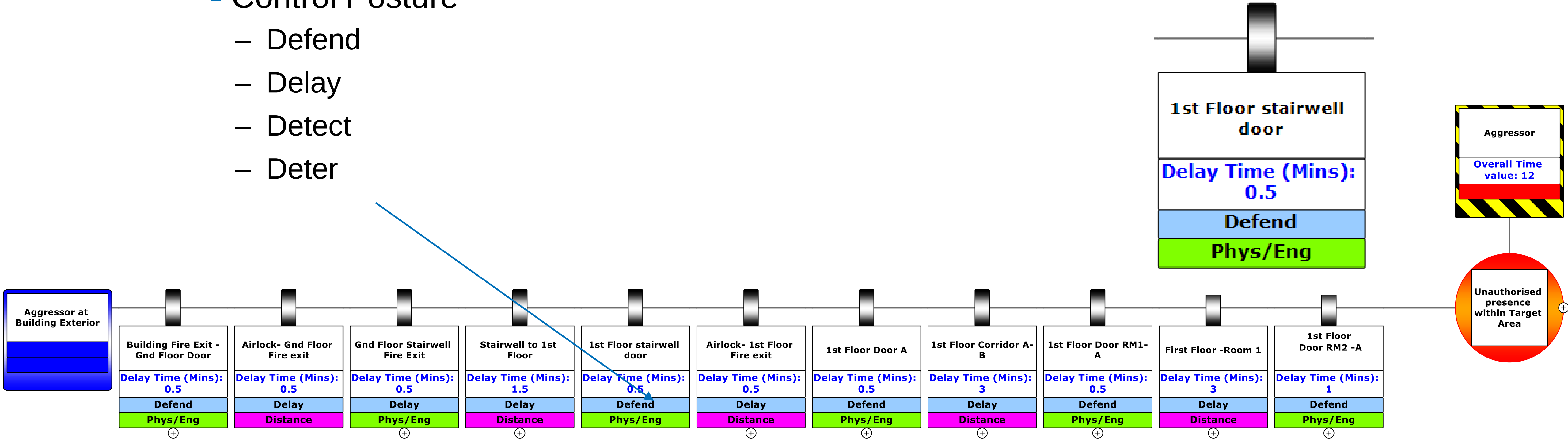
First Floor -Room 1
Delay Time (Mins): 3
Distance

1st Floor Door RM2 -A
Delay Time (Mins): 1
Phys/Eng

Unauthorised presence within Target Area

Bowtie – Adversary Pathway additional Information

- Additional information can be added
- Control Posture
  - Defend
  - Delay
  - Detect
  - Deter



1st Floor stairwell door

Delay Time (Mins): 0.5

Defend

Phys/Eng

Aggressor

Overall Time value: 12

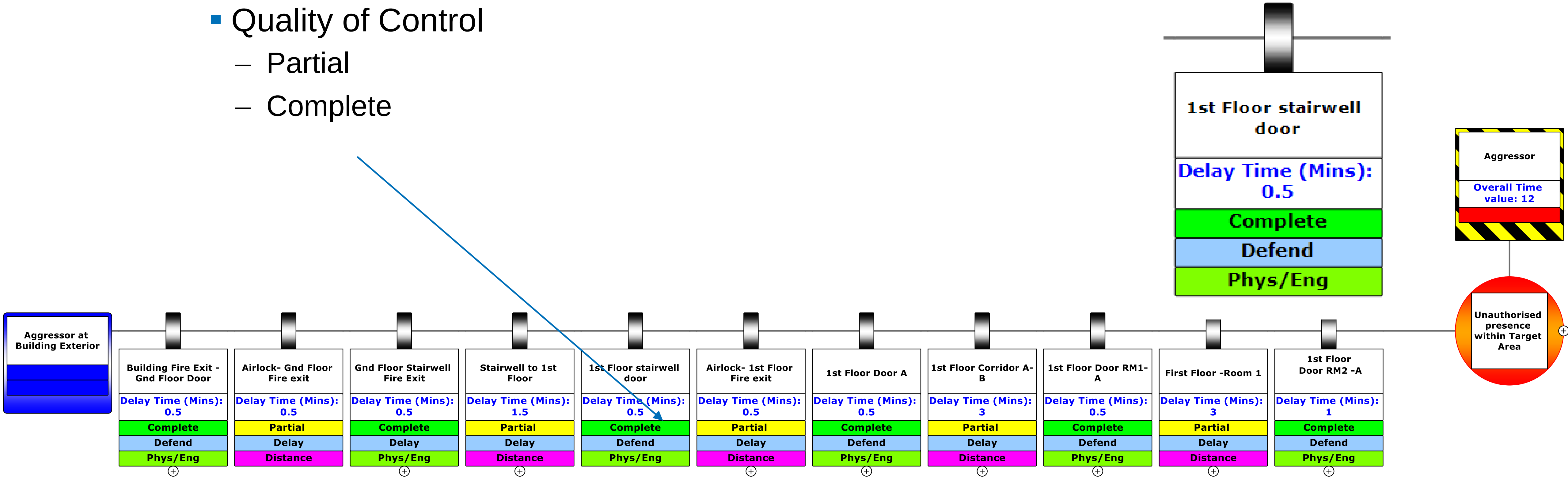
Aggressor at Building Exterior

Barrier	Delay Time (Mins)	Posture	Type
Building Fire Exit - Gnd Floor Door	0.5	Defend	Phys/Eng
Airlock- Gnd Floor Fire exit	0.5	Delay	Distance
Gnd Floor Stairwell Fire Exit	0.5	Delay	Phys/Eng
Stairwell to 1st Floor	1.5	Delay	Distance
1st Floor stairwell door	0.5	Defend	Phys/Eng
Airlock- 1st Floor Fire exit	0.5	Delay	Distance
1st Floor Door A	0.5	Defend	Phys/Eng
1st Floor Corridor A-B	3	Delay	Distance
1st Floor Door RM1-A	0.5	Defend	Phys/Eng
First Floor -Room 1	3	Delay	Distance
1st Floor Door RM2 -A	1	Defend	Phys/Eng

Unauthorised presence within Target Area

Bowtie – Bowtie –Adversary Pathway additional Information

- Additional information can be added
- Quality of Control
  - Partial
  - Complete



1st Floor stairwell door

Delay Time (Mins): 0.5

Complete

Defend

Phys/Eng

Aggressor

Overall Time value: 12

Aggressor at Building Exterior

Barrier	Delay Time (Mins)	Quality	Function	Type
Building Fire Exit - Gnd Floor Door	0.5	Complete	Defend	Phys/Eng
Airlock- Gnd Floor Fire exit	0.5	Partial	Delay	Distance
Gnd Floor Stairwell Fire Exit	0.5	Complete	Delay	Phys/Eng
Stairwell to 1st Floor	1.5	Partial	Delay	Distance
1st Floor stairwell door	0.5	Complete	Defend	Phys/Eng
Airlock- 1st Floor Fire exit	0.5	Partial	Delay	Distance
1st Floor Door A	0.5	Complete	Defend	Phys/Eng
1st Floor Corridor A-B	3	Partial	Delay	Distance
1st Floor Door RM1-A	0.5	Complete	Defend	Phys/Eng
First Floor -Room 1	3	Partial	Delay	Distance
1st Floor Door RM2 -A	1	Complete	Defend	Phys/Eng

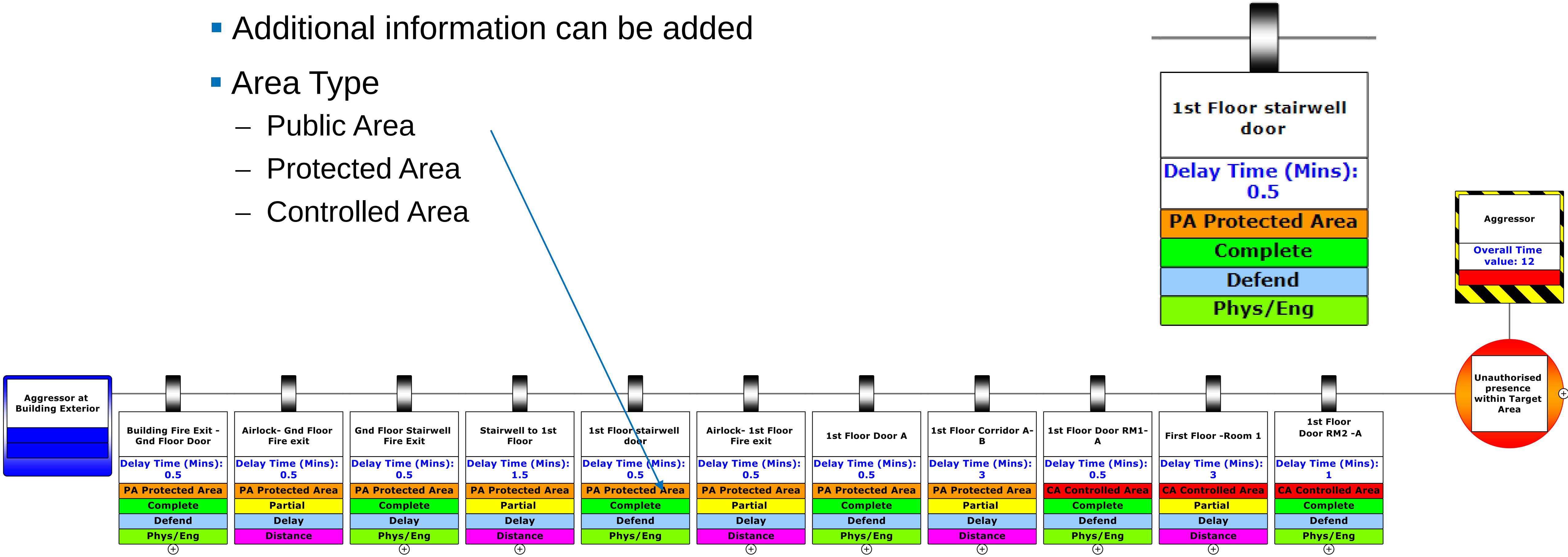
Unauthorised presence within Target Area

Providing Balanced and Graded Protection

- **Graded Protection:**
  - refers to the concept that a facility should be protected to a level that is commensurate with its importance, or consequence.
  - The Security Assessment will identify the critical assets providing identification of protection zones based on the consequences of sabotage of the asset within them. This identifies the holistic requirement for graded protection to be applied.
- **Balanced Protection:**
  - refers to the concept that an adversary should be hindered by Physical Protection Systems independent of which attack strategy and path is chosen.

Bowtie –Bowtie –Graded Security

- Additional information can be added
- Area Type
  - Public Area
  - Protected Area
  - Controlled Area



1st Floor stairwell door

Delay Time (Mins): 0.5

PA Protected Area

Complete

Defend

Phys/Eng

Aggressor

Overall Time value: 12

Aggressor at Building Exterior

Barrier	Delay Time (Mins)	Area	Effectiveness	Function	Type
Building Fire Exit - Gnd Floor Door	0.5	PA Protected Area	Complete	Defend	Phys/Eng
Airlock- Gnd Floor Fire exit	0.5	PA Protected Area	Partial	Delay	Distance
Gnd Floor Stairwell Fire Exit	0.5	PA Protected Area	Complete	Delay	Phys/Eng
Stairwell to 1st Floor	1.5	PA Protected Area	Partial	Delay	Distance
1st Floor stairwell door	0.5	PA Protected Area	Complete	Defend	Phys/Eng
Airlock- 1st Floor Fire exit	0.5	PA Protected Area	Partial	Delay	Distance
1st Floor Door A	0.5	PA Protected Area	Complete	Defend	Phys/Eng
1st Floor Corridor A-B	3	PA Protected Area	Partial	Delay	Distance
1st Floor Door RM1-A	0.5	CA Controlled Area	Complete	Defend	Phys/Eng
First Floor -Room 1	3	CA Controlled Area	Partial	Delay	Distance
1st Floor Door RM2 -A	1	CA Controlled Area	Complete	Defend	Phys/Eng

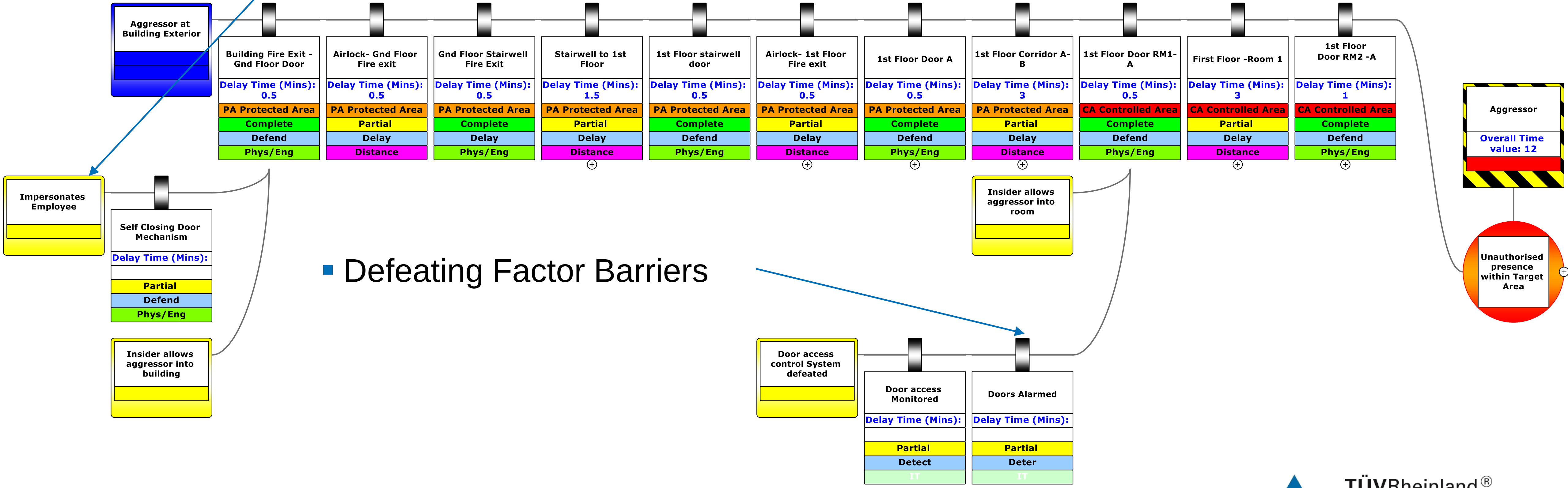
Unauthorised presence within Target Area

- Based on the Critical Assets in an area. The area can be zoned identifying the need for graded security

How can we show security and how it can be defeated?

- Defeating Factor

- Defeating Factor Barriers



Aggressor at Building Exterior

Building Fire Exit - Gnd Floor Door
Delay Time (Mins): 0.5
PA Protected Area
Complete
Defend
Phys/Eng

Airlock- Gnd Floor Fire exit
Delay Time (Mins): 0.5
PA Protected Area
Partial
Delay
Distance

Gnd Floor Stairwell Fire Exit
Delay Time (Mins): 0.5
PA Protected Area
Complete
Delay
Phys/Eng

Stairwell to 1st Floor
Delay Time (Mins): 1.5
PA Protected Area
Partial
Delay
Distance

1st Floor stairwell door
Delay Time (Mins): 0.5
PA Protected Area
Complete
Defend
Phys/Eng

Airlock- 1st Floor Fire exit
Delay Time (Mins): 0.5
PA Protected Area
Partial
Delay
Distance

1st Floor Door A
Delay Time (Mins): 0.5
PA Protected Area
Complete
Defend
Phys/Eng

1st Floor Corridor A-B
Delay Time (Mins): 3
PA Protected Area
Partial
Delay
Distance

1st Floor Door RM1-A
Delay Time (Mins): 0.5
CA Controlled Area
Complete
Defend
Phys/Eng

First Floor -Room 1
Delay Time (Mins): 3
CA Controlled Area
Partial
Delay
Distance

1st Floor Door RM2 -A
Delay Time (Mins): 1
CA Controlled Area
Complete
Defend
Phys/Eng

Aggressor
Overall Time value: 12

Unauthorised presence within Target Area

Impersonates Employee

Self Closing Door Mechanism
Delay Time (Mins):
Partial
Defend
Phys/Eng

Insider allows aggressor into building

Insider allows aggressor into room

Door access control System defeated

Door access Monitored
Delay Time (Mins):
Partial
Detect
IT

Doors Alarmed
Delay Time (Mins):
Partial
Deter
IT

What features of Bowtie are used in Adversary Pathway Analysis?

- The Bowties shown use:
  - BowtieXL
  - Using a number user defined “user data”
  - Analysis uses Excel Functions:
    - Offset
    - Indirect

Thank you for your attention

Any Questions?

Mel Davies – Principal Consultant
Mel.davies@Risktec.tuv.com

TÜVRheinland®
Risktec