Physical Vulnerability Assessments for Internal Employees

Bill Graydon

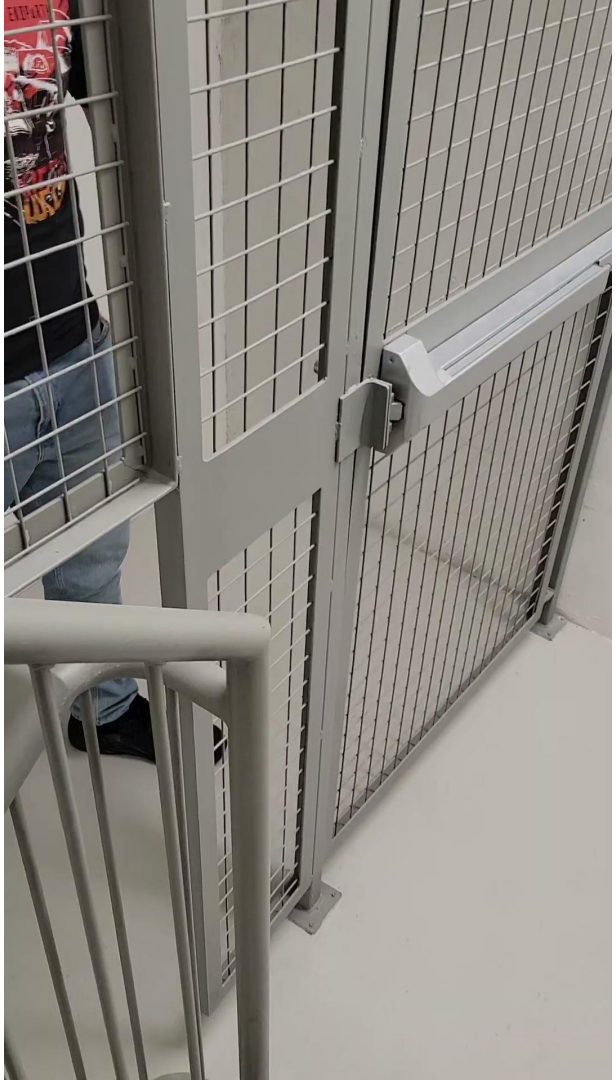
@access_ctrl
b.graydon@ggrsecurity.com



So your employer’s security sucks…

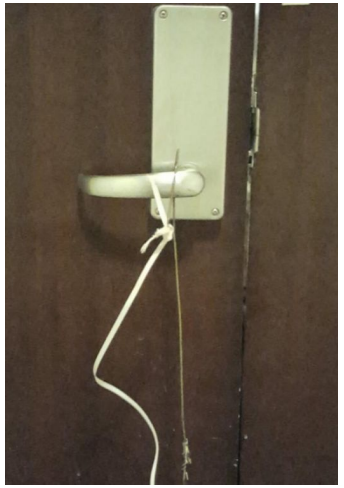
- Why?
  - Bypass
  - Lockpicking
  - Forcible Entry
  - Alarm & Detection
  - Surveillance
- What to focus on
- How to bring it up
- How to get action

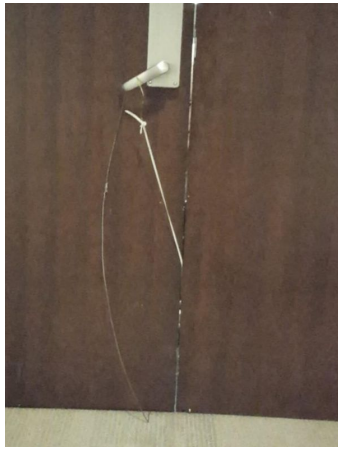




Under Door Tool

1. Insert the tool under the door
2. Maneuver the tool until the top hook rests behind the door handle.
3. Move the tool to the end of the handle.
4. Pull on the string, actuating the lever.





Latch Targeted Bypass



Carding targets the latches that hold the door closed.

Depending on the orientation of the latch, one is able to either “shove” or “pull” the latch.

Outward Swinging Doors

After ensuring that the deadlatch is not actuated:

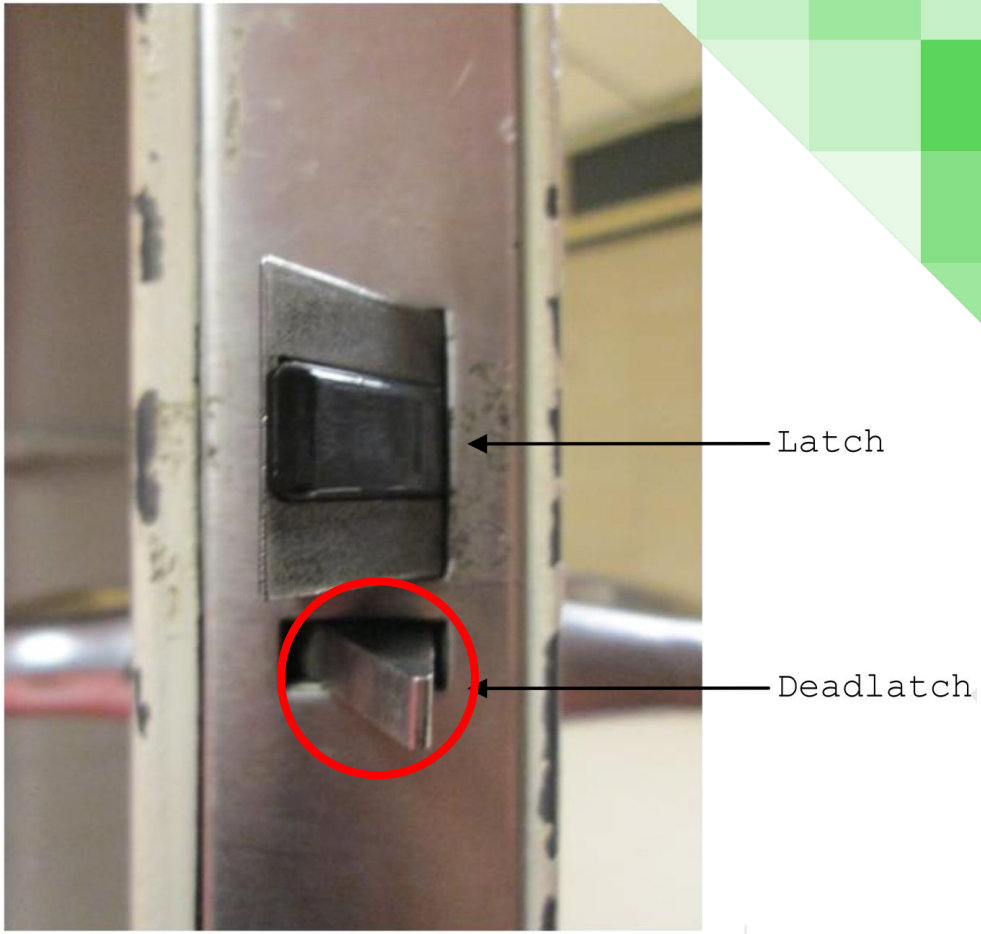
1. Place the latch slip tool behind the latch. Wiggle the latch slip to move the latch into the door.
2. Without removing the tool from holding in the latch, pull the door open.




F
DOREX
SS

Deadlatch





Lockpicking

Lockpicking

This is not a lockpicking talk!

Ask permission before you attempt to pick any locks!

Your expertise will tell you how difficult it is to pick without attempting it though.

Consider:

- Cabinets, locked desks
- Key boxes
- Main doors



Lishis

- I do consider this to be a threat vector worth fixing







Forcible Entry

Why hackers often get physical security wrong



Bill Graydon
b.graydon@ggrsecurity.com
@access_ctrl

No Door is Invulnerable.

- Any door can be breached with sufficient force, skill, time, money and motivation.
- How can we defend against this?
- Detect & respond!





Table 2-1 Forced Entry Tool Sets

THREAT SEVERITY LEVEL	WEAPONS	TOOLS
V	Handguns and sub-machine guns (up to UL 752 Level 3 to overpower guards)	Bulk explosives (up to 20 lbs. /9 kg TNT); linear shaped charges (up to 10,500 grains per foot); unlimited hand, power, and thermal tools
IV		Unlimited hand, power, and thermal tools
III	None	Unlimited hand tools - limited power tools
II		Limited hand tools - low observables

NOTE: For convenience, this table has been derived from information contained in UFC 4-020-01. Information in the current version of that document takes precedence over information in this table.




07-20-2016 Wed 10:47:29
Camera 06



To Secure a Site…

- Detectors on entire perimeter or interior
- Delay the intruder
- Respond fast enough
- … with greater force

Timeline of an Intrusion



Intrusion Begins

The intruder crosses the line from normal to intrusive behaviour

Intruder Sensed

The Blue Team becomes aware of a possible intrusion

Confirmation, Trigger

Sensors confirm intrusion; response is triggered

Intruder Delayed

The Red Team takes time necessary to complete their mission, and overcome the Blue Team's Delays

Response Completes

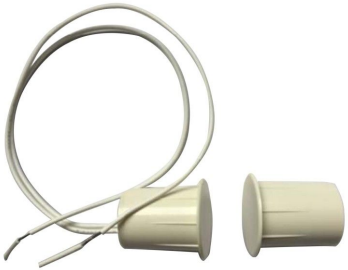
The triggered response completes - either intercepting the Red Team or failing to do so.














1


2

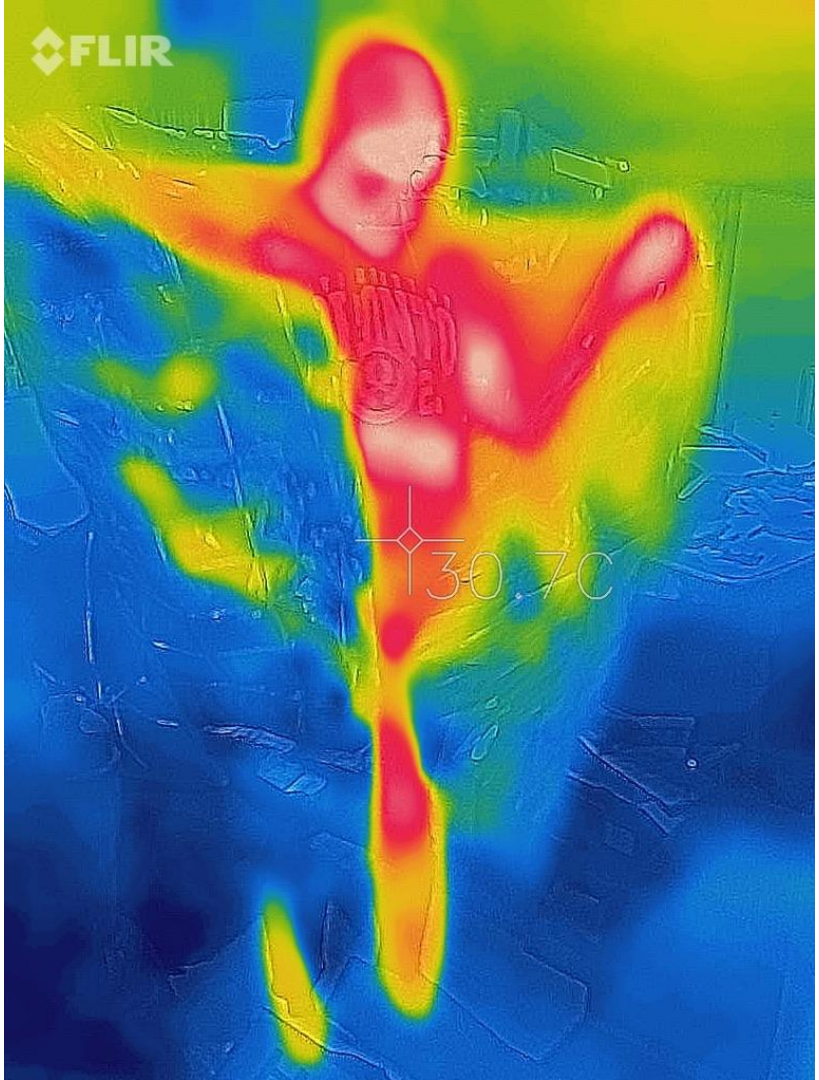

3

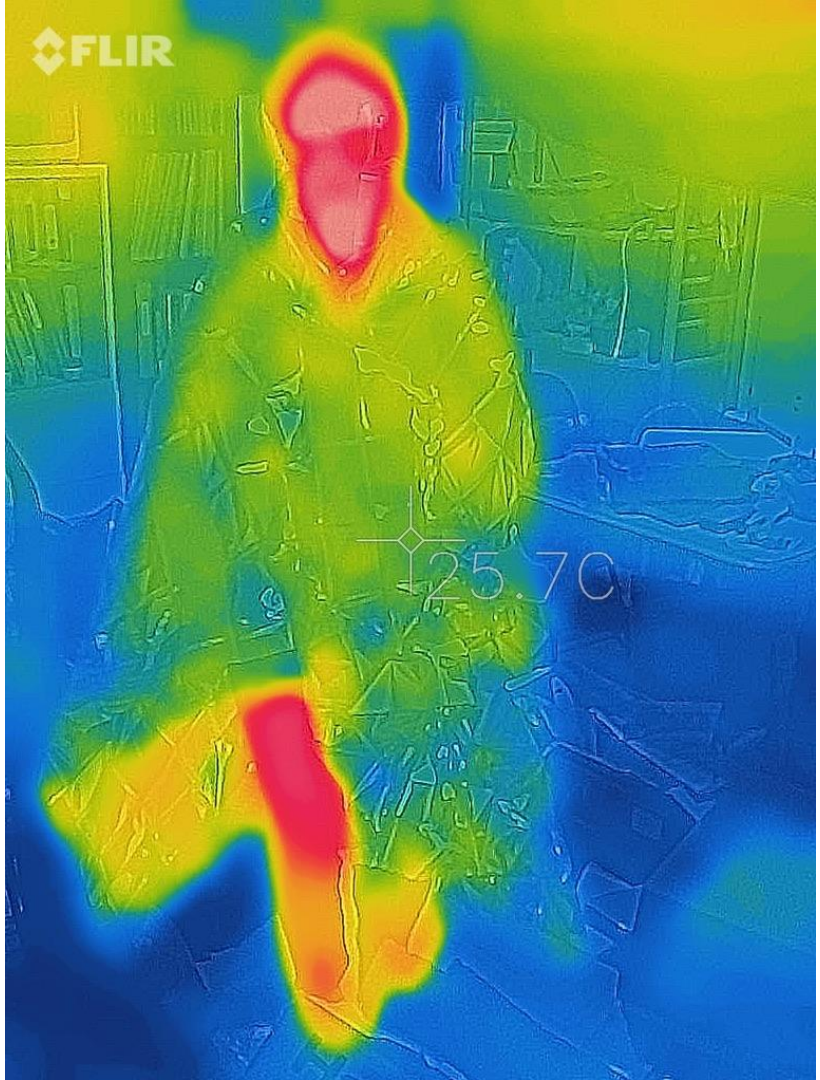




PIR Intrusion Sensor Defeat

- IR Blocking Material
- Move slowly
- Move out of focus range (e.g. pets)
- Avoid perpendicular motion


FLIR
30.7C


FLIR
25.7C



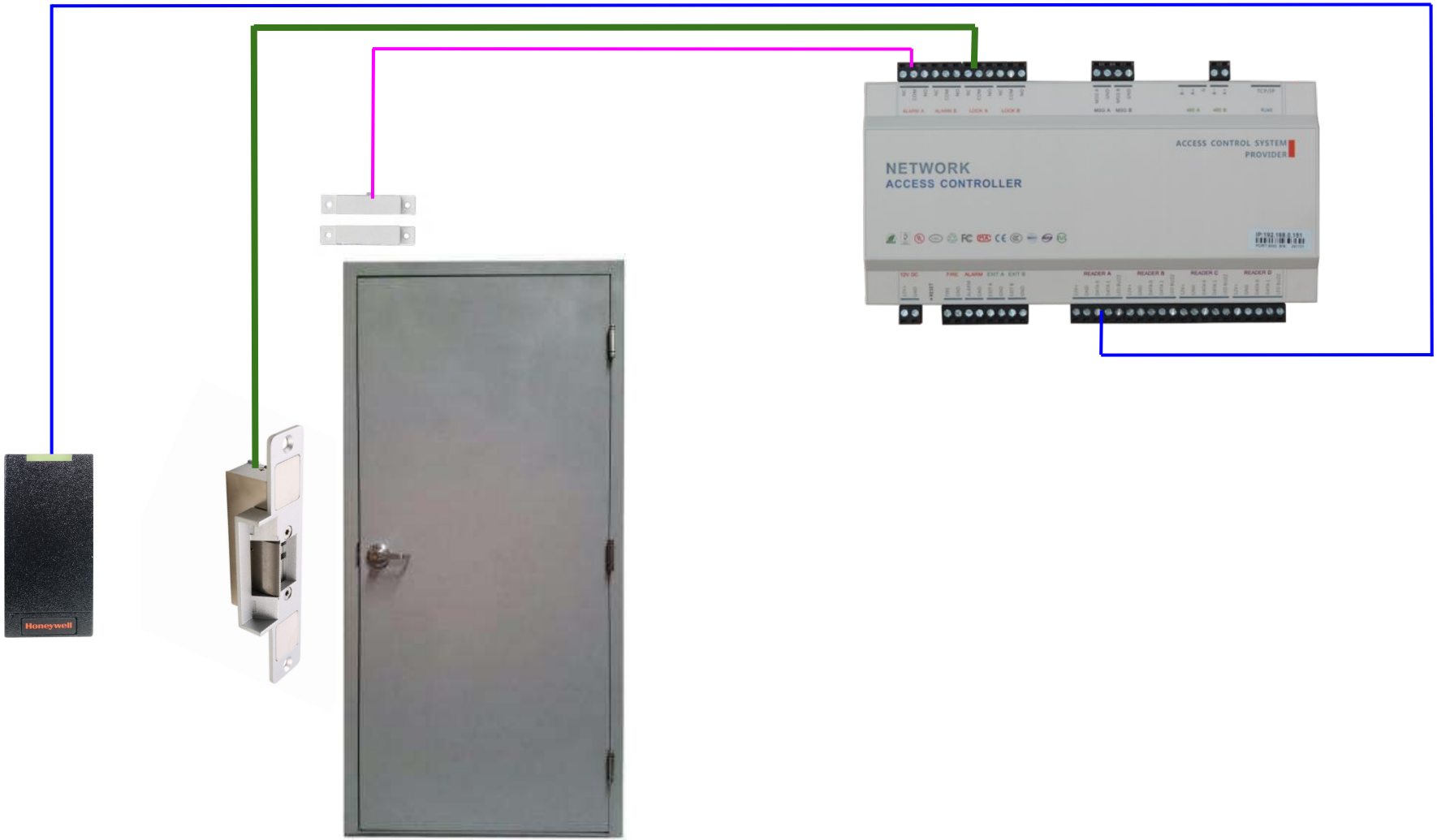

JOIN THE CELEBRATION
Celebrating 60 years
LIP CARE
Celebrating
60

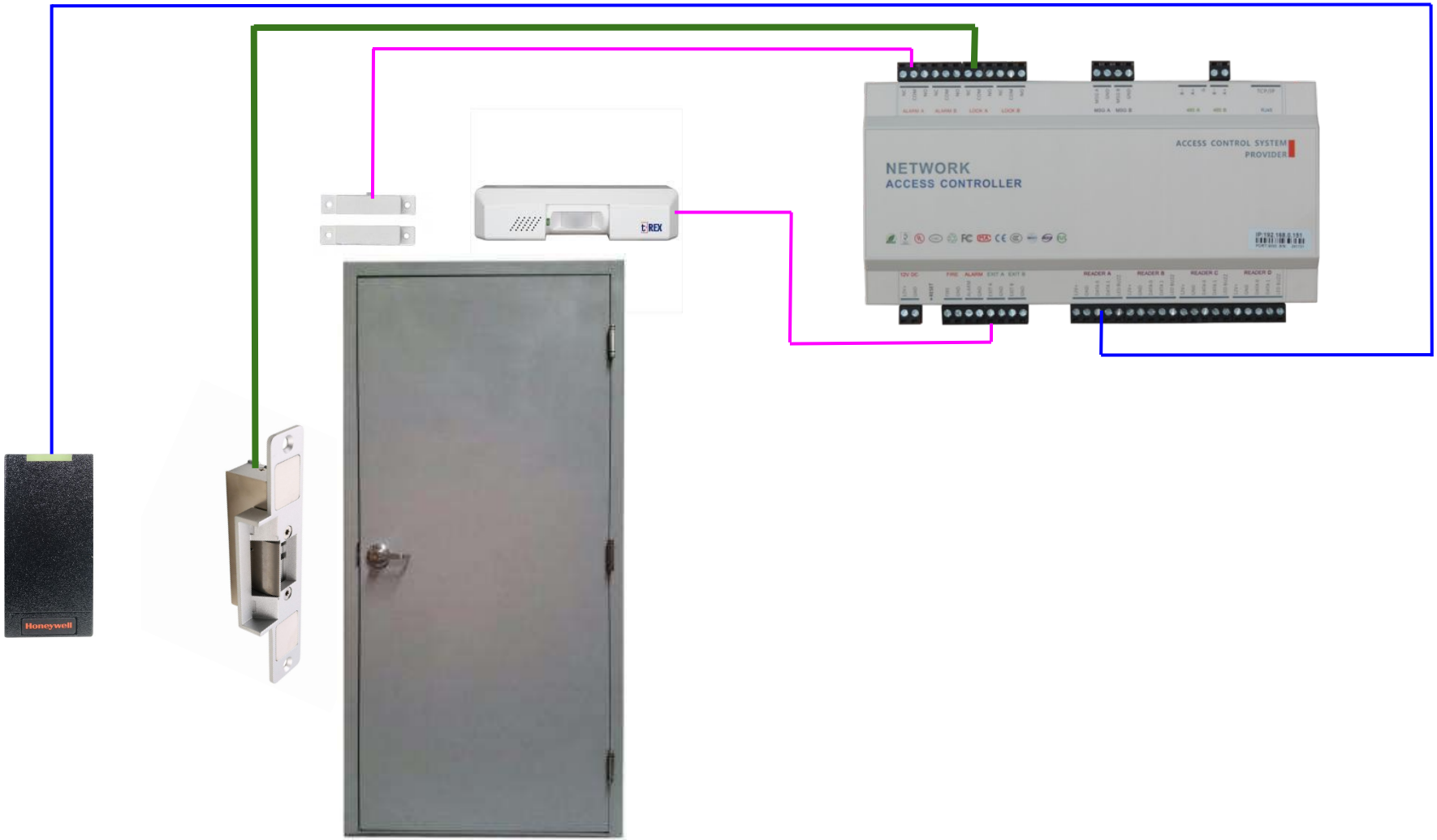
Access Control

@access_ctrl




Honeywell
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER


Honeywell
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER


Honeywell
tREX
NETWORK
ACCESS CONTROLLER
ACCESS CONTROL SYSTEM
PROVIDER

Passive Infrared Sensor




DOOR
EXIT





Access Control Checklist

- This is a blue team talk!

- ❑ Does it allow entry to the correct card
- ❑ Does it deny entry to the wrong card
- ❑ Does it reliably allow egress without false alarming?
  - ❑ Walk slowly up to the door. Approach from the side. Walk quickly.
- ❑ Prop the door open for 5 minutes. Does it alarm?
- ❑ Simulate a forced entry. Does it alarm?
- ❑ Is the alarm actually responded to?
- ❑ Look for low-hanging fruit red team bypasses





- Coverage
- Lighting
- Resolution
- Tampering

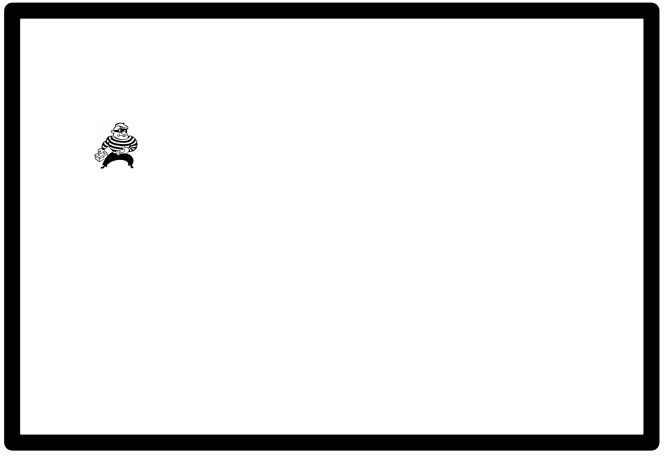
Identify
120%

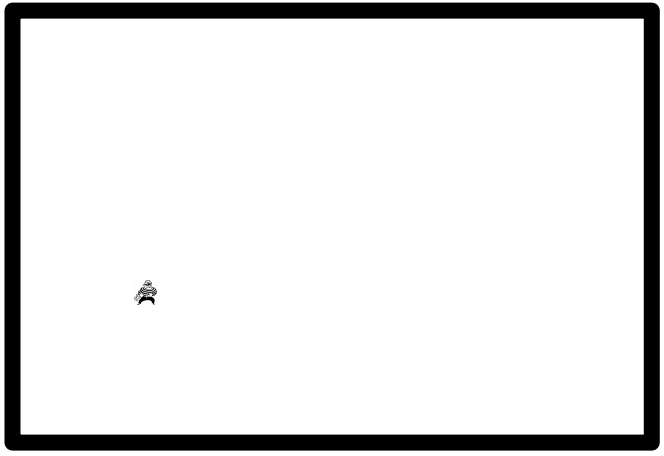




Recognise
50%

Detect
10%



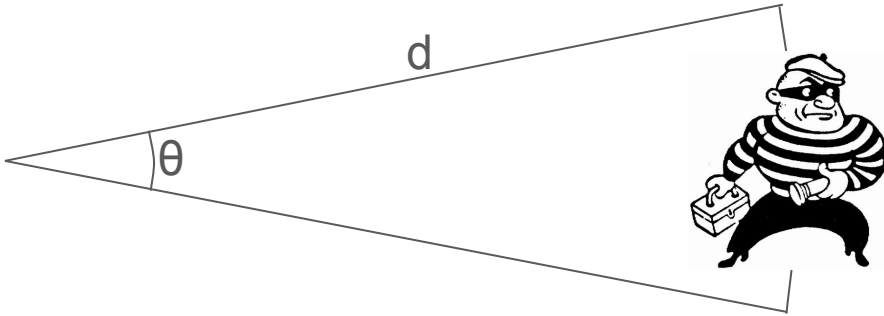


Monitor
5%

Pixel Density

Pixels per foot or metre

Action	PPF	PPM
Inspect	300	1000
Identify	75	250
Recognise	40	125
Observe	20	62
Detect	10	25
Monitor	5	12



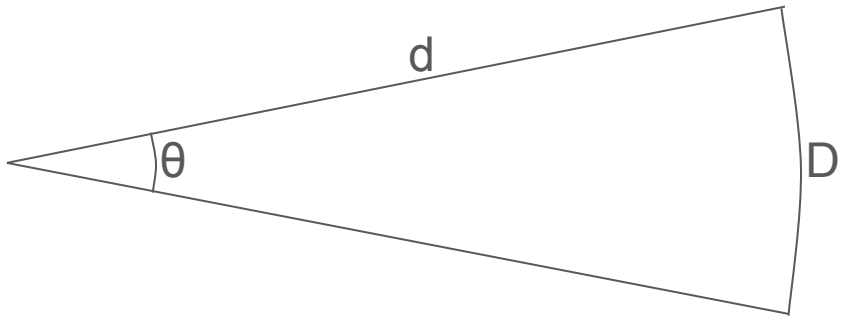
Pixel Density Calculation

Given:

d: distance from camera to subject in feet or metres

θ: field of view in degrees

r: resolution of camera in pixels



Calculate:

PPF/PPM: pixels per foot or metre

$$D = d\theta \frac{2\pi}{360^\circ}$$

$$PPM = \frac{r}{D} = \frac{360r}{2\pi d\theta}$$

IPVM

All Projects

New Project

211 43rd St 24th fl, New Yo

Share Export Add Floor Change

Camera Devices More

All Project Items

Name Camera 1

Model Generic Camera Select Model

Color

Resolution 4MP Distance 30 m

PPM 64.2 Width 41.9 m

Unit Metric HAoV 80 °

Simulated View

AoV: 80° Scenes



Map Types

Google Imagery ©2023 20 m Terms of Use Report a map error

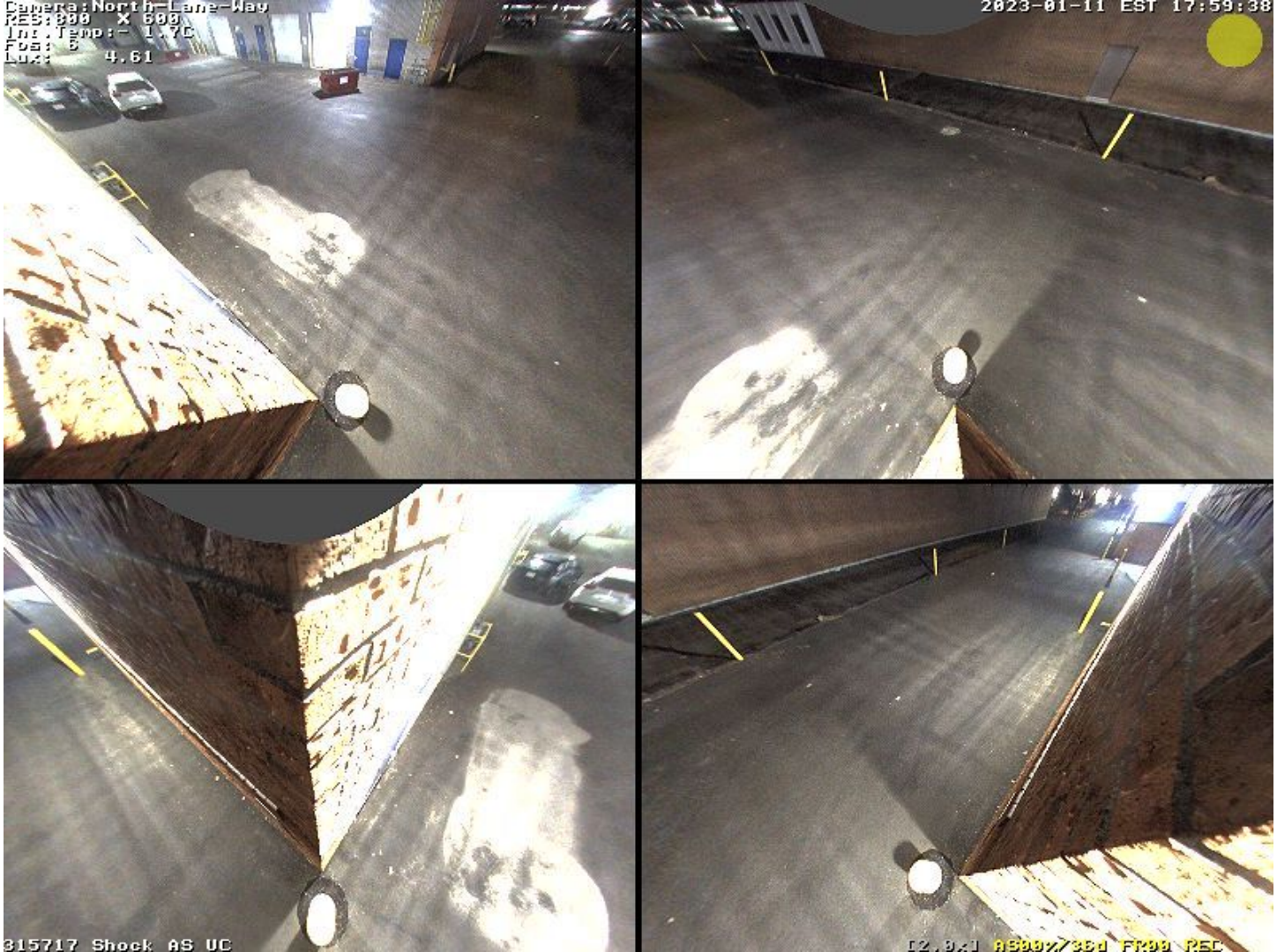
Simulated Person


www.KillamREIT.com
2023-01-11 EST 17:43:35



IR Glare




Camera:North-Lane-Way
RES:800 X 600
Int. Temp:- 1.7C
Fps: 5
Lux: 4.61
2023-01-11 EST 17:59:38
315717 Shock AS VC


Hdy638-Bruce-Mines-PV
800 x 600
Int.Temp: 4.9C
fps:14
2023-01-11 EST 18:12:56
748572 AS SB Arm Record_VM.SB Arm Record_AS UC SB Arm Record_UC
[1.0x] FR02 REC

2023-01-12 22:52:26

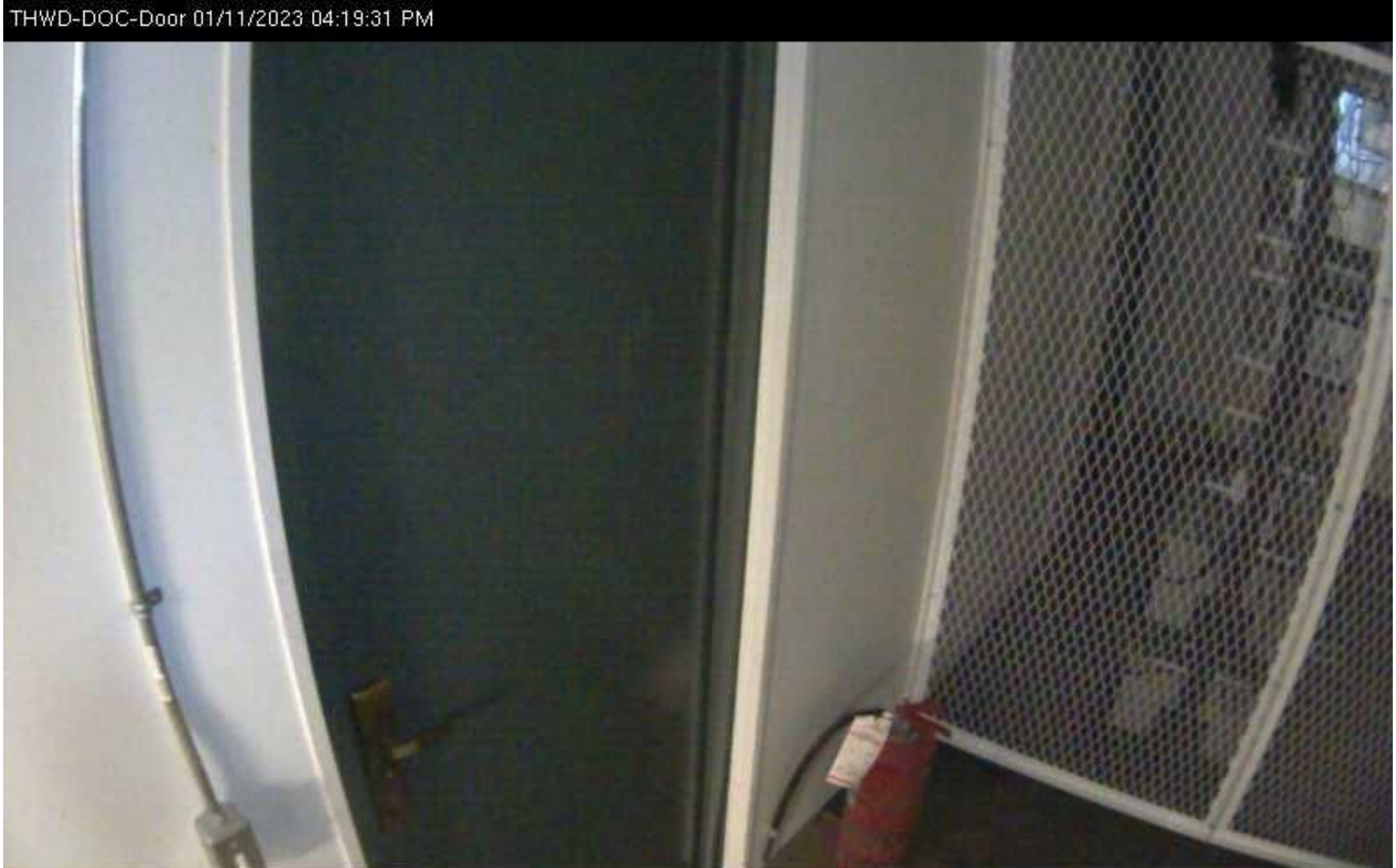

2023-01-11 23:50:38




AXIS




THWD-AOC-Door 01/11/2023 04:18:44 PM


THWD-DOC-Door 01/11/2023 04:19:31 PM

Tampering, Blocking & Repositioning


8






ANY VANDALS?
NOPE.


1171
1169





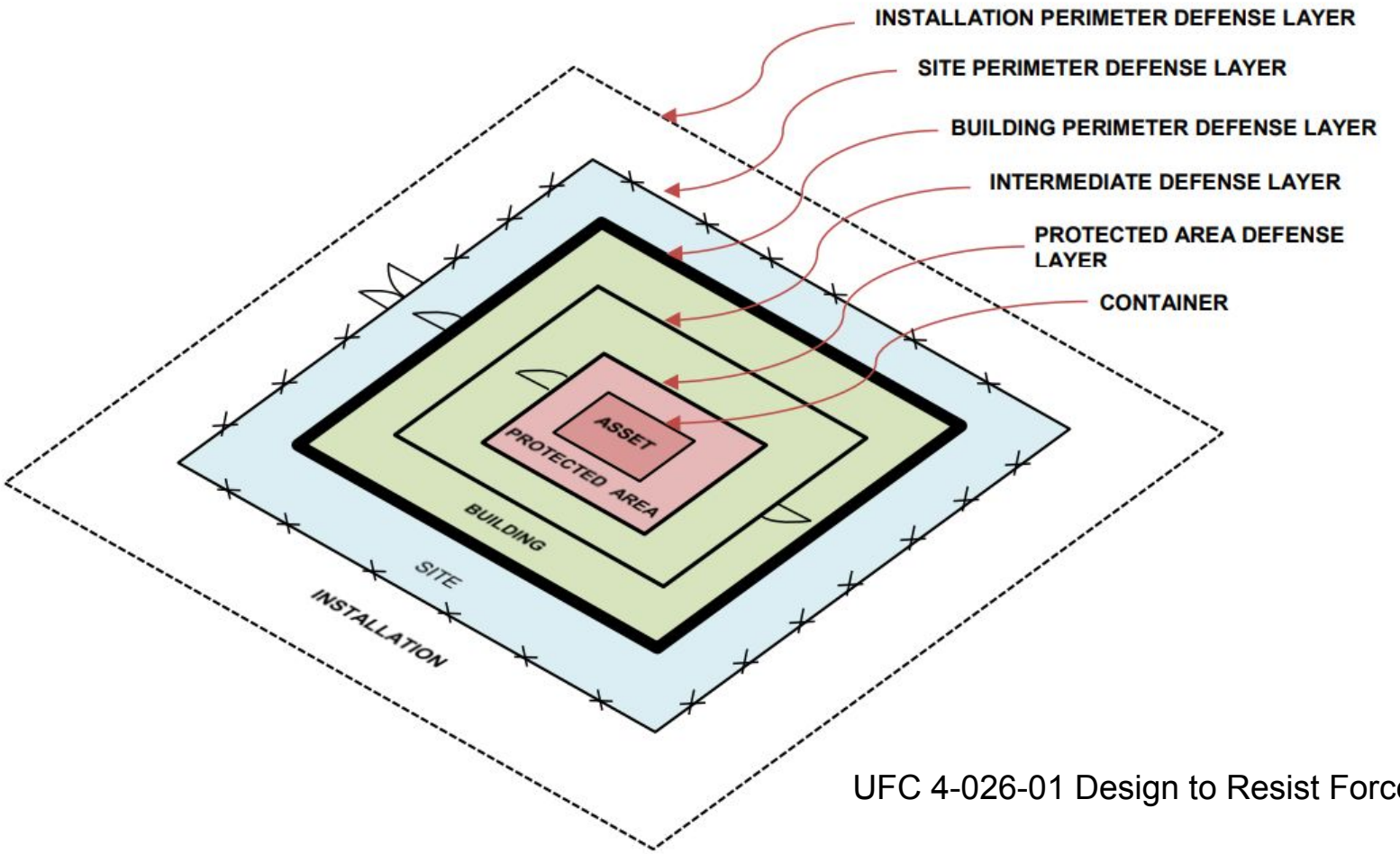
Quick Test of Your Camera Coverage:



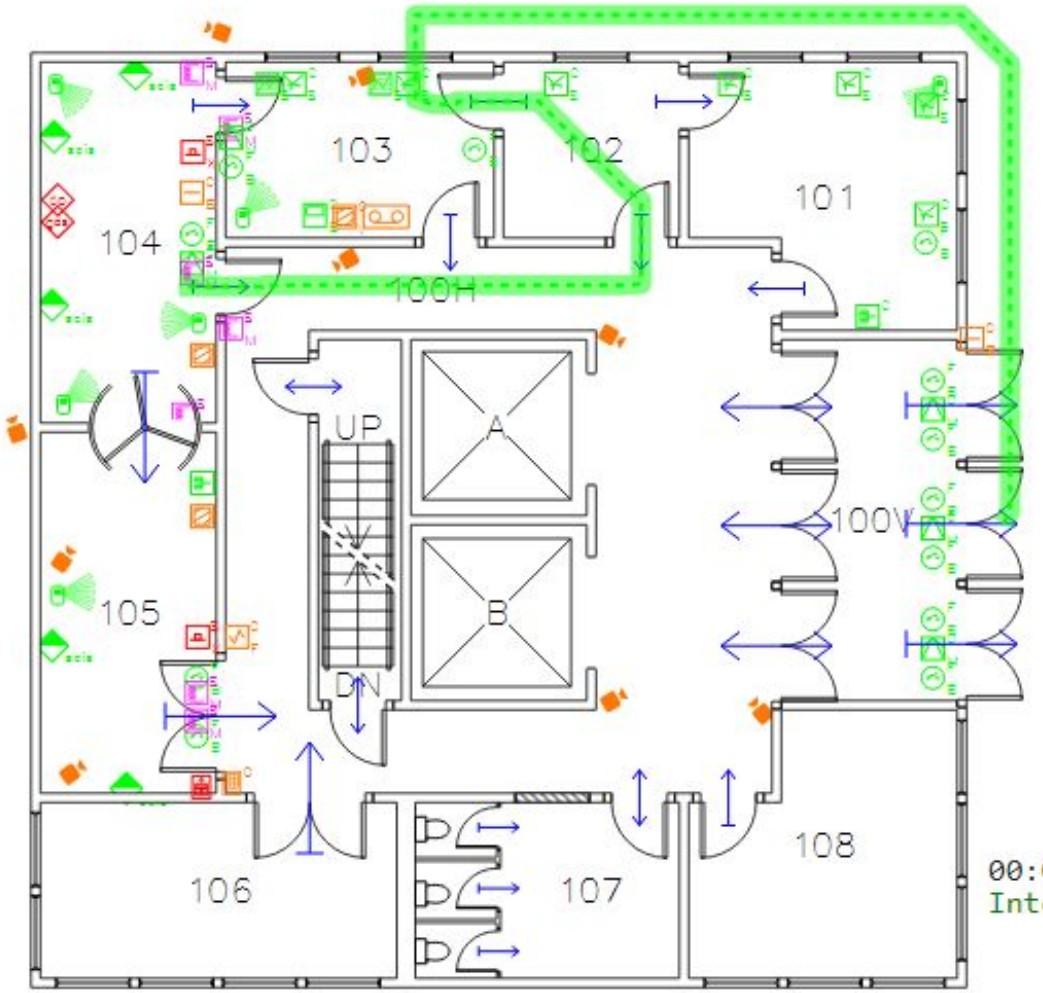


- Do a walkthrough of your facility
  - Entrances / exits
  - Sensitive areas to be protected
- Check your footage of the walkthrough for:
  - Can you see identifying details of the person on tape? Can you read the license plate on vehicles?
  - When is the person not in view?
  - When in view, can you tell what the person is doing?
- Repeat at night. Repeat after shutting off power at the breakers. Repeat in inclement weather.
  - Is lighting sufficient?
  - Is there significant glare?
  - Can you still make out identifying features?
  - Can you still tell what the person is doing?
- Inspect your camera placement and cable runs for ease of tampering
  - Your DVR should be in a time-rated safe! (or backed up offsite)

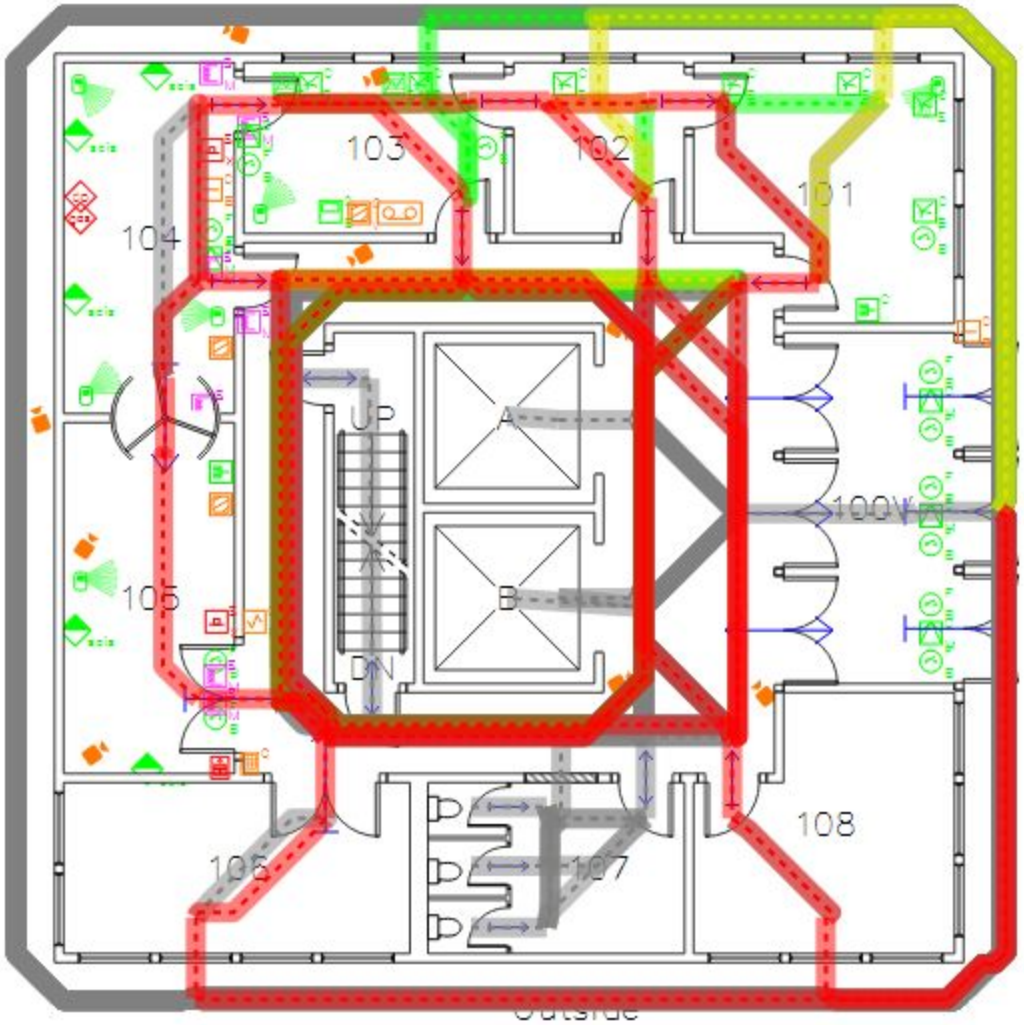
Figure 3-1 Defense Layers



UFC 4-026-01 Design to Resist Forced Entry



00:02:56: 58' - Outside | Window | Single | 8 Si | 21' - Si
Intercept


103
102
101
104
UP
A
100W
B
105
DN
108
106
107
Outside

Likelihood	Consequence: Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Process to Fix Findings

- Make note of all findings
- Bring up only the most critical, to underscore importance
- Get connected with the Facilities team, if there is one
- Don’t be a pedant about low-probability or low-impact findings
- Focus on getting systems working as intended before worrying about bypasses

Questions?

Bill Graydon
b.graydon@ggrsecurity.com
@access_ctrl

Go Try It in the Physical Security Village!

GGR SECURITY CONSULTANTS