XDtec Technical Services

www.xdtec.co.uk

Threat Definition and Performance Evaluation for Multi-Technology Integrated Explosives and Weapons Detection Systems

Tim Sheldon BSc, CPhys

XDtec Technical Services

tim.sheldon@xdtec.co.uk

Multi-technology detection systems

Systems comprising multiple detection technologies are typically used to:

- Provide comprehensive detection capability
  Explosives detection + metal detection
- Increase speed by using faster systems to pre-screen for slower, more accurate systems
  Walk-Through Metal Detector followed by manual search
- Improve detection accuracy and hence detection capability by combining "orthogonal" techniques
  Millimetre wave imaging + standoff trace

Individual components may be unconnected (today) or "data fused" (future) for centralised, automated decision making (1,2).

System design issues

Explosives and weapons detection devices are designed, used and tested as standalone items, not components. An electronic engineer uses components whose performance is presented in a standard form, based on standard test methods.

The engineer designing a multi-technology explosives and weapons detection system has components – the individual detection devices – which are typically tested in a range of non-standard tests, against a range of threats and in measurement "dimensions" which are different for each type of equipment.

- Hold baggage screening – probability of detection/probability of false alarms for charge mass and shape (% probability)
- Trace Detection – minimum detectable quantity (nanograms)

Lab v operational performance

Devices used operationally do not usually perform as well as they did in laboratory testing because of:

- Environment
  Cold, heat, dirt, moisture
- Human factors
  Operator skill, inconsistency in calibration and use

The problem is acute in devices which rely on a human operator to interpret an image.

The actual performance of equipment in the field is often unquantified. Although some regulators carry out covert field testing, this is done differently to lab testing, so results are hard to feed back into design.

Security

The methods and results of the most comprehensive testing – by government agencies - are often not available to the designer because of:

- Security: publication of test standards could help the terrorist/criminal to beat the system
- Fear of suppliers designing devices to pass the test, rather than aiming for a comprehensive detection capability

Standards

Device suppliers, researchers, system designers, end users and regulators need access to standard test methods which are:

- Realistic and reproducible
- Allow different technologies to be compared
- Allow operational test results to be fed back into system design
- Doesn't give away confidential information

The key first step in standardising test methods is defining the **Threat**

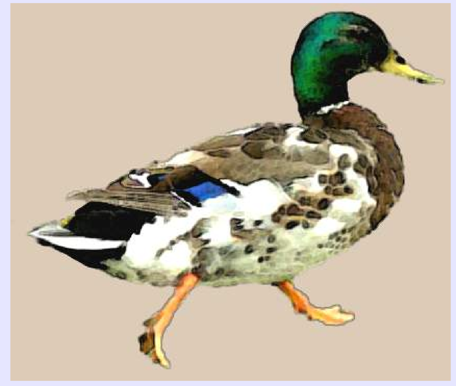
Multidimensional threats

A threat such as an IED has multiple "dimensions" - characteristics which affect it's detection by different techniques. A person-borne improvised explosives device, for instance, can be characterised by dimensions such as:

- Appearance
- Position of bomb on body
- Metal content
- Explosive type
- Explosive mass
- Trace contamination (quantity and location)
- Vapour emissions (concentration & source location)
- Body shape
- Clothing

Detection dimensions

"If it looks like a duck, and quacks like a duck, it's a duck!"

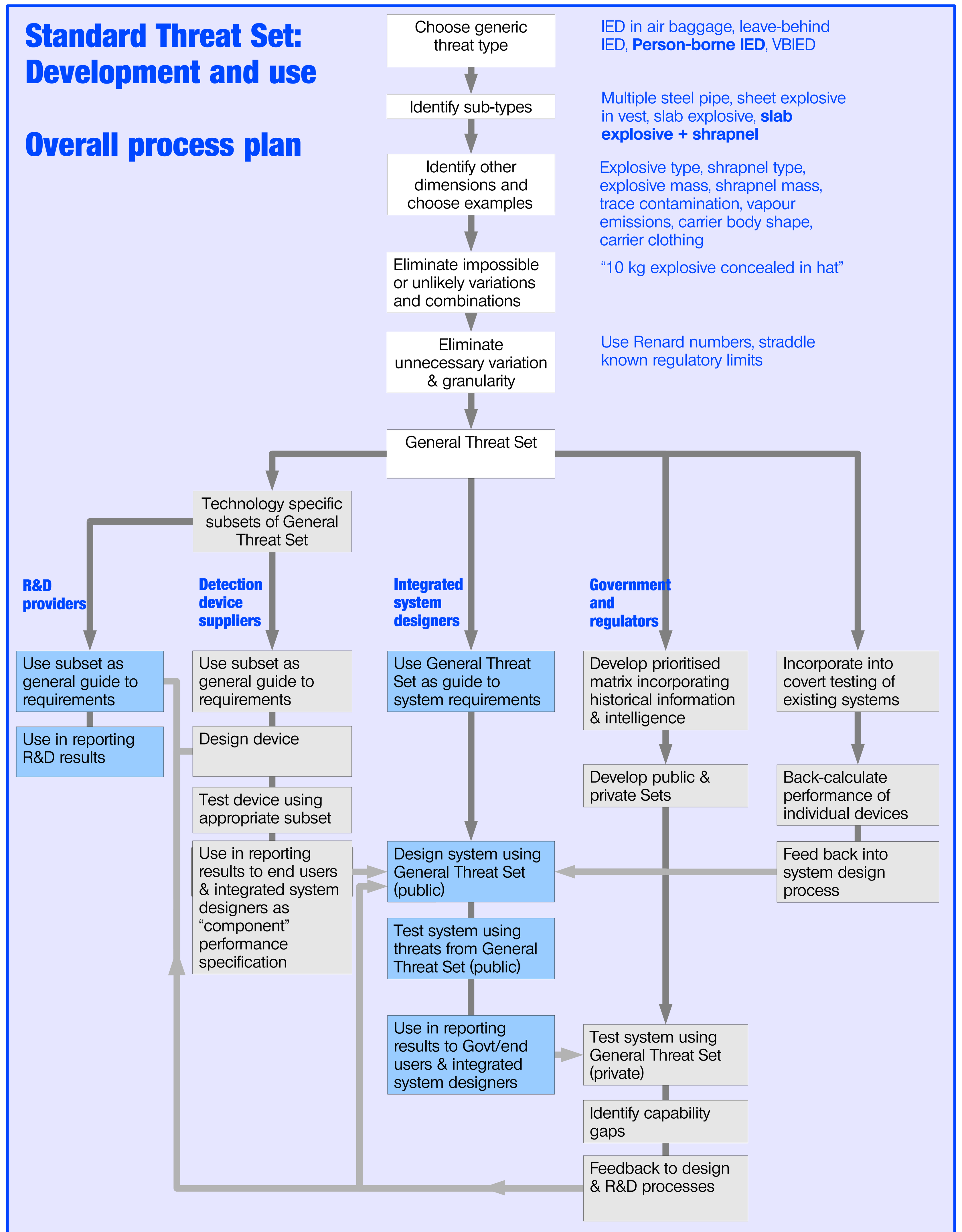


- We could build a duck detector which detected a duck by its appearance
- Or we could detect its call
- Either device would be likely to make some errors and produce false alarms on birds that resembled ducks or sounded like ducks
- Combining the two "dimensions" of appearance and call (so to get an alarm we need to detect a duck-like appearance AND a quack) would produce a much lower false alarm rate (PFA)
- We could consequently increase the sensitivity of either or both detectors to increase the probability of detection
- These two dimensions are effectively **orthogonal** because they are strongly associated only in ducks – unlike, say "having feathers" and "flight" which are associated in many birds

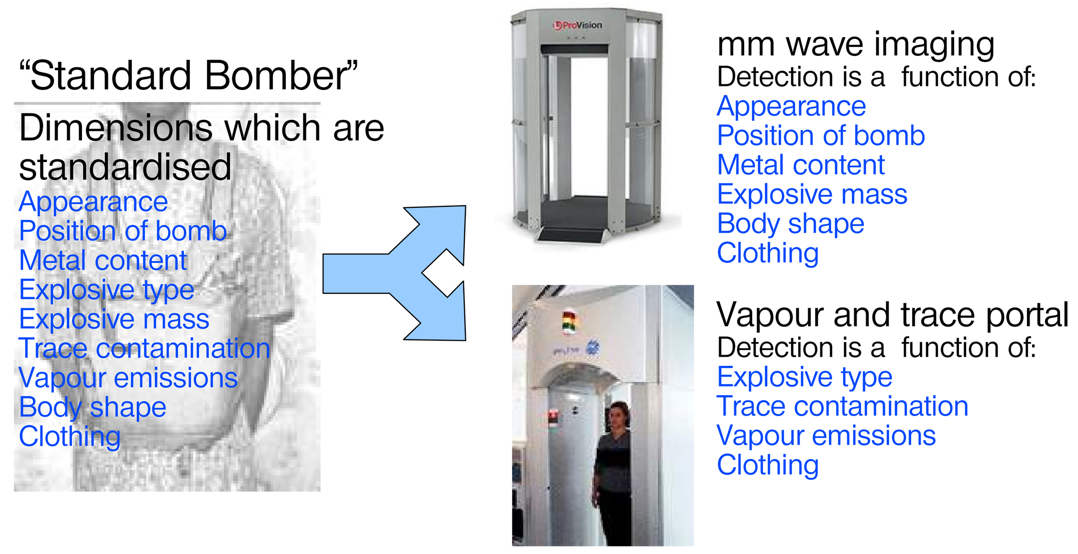
PD (Duck) = PD (Duck looks) x PD (Quack)
PFA (Duck)=PFA (Duck looks) + PFA (Quack) – PFA (Duck looks) x PFA (Quack)

Standard Threat Set: Development and use

Overall process plan



Multi-technology threat detection



Overall detection probability can be predicted for the Standard Bomber if the response of each detection device to a subset of the Standard Bomber's dimensions is known.

So Standard Bomber has to be "mm wave correct" and "vapour and trace correct"

Challenges in producing a Standard Threat Set

The process of producing the Threat Set needs to balance:

- Realism **v** Complexity
- Need for gradation **v** excessive numbers of tests

Who designs the Threat Set?

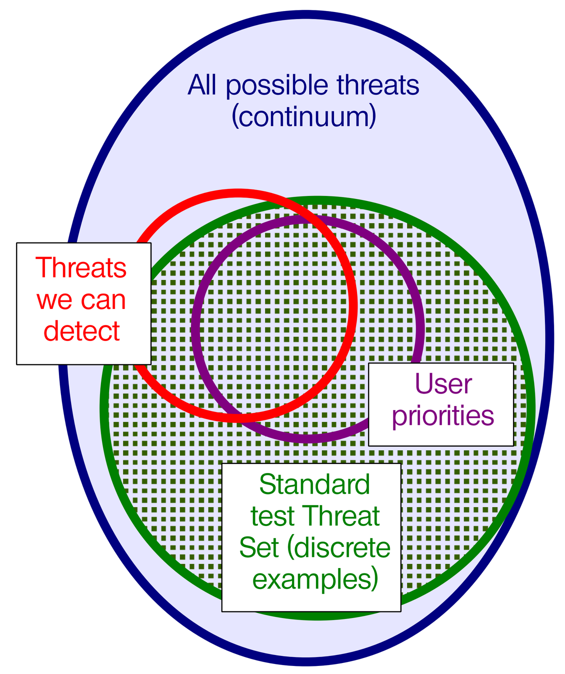
- Industry or government?
- Limited benefit for a single company
- Government risk disclosing confidential criteria
- Possibly joint approach like IWPC millimetre wave test protocol (3)

How to report test results?

- Threats have more than three dimensions and combined systems will look at a wide range of dimensions

Taking into account user needs

- Standard test Threat Set is independent of users
- Threat set encompasses and "straddles" typical user needs
  eg. use explosives quantities both above and below user's standard thresholds
- Supplier tests own equipment, reports results against Threat Set in a matrix
- User attaches a priority weighting to each threat which modifies the result matrix – weightings are user specific and need not be disclosed
- User can apply past experience and intelligence in calculating priorities



Conclusions

Design of multi-technology systems requires a working definition of threat as a key system requirement. To facilitate testing of component devices, a Standard Threat Set should be developed which:

- Includes a wide range of threat objects defined and graded in terms of their "Detection Dimensions", the properties that enable detection by different techniques
- Is bigger in scope than, but encompasses, the requirements of any individual user

This Threat Set should be used by suppliers to specify performance, system designers to predict system performance, users to match performance against requirements and regulators to design more meaningful operational testing

References

1. Existing and Potential Standoff Explosives Detection Techniques Committee on the Existing and Potential Standoff Explosives Detection Techniques, National Research Council, 2004
2. Fusion of Security System Data to Improve Airport Security, Committee on Assessment of Security Technologies for Transportation, National Research Council, 2007
3. IWPC Millimeter-Wave Security Sensor Test Protocol, International Wireless Industry Consortium, 2008