This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2018-13325C

VULNERABILITY ASSESSMENT OF RADIOACTIVE MATERIAL

M.K. Snell, D.R. Ek

IAEA Conference on the Security of Radioactive material: The Way Forward for Prevention and Detection
Vienna, Austria
December 3-7, 2018

PRESENTED BY

Mark Snell, Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

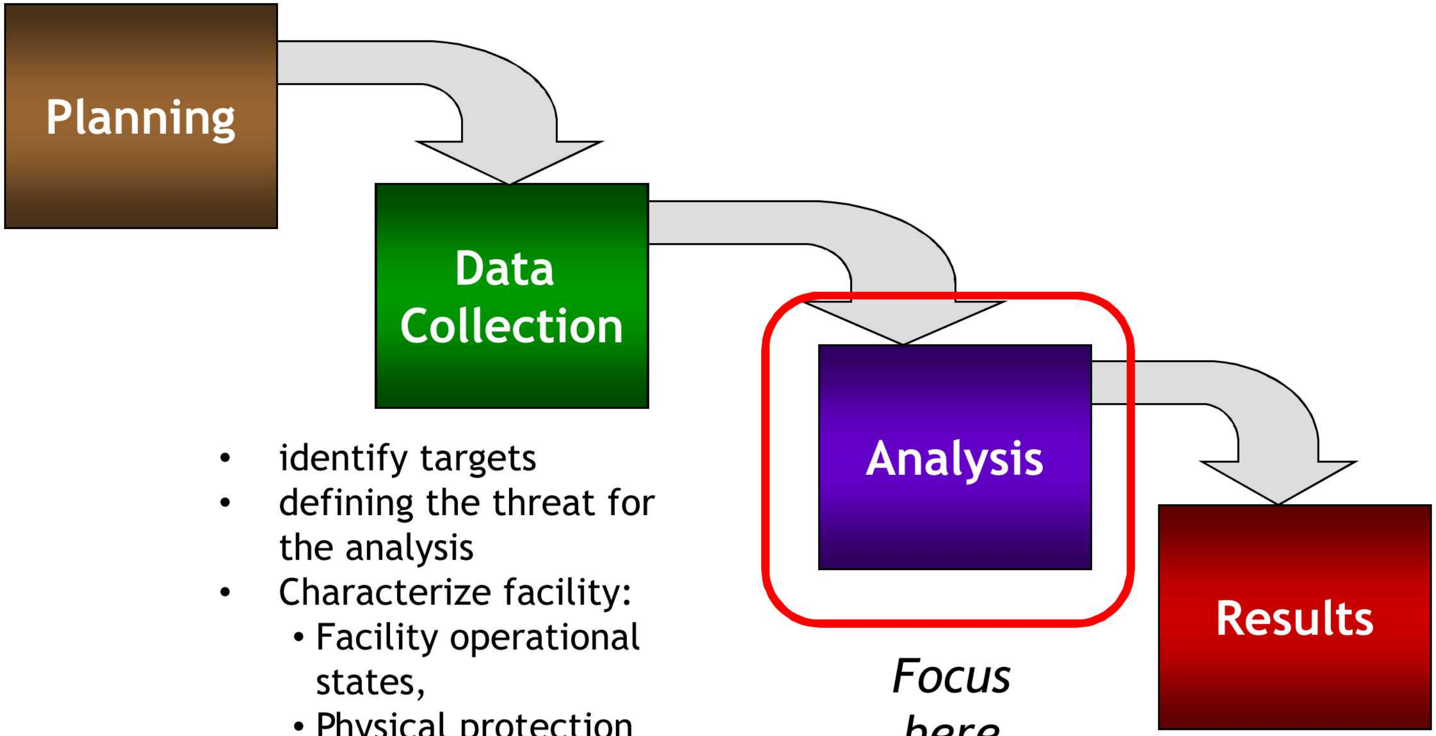
Outline

- Qualitative versus quantitative vulnerability analyses (VA's)
- Phases in the VA process
- Analysis Processes: quantitative vs. qualitative approaches
  - Quantitative: times and probabilities
  - Qualitative: Low, Medium, High robustness
- Robustness factor tables
- Combining robustness factors
- Example

Use of Qualitative versus Quantitative Metrics

- Quantitative VA's, with estimates of probabilities and delay times, are appropriate when
  - There is a Design Basis Threat (DBT)
  - Probabilities of detection, interruption, or neutralization need to be estimated
  - Delay times, detection times, and response times are measured
  - There is sufficient training, personnel, and resources to carry out the analysis
- Qualitative VA's are probably more appropriate for VA's for facilities with radioactive material
  - Limited time and staff available to perform the VA
  - No direct access to a DBT/Alternate Threat Statement (ATS)
  - No databases of delay times or probabilities of detection
  - No interest in most-vulnerable paths/scenarios

Phases in the Vulnerability Assessment Process

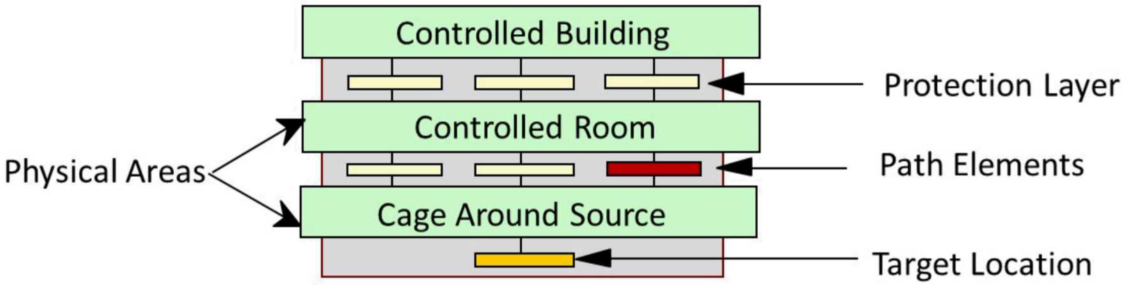


Focus here

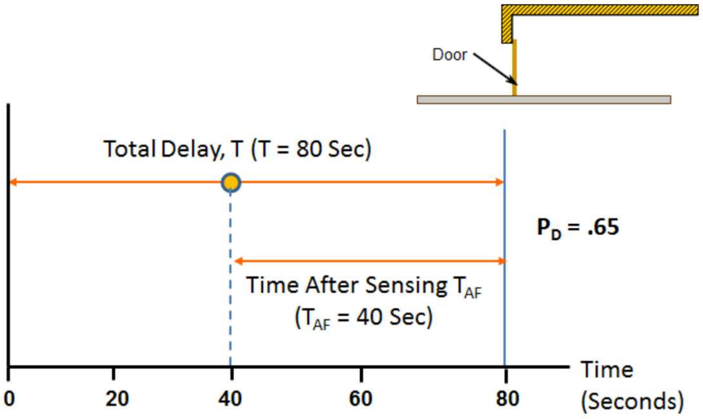
- identify targets
- defining the threat for the analysis
- Characterize facility:
  - Facility operational states,
  - Physical protection measures,
  - Response strategy
  - Security plans, etc.

Analysis Phases of Vulnerability Assessment (VA) – Traditional Quantitative versus Qualitative Process

1. Represent facility areas and layers of protection



2. For each Element/Area, characterize Probability of Detection, P_D, Total Delay Time, T, Time After Sensing, T_{AF}

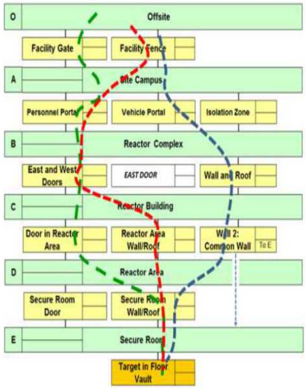


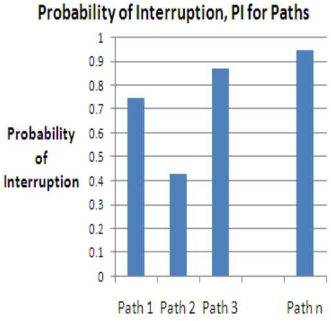
Quantitative	Qualitative (Elements Only)
P_D between 0 and 1	P_D = Low (L), Medium (M), High (H)
T = number	T = L, M, H
T_{AF} = number	Addressed during VA process
T_{AF} is no bigger than T	

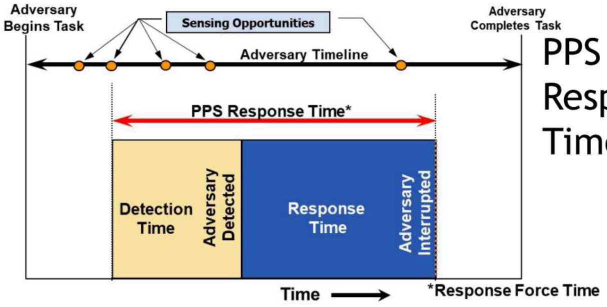
Analysis Phases of Vulnerability Assessment (VA) – Traditional Quantitative versus Qualitative Process – Tools and Metrics

Quantitative Approach

3. Determine Most-Vulnerable P_I Path using Timelines, Detection Times, and Response Times







PPS Response Time

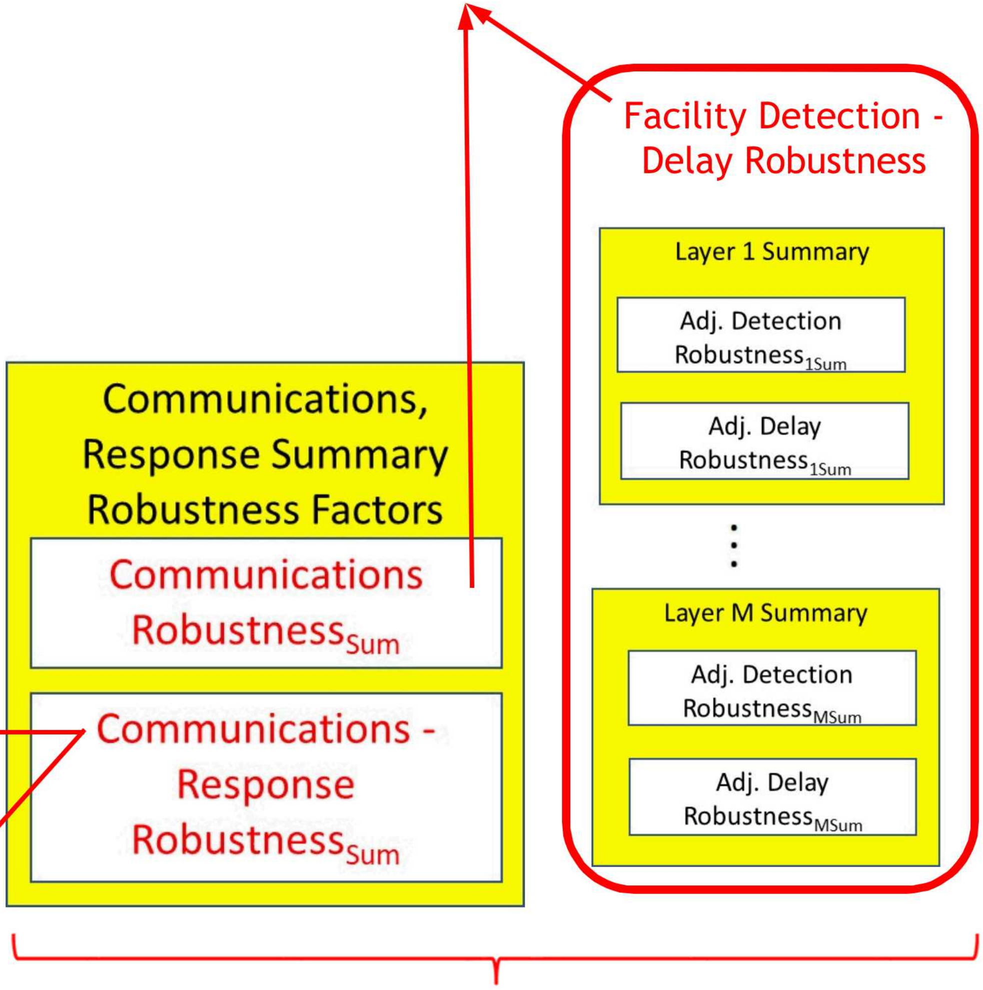
4. Perform Scenario Analysis to Determine P_N and P_E

P_N

P_E

Qualitative Approach

Facility Timeliness Robustness



Facility Detection - Delay Robustness

Layer 1 Summary

Adj. Detection Robustness_{1Sum}

Adj. Delay Robustness_{1Sum}

⋮

Layer M Summary

Adj. Detection Robustness_{MSum}

Adj. Delay Robustness_{MSum}

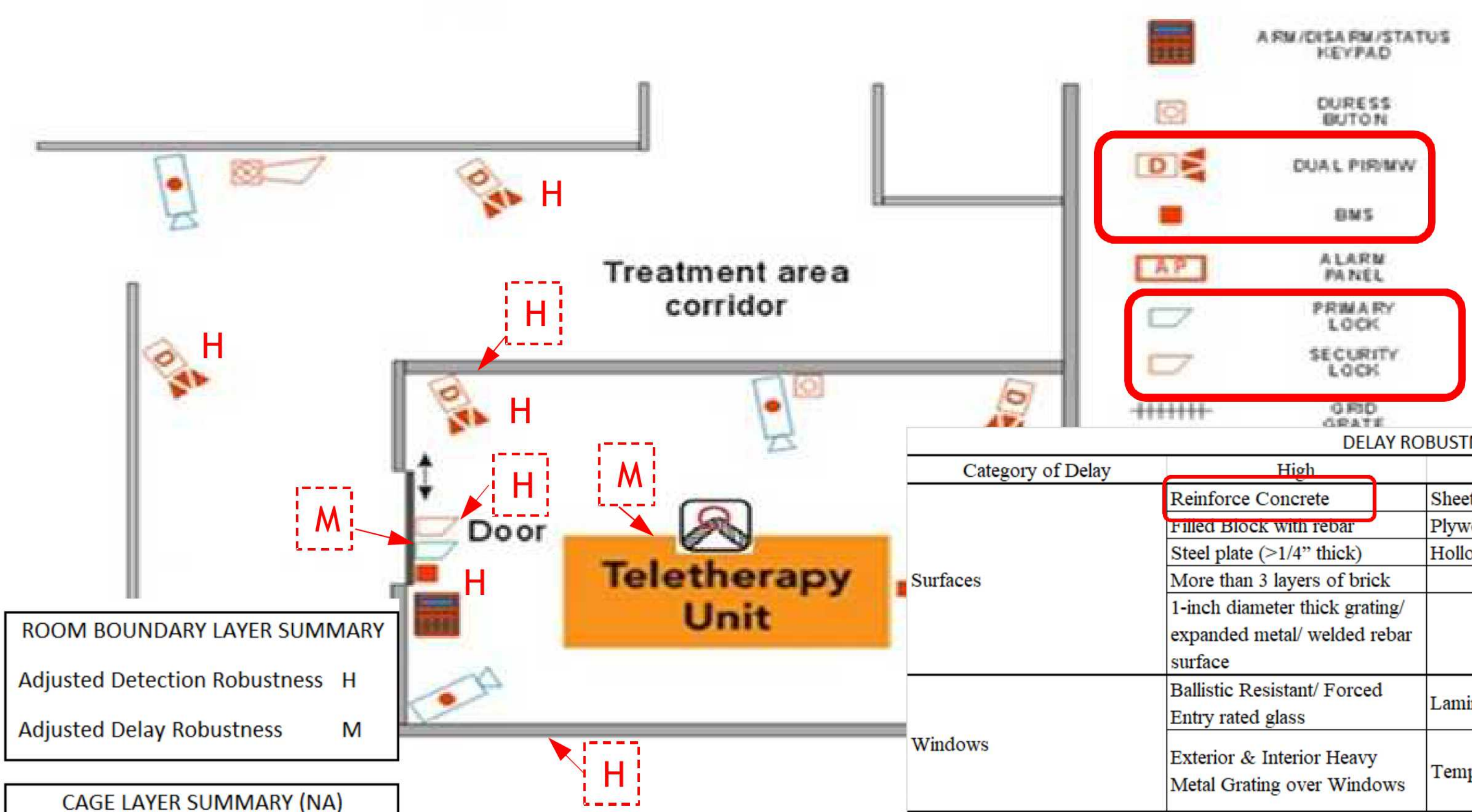
Communications, Response Summary Robustness Factors

Communications Robustness_{Sum}

Communications - Response Robustness_{Sum}

Facility Robustness

Hypothetical Facility – Example of Setting Robustness Factors



ROOM BOUNDARY LAYER SUMMARY

Adjusted Detection Robustness	H
Adjusted Delay Robustness	M

CAGE LAYER SUMMARY (NA)

Adjusted Detection Robustness	NA
Adjusted Delay Robustness	NA

TELETHERAPY UNIT SUMMARY

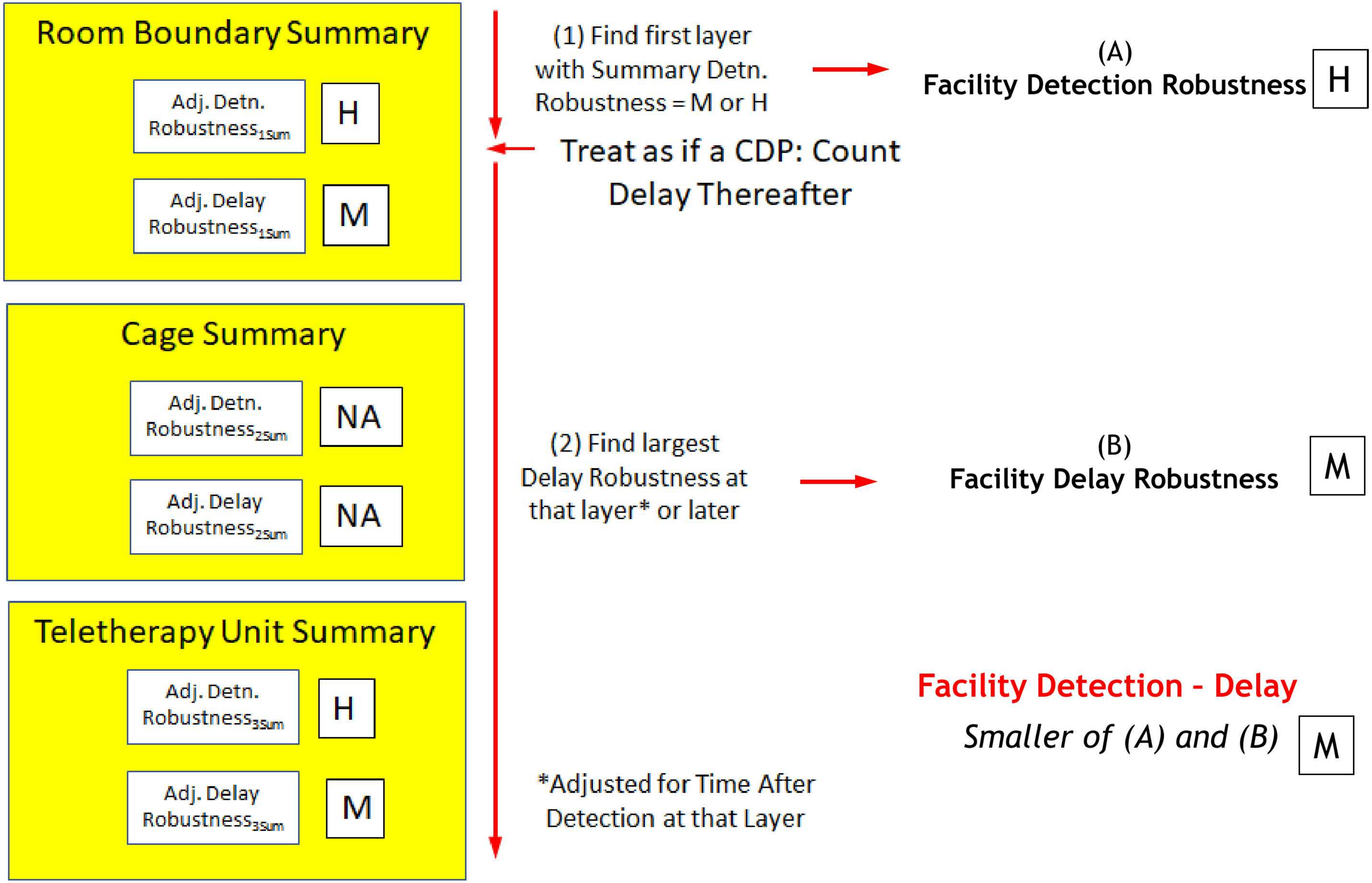
Adjusted Detection Robustness	H
Adjusted Delay Robustness	M

Category of Detection	Type of Detection
Electronic Detection	Door Position
	Volume/room

DELAY ROBUSTNESS

Category of Delay	High	Medium	
Surfaces	Reinforce Concrete	Sheet metal	Plaster
	Filled Block with rebar	Plywood	Comp
	Steel plate (>1/4" thick)	Hollow brick (1-2 layers)	Chain-
	More than 3 layers of brick		Welde
	1-inch diameter thick grating/ expanded metal/ welded rebar surface		
Windows	Ballistic Resistant/ Forced Entry rated glass	Laminated glass	Standa
	Exterior & Interior Heavy Metal Grating over Windows	Tempered glass	Wired Film-c
Doors	GSA Class IV & V Vault	Solid wooden doors with hinge pins and quality locks	Hollov
	UL 608 vault doors or other burglary rated doors	Hollow steel doors with steel frames with hinge pins and quality locks	Any d windo allow (unlock
Locks	Shrouded "Hockey Puck" Locks	Multiple Deadbolt	Single
	Shrouded Padlocks		Cipher
	Electromagnetic Locks		Typica
Source	Industrial Irradiators	Brain Tumour Irradiators Blood Irradiator	Radio;

Facility-level Detection and Delay Robustness is Then Combined



Room Boundary Summary

Adj. Detn. Robustness$_{1Sum}$ H

Adj. Delay Robustness$_{1Sum}$ M

Cage Summary

Adj. Detn. Robustness$_{2Sum}$ NA

Adj. Delay Robustness$_{2Sum}$ NA

Teletherapy Unit Summary

Adj. Detn. Robustness$_{3Sum}$ H

Adj. Delay Robustness$_{3Sum}$ M

(1) Find first layer with Summary Detn. Robustness = M or H

(A)
Facility Detection Robustness H

Treat as if a CDP: Count Delay Thereafter

(2) Find largest Delay Robustness at that layer* or later

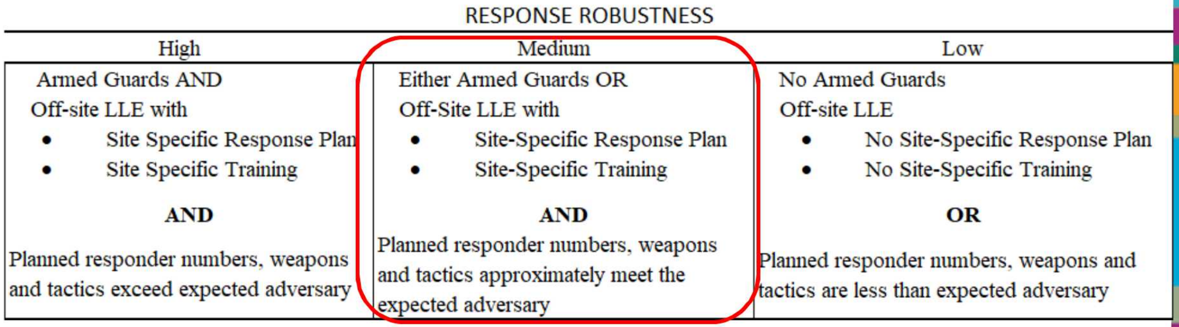
(B)
Facility Delay Robustness M

Facility Detection – Delay

Smaller of (A) and (B) M

*Adjusted for Time After Detection at that Layer

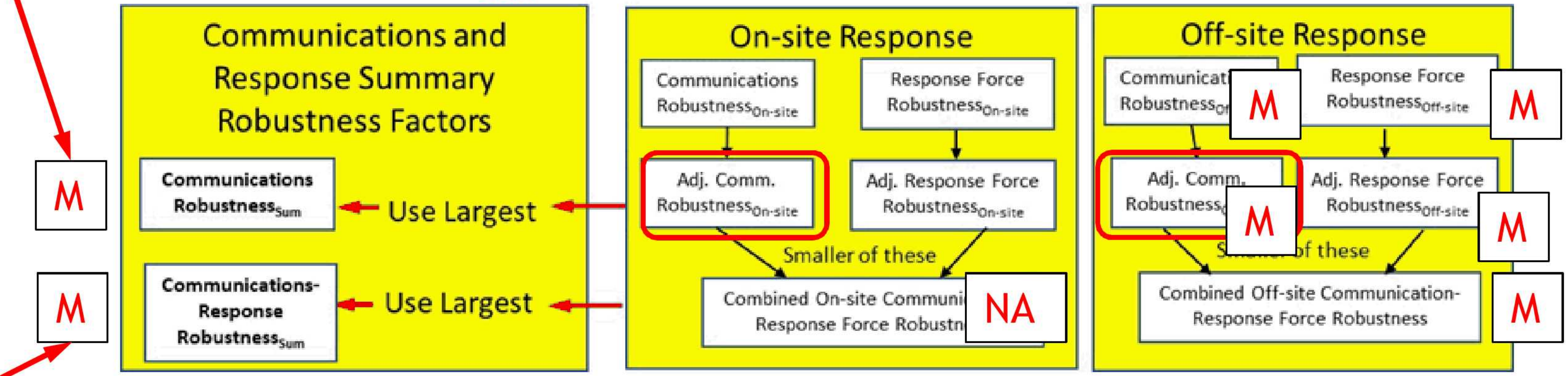
Determining Facility-Level Response- and Communications-Related Robustness Fact



RESPONSE ROBUSTNESS

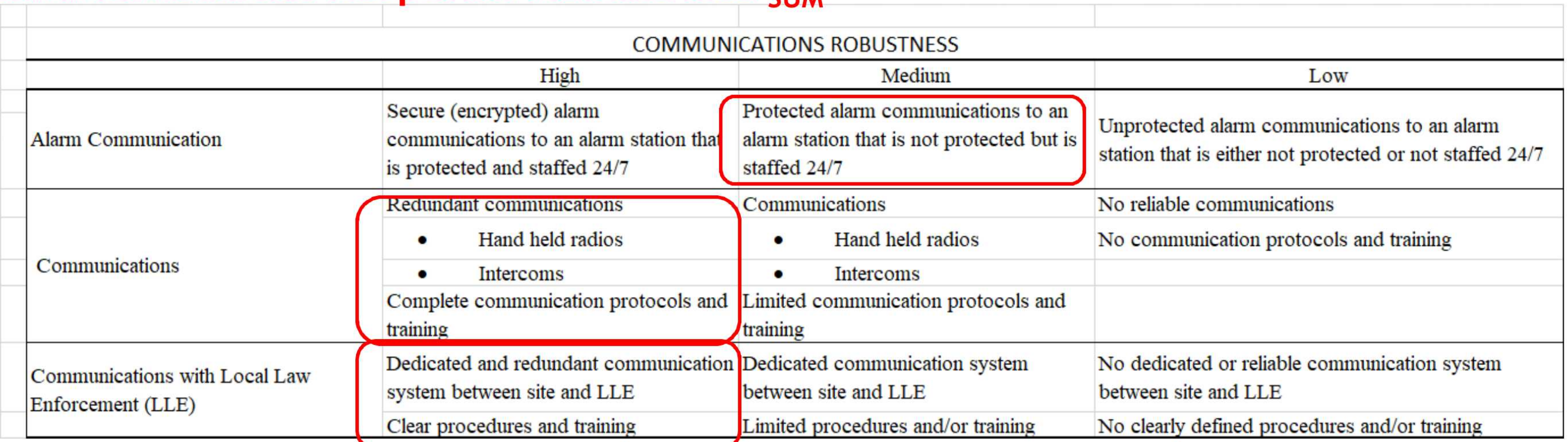
High	Medium	Low
Armed Guards AND Off-site LLE with • Site Specific Response Plan • Site Specific Training **AND** Planned responder numbers, weapons and tactics exceed expected adversary	Either Armed Guards OR Off-Site LLE with • Site-Specific Response Plan • Site-Specific Training **AND** Planned responder numbers, weapons and tactics approximately meet the expected adversary	No Armed Guards Off-site LLE • No Site-Specific Response Plan • No Site-Specific Training **OR** Planned responder numbers, weapons and tactics are less than expected adversary

Communications Robustness $_{SUM}$



M
M
Communications and Response Summary Robustness Factors
Communications Robustness$_{Sum}$
Use Largest
Communications-Response Robustness$_{Sum}$
Use Largest
On-site Response
Communications Robustness$_{On-site}$
Response Force Robustness$_{On-site}$
Adj. Comm. Robustness$_{On-site}$
Adj. Response Force Robustness$_{On-site}$
Smaller of these
Combined On-site Communi
Response Force Robustn
NA
Off-site Response
Communicat
Robustness$_{Of}$
M
Response Force Robustness$_{Off-site}$
M
Adj. Comm. Robustness
M
Adj. Response Force Robustness$_{Off-site}$
M
of these
Combined Off-site Communication-Response Force Robustness
M

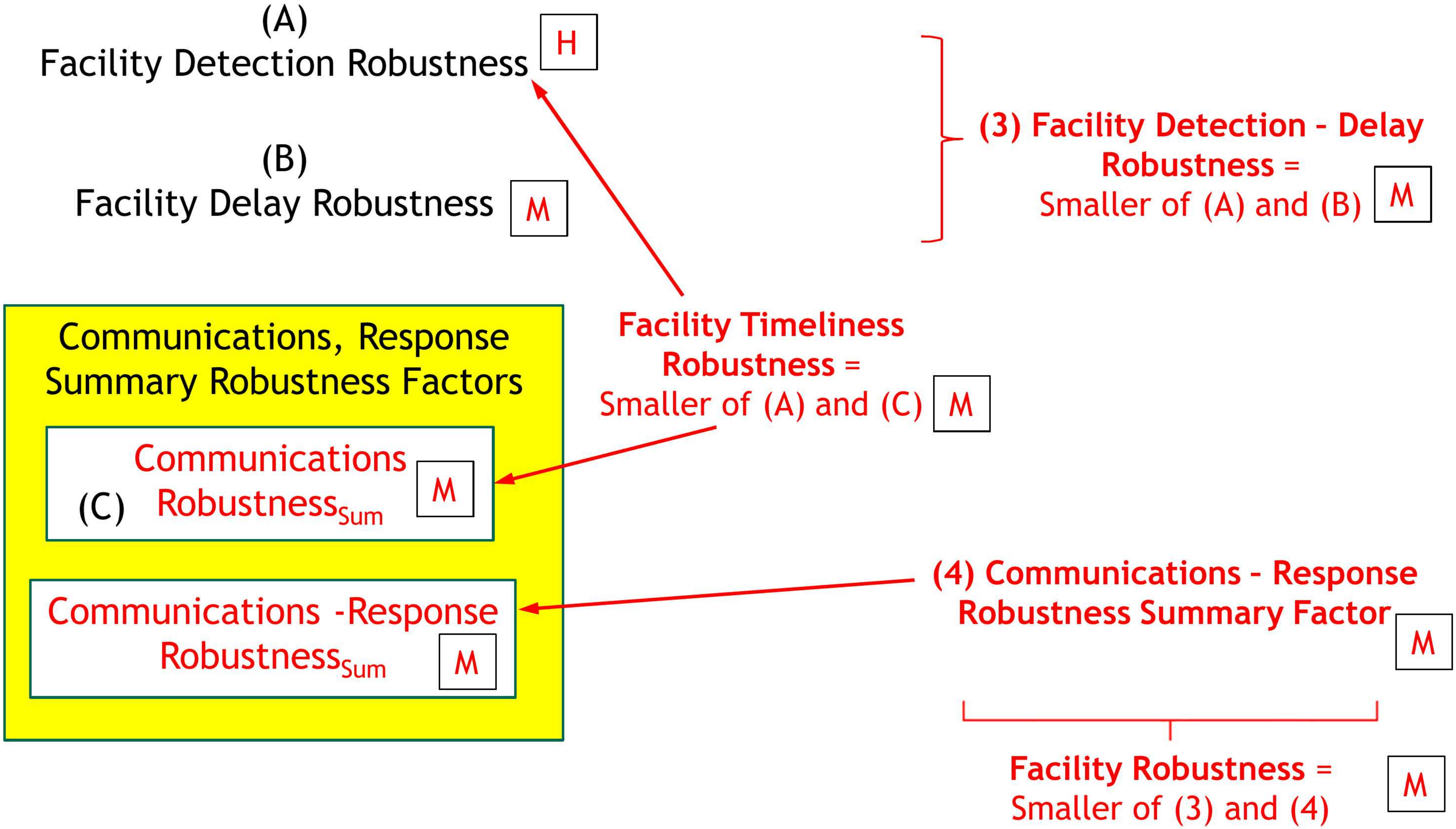
Communications-Response Robustness $_{SUM}$



COMMUNICATIONS ROBUSTNESS

	High	Medium	Low
Alarm Communication	Secure (encrypted) alarm communications to an alarm station that is protected and staffed 24/7	Protected alarm communications to an alarm station that is not protected but is staffed 24/7	Unprotected alarm communications to an alarm station that is either not protected or not staffed 24/7
Communications	Redundant communications	Communications	No reliable communications
	• Hand held radios	• Hand held radios	No communication protocols and training
	• Intercoms	• Intercoms	
	Complete communication protocols and training	Limited communication protocols and training	
Communications with Local Law Enforcement (LLE)	Dedicated and redundant communication system between site and LLE	Dedicated communication system between site and LLE	No dedicated or reliable communication system between site and LLE
	Clear procedures and training	Limited procedures and/or training	No clearly defined procedures and/or training

Assigning Facility-Level Robustness Factors



(A)
Facility Detection Robustness H

(B)
Facility Delay Robustness M

(3) Facility Detection - Delay Robustness =
Smaller of (A) and (B) M

Communications, Response Summary Robustness Factors

(C) Communications Robustness$_{Sum}$ M

Communications -Response Robustness$_{Sum}$ M

Facility Timeliness Robustness =
Smaller of (A) and (C) M

(4) Communications - Response Robustness Summary Factor M

Facility Robustness =
Smaller of (3) and (4) M

Closing Thoughts and Summary

- The assignments of physical protection measures to L, M, H robustness can be performed by the regulator based on a DBT or ATS that the operator doesn't need to see

- Vulnerabilities can be defined several ways
  - Any cause that changes robustness from a M or H to a L
  - Any cause that changes robustness one level: M to L or H to M

- Conclusions
  - Approach is very simple and does not require mathematics
  - No databases of delay times or probabilities of detection required
  - No need to define most-vulnerable paths/scenarios