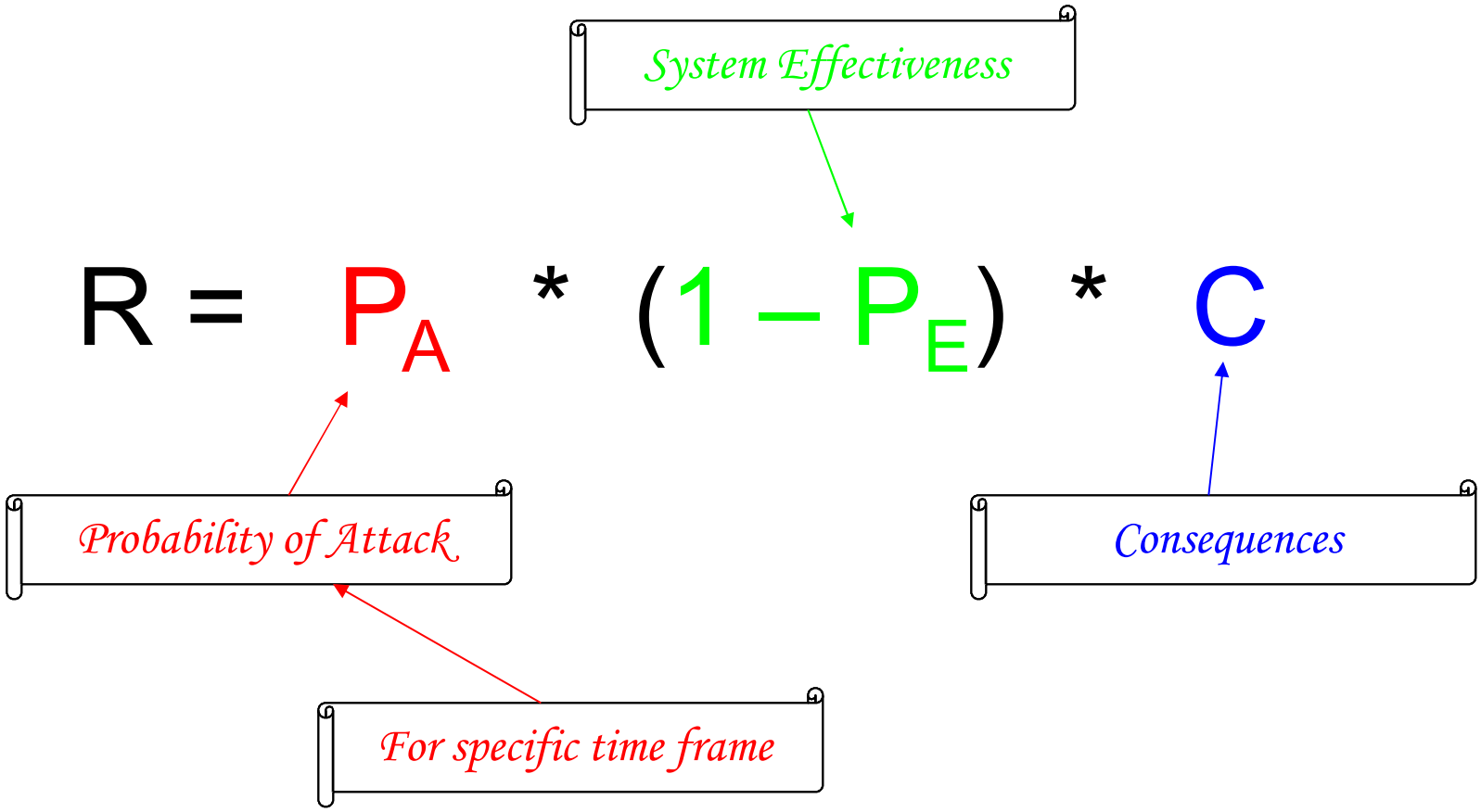
SAND2007-1958C

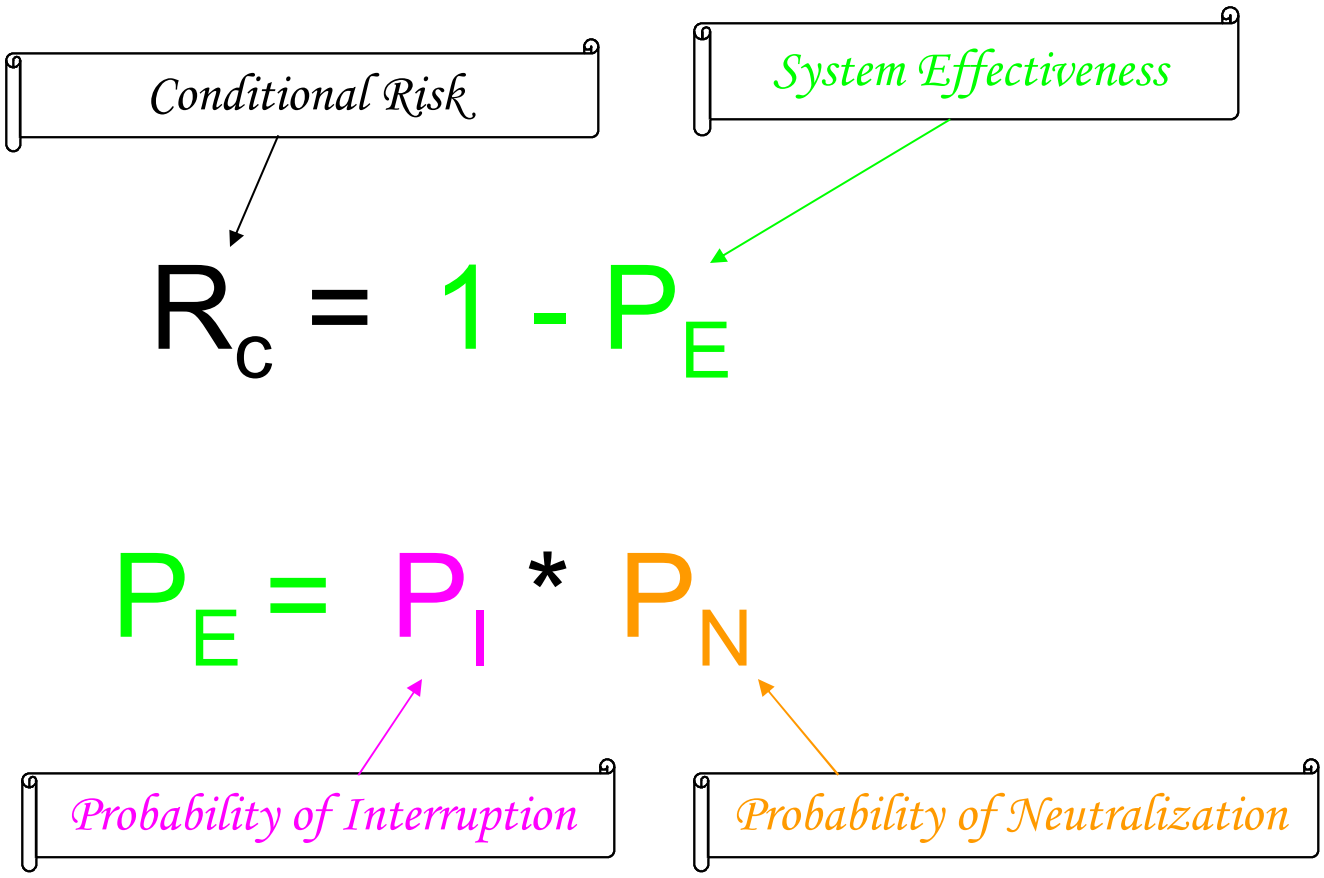
Integrated $\mathcal{P}_E$ Tool ($I\mathcal{P}_E T$)

Presented to the SCG
March 22, 2007

Nate Roehrig/Mark Snell
Manoj Bhardwaj

Brief background of risk equation

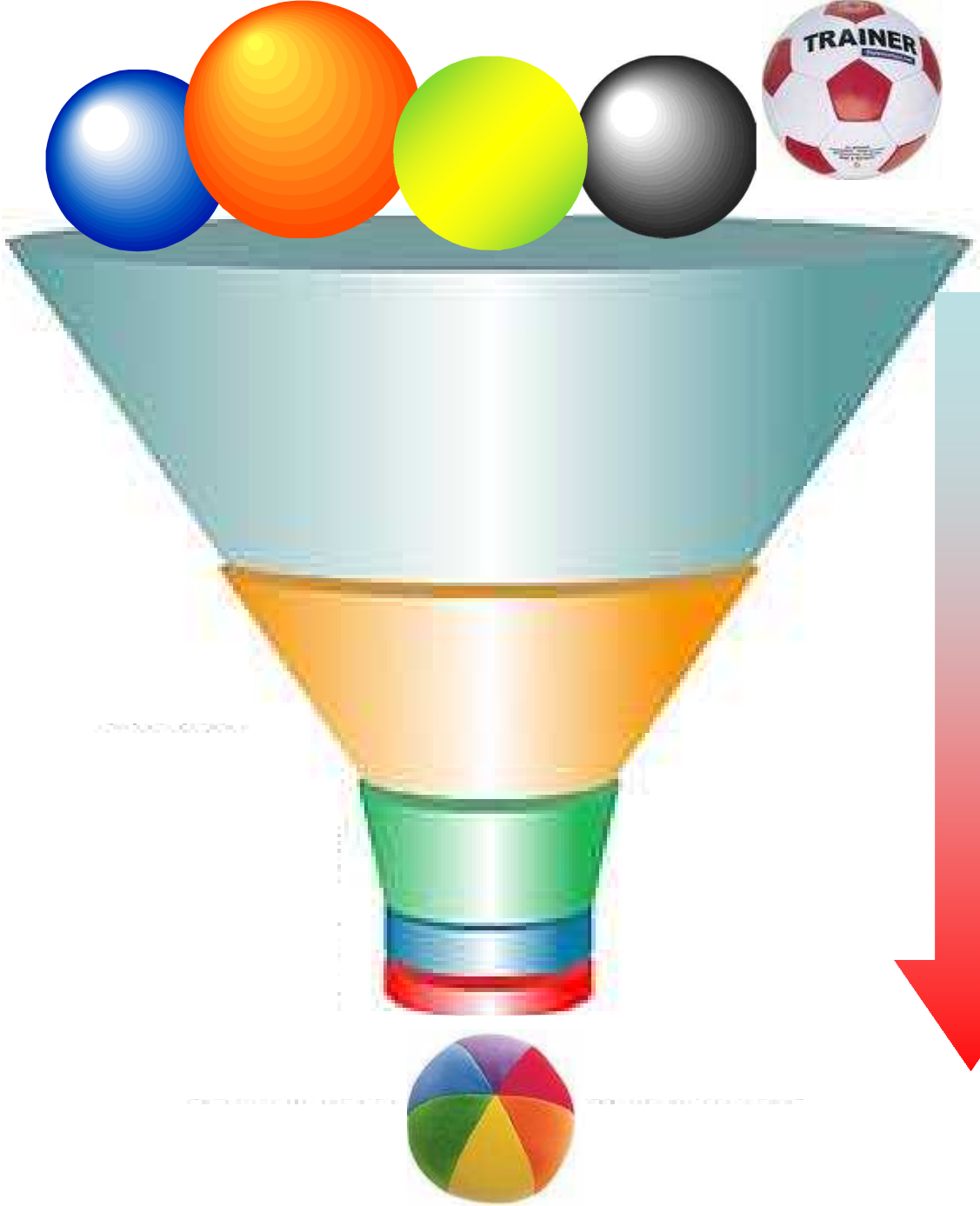

System Effectiveness
R = P_A * (1 – P_E) * C
Probability of Attack
Consequences
For specific time frame


Conditional Risk
System Effectiveness
$R_c = 1 - P_E$
$P_E = P_I * P_N$
Probability of Interruption
Probability of Neutralization

Vulnerability Analysis

- ASSESS/ATLAS used for P_I
- JCATS used to help determine P_N
- Most vulnerable paths should minimize P_E
- Historically, we minimize P_I

SCENARIO FUNNEL



ATLAS/ASSESS

AVERT

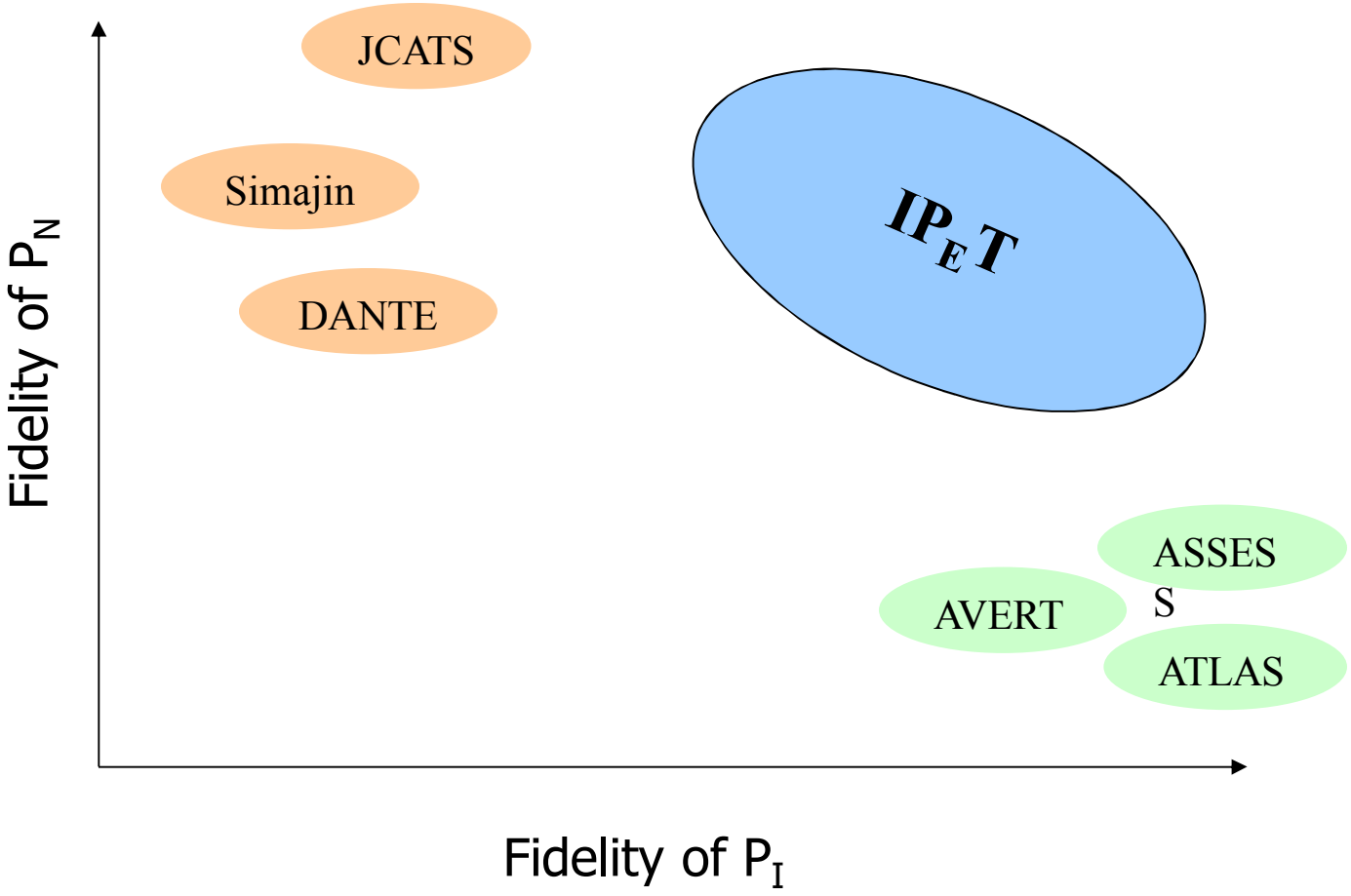
JCATS

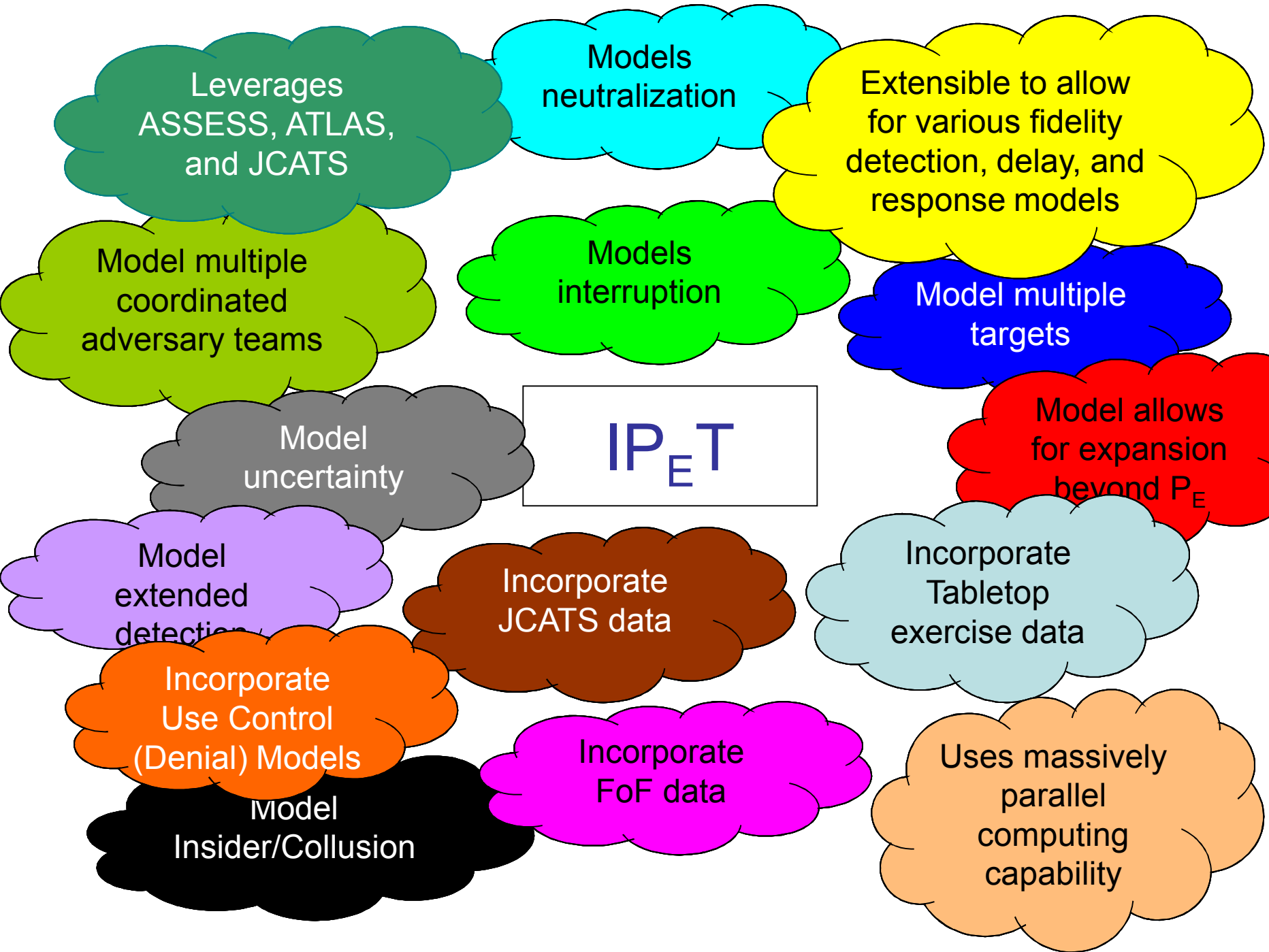
DANTE/SIMAJIN

Tabletops/FoF

Vision of IP_ET

- How does VPEDS (or your favorite technology) help the overall physical security system?
- Given $3M, what investments should we make to use these resources optimally in improving the overall physical security system?
- Should we invest in technology (one time fixed cost + maintenance) or man power (recurring cost)?


JCATS
Simajin
DANTE
IPET
ASSES
S
AVERT
ATLAS
Fidelity of P_N
Fidelity of P_I


Leverages ASSESS, ATLAS, and JCATS
Models neutralization
Extensible to allow for various fidelity detection, delay, and response models
Model multiple coordinated adversary teams
Models interruption
Model multiple targets
Model uncertainty
IPET
Model allows for expansion beyond PE
Model extended detection
Incorporate JCATS data
Incorporate Tabletop exercise data
Incorporate Use Control (Denial) Models
Incorporate FoF data
Model Insider/Collusion
Uses massively parallel computing capability

IP_ET Demo