A Novel Architecture for Intrusion Detection Based On "Deliberate Motion Analytics"

An Enabling Technology for Security of the Future

John Russell
Distinguished Member of Technical Staff
Sandia National Laboratories
Email: Jlrusse@sandia.gov
Cell: 505 977-6707

Dr. Carl Stern
PhD Computer Science
Management Sciences Inc.
Email: cstern@mgtsciences.com
Cell: 505 321-6856

Peter Blemel
MS Computer Science
Management Sciences Inc.
Email: Peter_Blemel@mgtsciences.com
Cell: 505 991-2112

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

SAND2022-4542 C

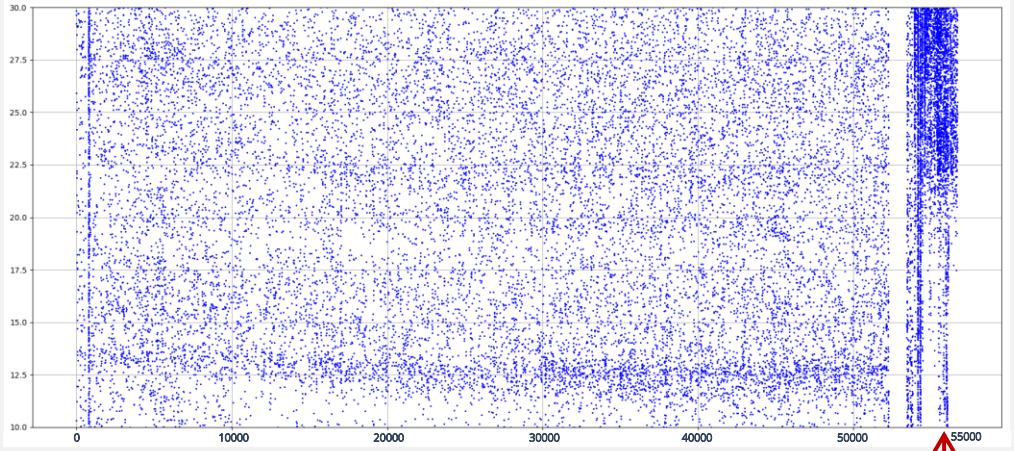
What is the Deliberate Motion Analytics (DMA) System?

DMA is a sensor fusion system fusing potentially diverse sensor outputs to create a multi-physics intrusion detection system

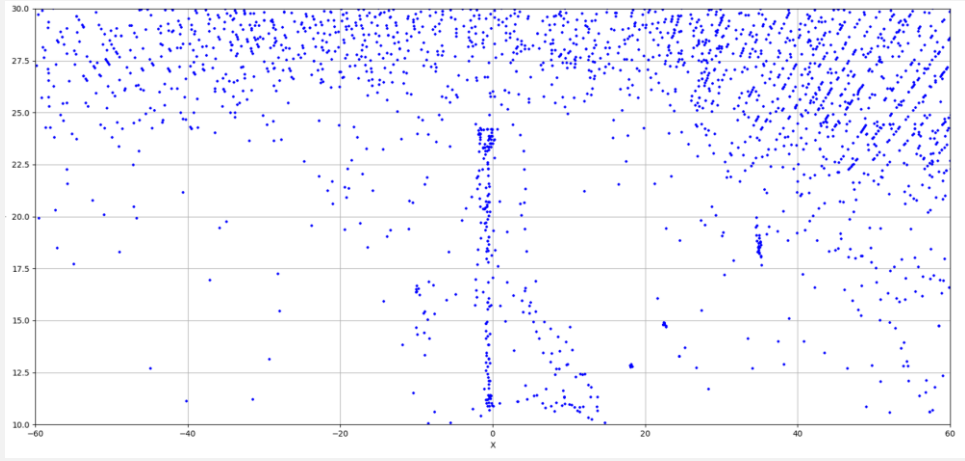
- With good design and layout, fusion of complementary sensors enhances the coverage and performance of a detection system over a wider range of intruders and detection conditions

DMA uses deliberate motion analytics to differentiate intruder alarms from nuisance alarm sources, including weather, moving fences, and foliage

- DMA provides a multilevel framework for distinguishing intruders from nuisance alarms
- Research has shown that high nuisance alarm rates can significantly degrade intrusion detection performance



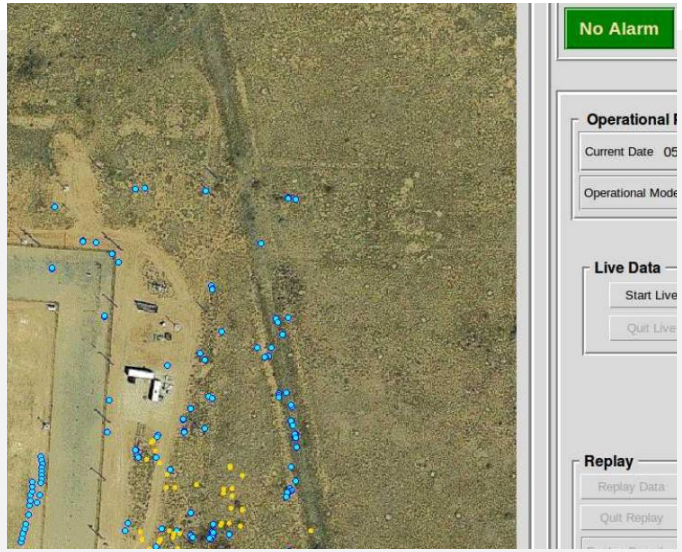
Raw Radar Alarms Collected Over a 15 Hour Period (each blue dot is an alarm)
Two DMA Alarms were declared between 54000 and 55000 seconds

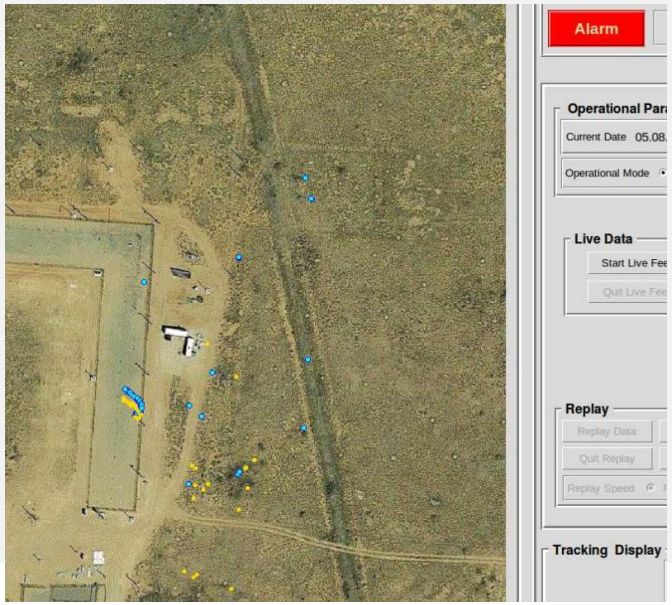


Both alarms were verified as human crossing the detection zone at Red Arrow

What is the DMA system?

- DMA implements a multi-intelligence fusion algorithm – applying:
  - A generalized form of multi-hypothesis tracking (MHT)
  - Recursive Bayesian probability models (Kalman filters), dynamic Bayesian networks (DBNs), and machine learning





Motivation for DMA

Current Challenges:

- Nuclear power generation faces increasing economic pressure
- Cost of physical security ranks high on plant operational costs
- U.S. nuclear power plants are seeking new, cost-effective physical security methods and technologies

Why Its Important:

- Represents an enabling capability to solve many problems encountered in traditional perimeter designs

- Can provide reliable “beyond the fence” detection, resulting in increased delay, giving response forces earlier notification of an impending attack

- New security architectures that will reduce cost; no lights needed, no fences needed for detection (may need for response or legal purposes)

- Significant reduction in cost

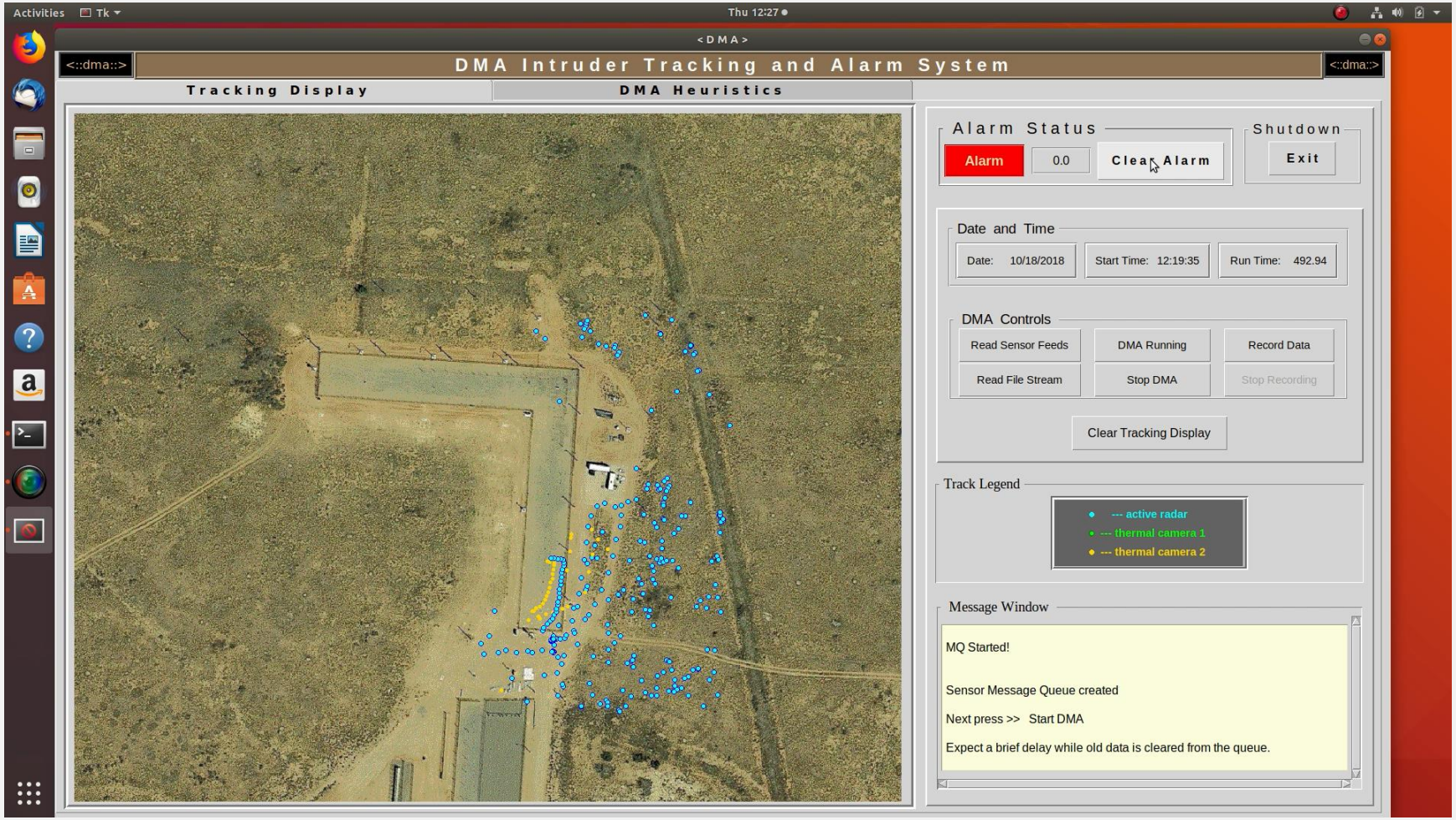
A Deeper Look at DMA

- Key ideas in DMA
  - DMA supports the recognition of human intruder motion and the factors that differentiate human motion from wildlife and weather-induced phenomena
  - The importance of controlling nuisance alarms, as high rates can impair the performance of human operators (see human research studies)
  - Managing attentional resources in time critical decision making – focusing on imminent intruder threats while postponing decisions in situations where more information may be forthcoming
  - Reducing the impact of uncertainty by avoiding premature decisions

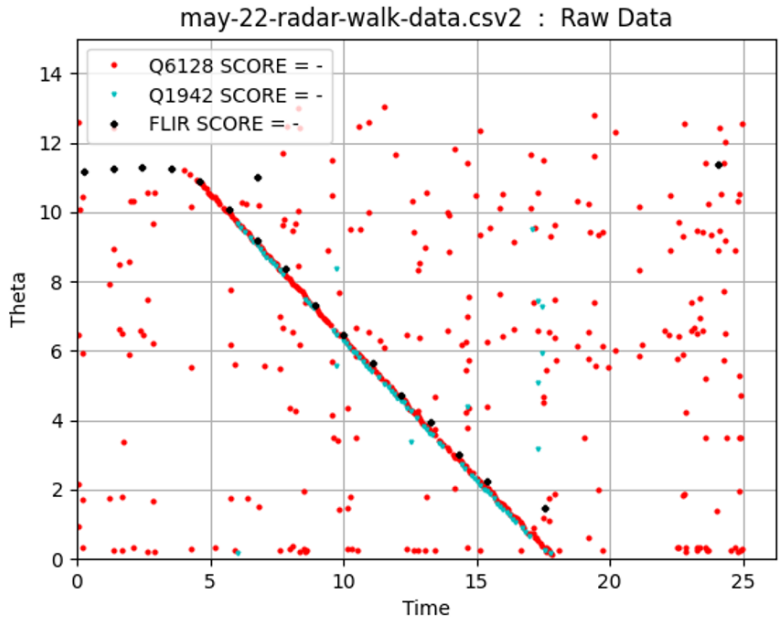
A Deeper Look at DMA

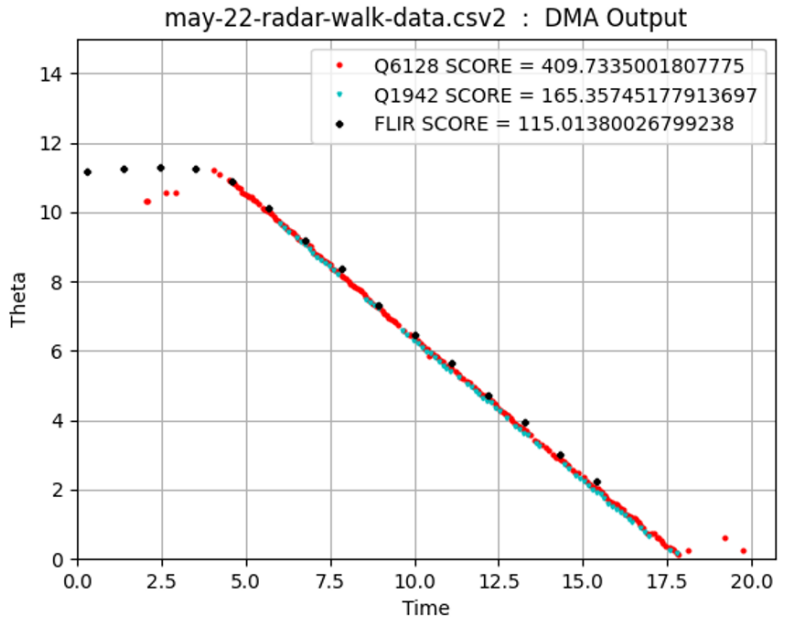
- DMA generalizes the MHT algorithm beyond a focus on simple tracking (intruder motion and location)
  - Diverse sensors and information sources with information about targets can be fused to further inform expectations about risks and threats
    - DMA is only one example of an information source
  - Each hypothesis represents a different vision and expectation of a potential future
  - Newly arriving information is interrogated through a wide range of diverse lenses (hypotheses), allowing a deeper and more exhaustive investigation of the potential meaning (risks and threats) associated with events

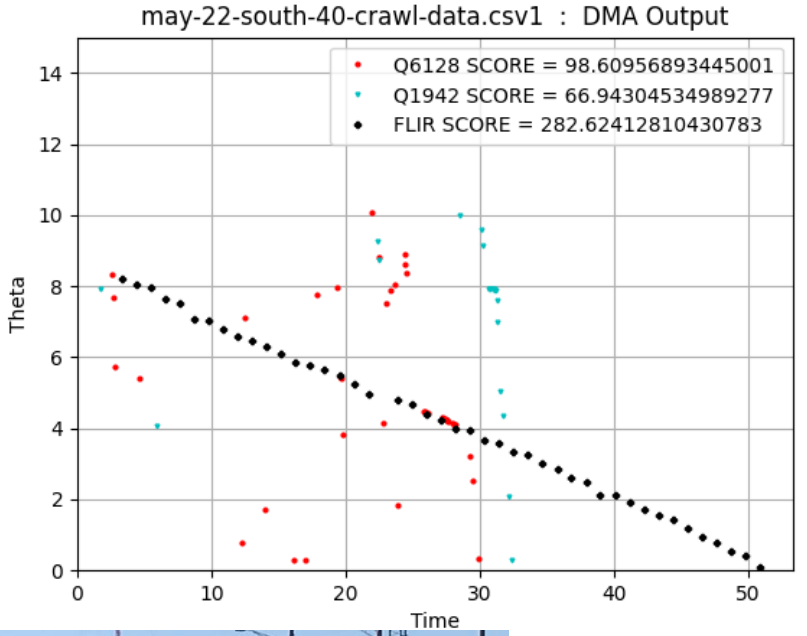
2018 Demonstration Inside the PIDS Fusing Radar and Thermal Radar



Beyond the Fence Test Results (Intrusion Tests)



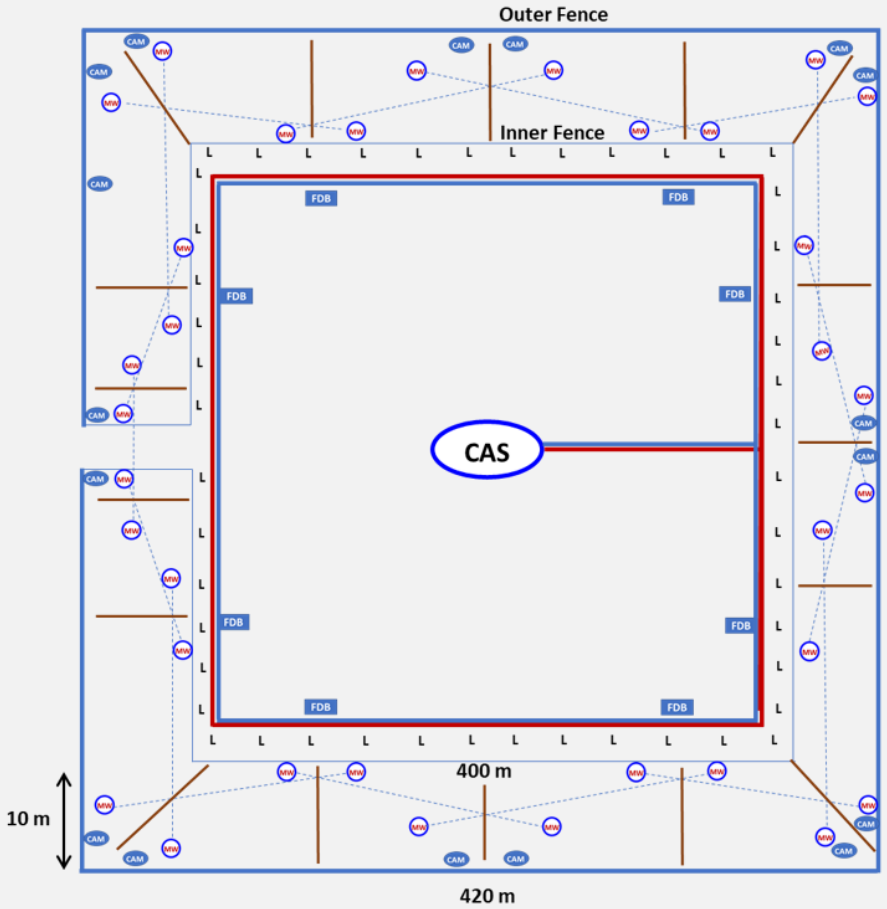




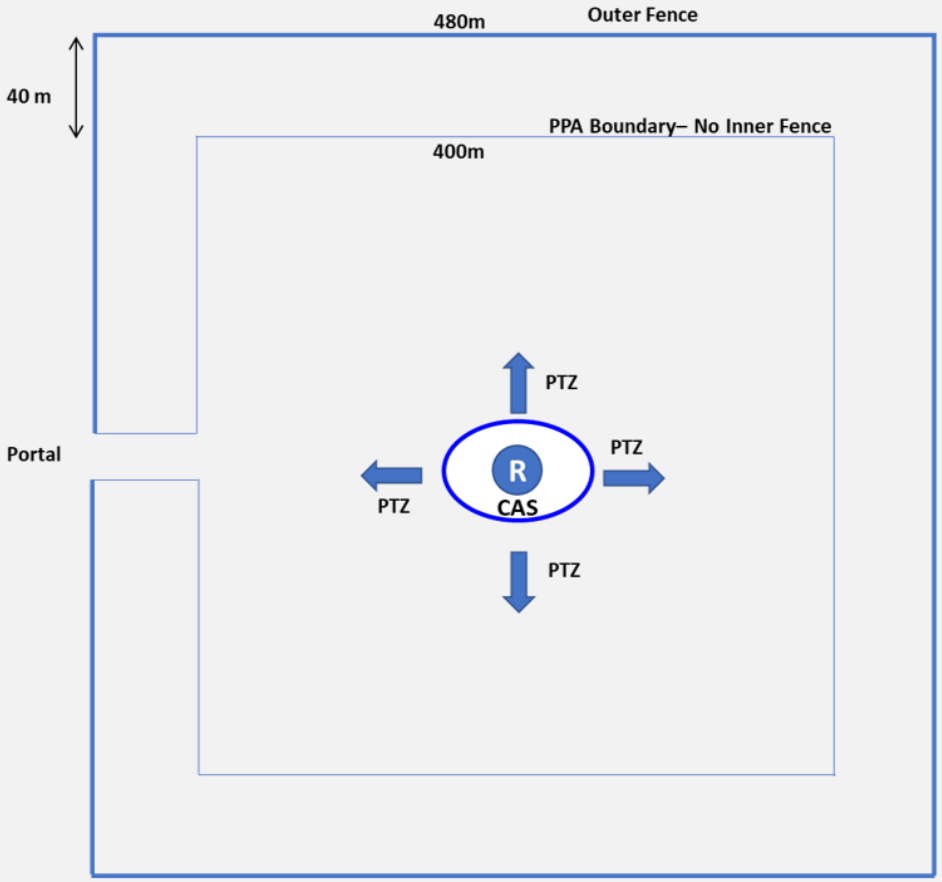
DMA Enabled New Security Architectures
Advanced Reactor Security by Design

- 400 m sides PPA* boundary
- 17 sectors – 16 plus 1 for access portal
- 34 microwaves
- 17 cameras
- 8 FDBs**
- 48 lights/light poles
- Trenching for power/comms
- 3,280 m (10,800 ft) fence line

Traditional Intrusion Detection System



New Intrusion Detection Architecture

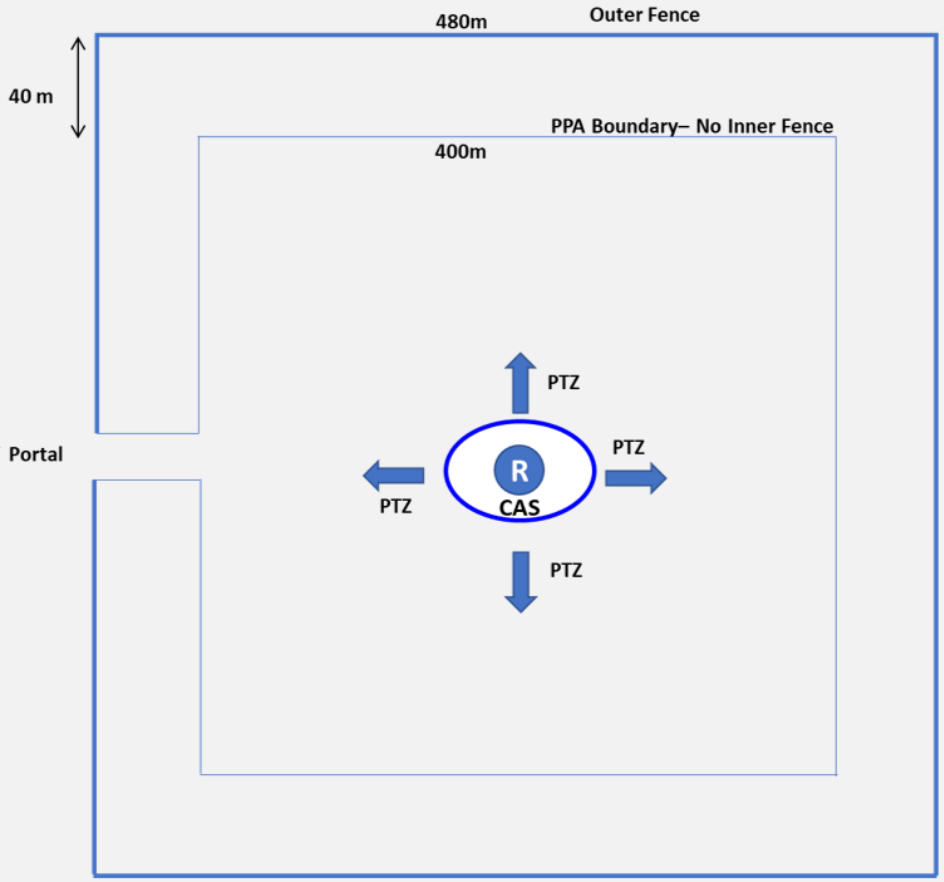


*PPA – Property Protection Area
**FDB – Field Distribution Box

DMA Enabled New Security Architectures
Advanced Reactor Security by Design

- 400 m sides PPA* boundary
- No lights
- No trenching power for lights
- No trenching power for sensors
- No trenching for comms
- No inner fence
- No FDBs*
- 1,920 m (6,340 ft) fence line

New Intrusion Detection Architecture



Estimated 40% reduction in costs

*PPA – Property Protection Area
**FDB – Field Distribution Box