



IT Solutions for Public Transport
**International Conference
and Exhibition**

18 - 20 February 2014
Karlsruhe Trade Fair Center
Germany

Human Factor in Video Analytics

Jeroen van Rest
Sr Consultant Security,
Sensors & Privacy

TNO innovation
for life

Patronage

Alexander Dobrindt MdB



Federal Ministry
of Transport and
Digital Infrastructure

Organisers



ADVANCING
PUBLIC
TRANSPORT



CONNECTING IDEAS.
Karlsruhe -
Messen und Kongresse

Behaviour is a constellation of actions and reactions



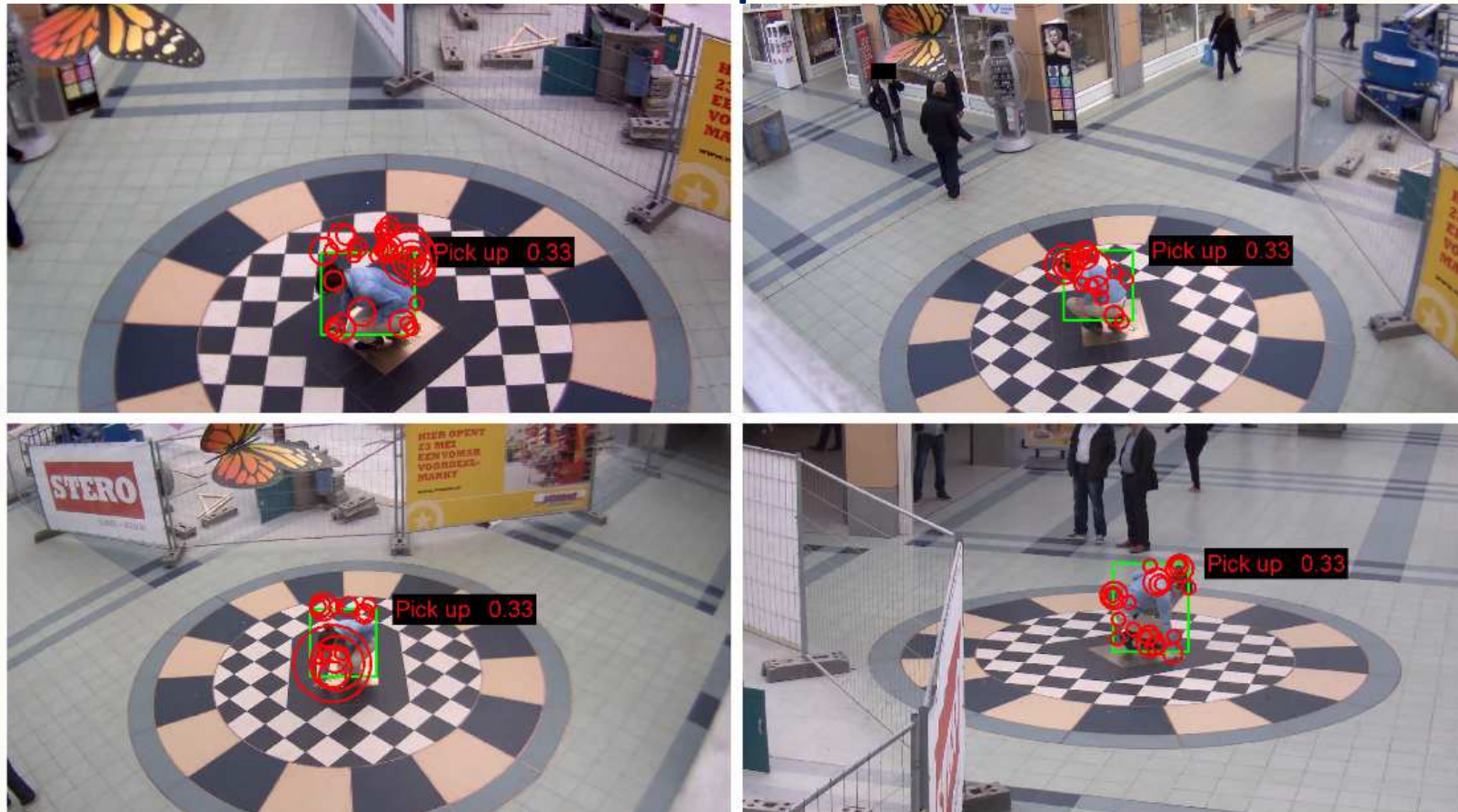
~10% improvement per additional viewpoint (tracking)



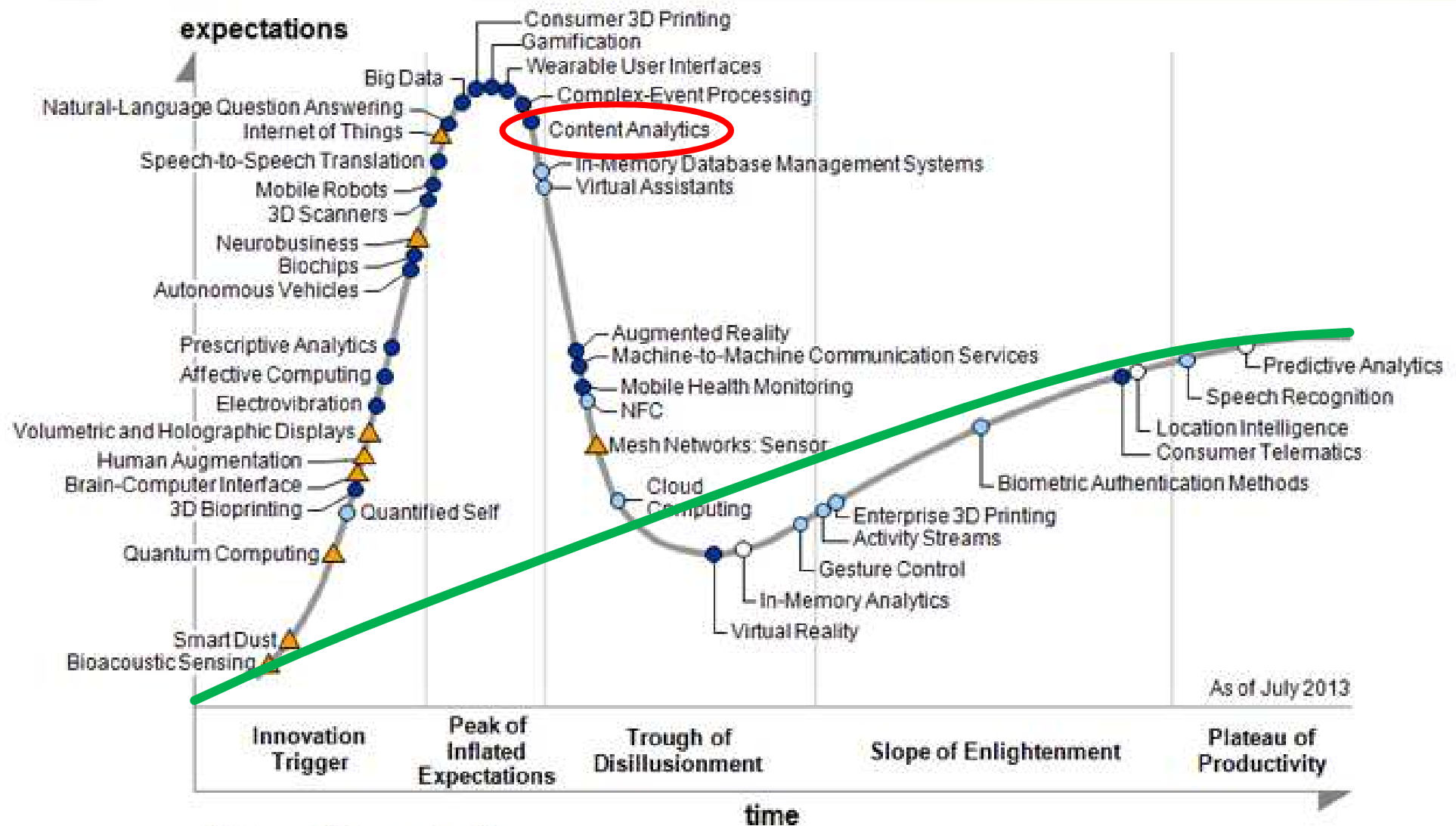
~10% improvement per additional
viewpoint (behaviour)



Video of Kanaleneiland-experiment



Cannot be distributed, and only be shown live because of the privacy of passers-by



Hype cycle for Emerging Technologies 2013; Source: Gartner August 2013

Mature content analytics

Examples:

- Intrusion detection
- Identification in controlled situations (ANPR and Biometrics)
- People counting
- Loitering

➔ Simple, small scenes.

Threats in crowded situations

- Aggression, shoplifting, pickpocketing, left luggage, swindling and drug dealing;
- Organised crime or even terrorism (more for police);
- Slow passengers, young unsupervised kids, rowdy youth and monitoring the (correct) use of company assets.
 - ➔ complex, dynamic scenes: interaction between people is key for understanding the scene

Threat mitigation

- Preparation (intelligence, testing, red-teaming, exercises);
- Prevention (prediction, nudging, “show the force”);
- Caught in the act (detection, recognition);
- Crisis response (live monitoring);
- Investigative (forensics, identification);
- Acceptance (liability);

Later in the incident → increasing costs

Technological developments

- Limited coverage → Continuous multi-viewpoint omnidirectional coverage
- Fixed → Moving camera platforms
- Single person → Crowded scenes
- Optimal lighting → Poor lighting
- Single modality → Fusion of multiple modalities

Allowing for:

- (1) Surveillance on free flow of people, and therefore in one sense less invasive surveillance;
- (2) Early detection of weak signals;

Predictive behaviour profiling

- Not based on ethnicity, age, gender, origin
- Based on behaviour
- Before the incident

“Deviant behaviour”

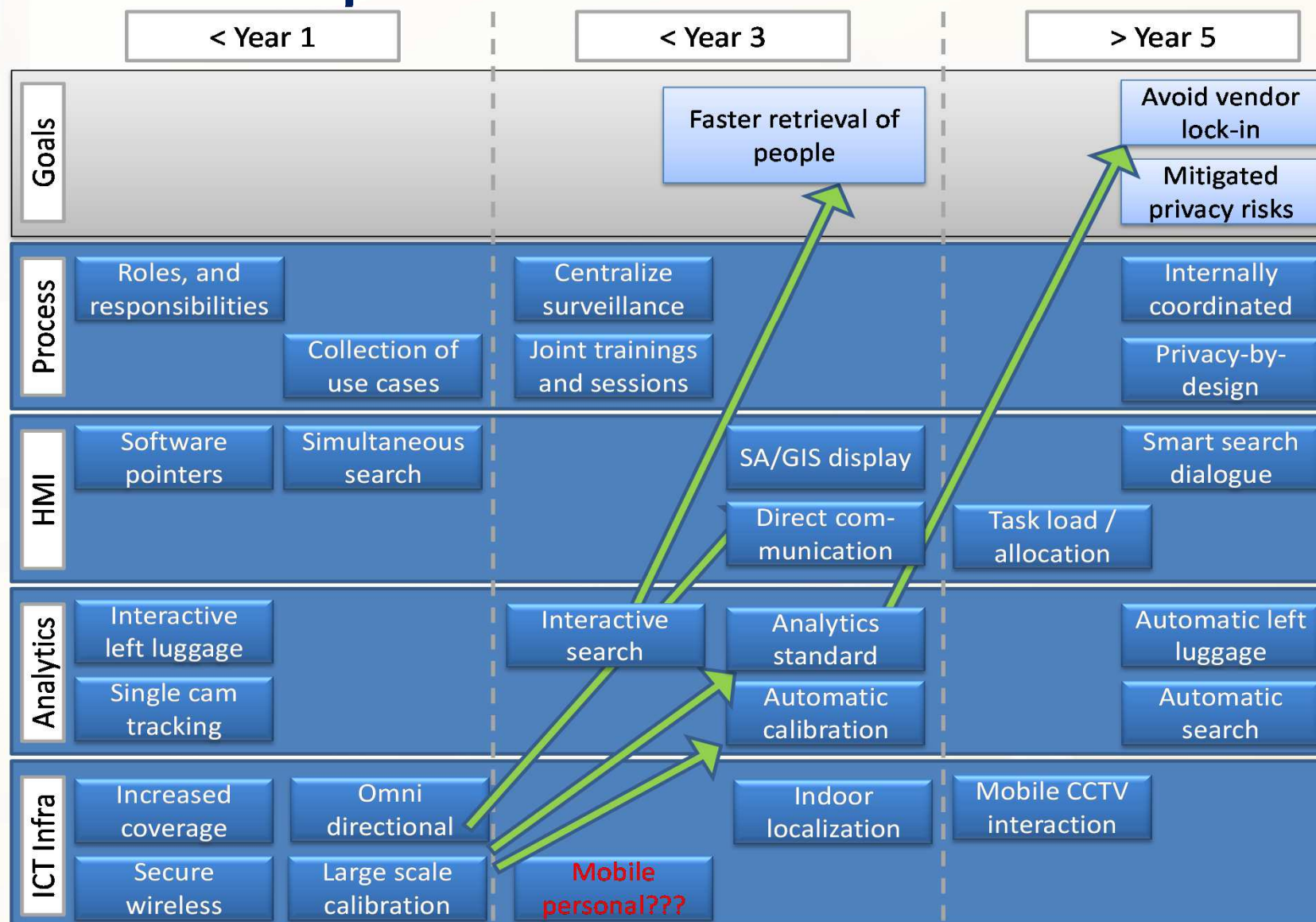
- Profiles of situations and social scenario's based on historical data, and / or ...
... based on expert knowledge.

Effective video analytics for deviant behaviour



1. **Garbage-in is garbage-out**: camera coverage, viewpoints, quality of cameras and network. You cannot fix something that is fundamentally broken.
2. The performance of video analytics improves with **~10% per additional viewpoint** on the scene, if the relative positions of cameras are accurately known.
3. **Behaviour is a constellation of actions and reactions**. A single action in a complex environment says nothing and only leads to false alarms. Therefore, tracking and recognition are essential. Identification however is too much detail and introduces unnecessary privacy risks.
4. **Test data** is needed. Because of privacy concerns few and old sets are publicly available. We have built a video database of pickpockets: 30 incidents amidst normal shopping behaviour. You are invited to join this effort.
5. **This kind of technology potentially increases specific biases**. Privacy by Design is still in its infancy, both as a policy instrument, and as a technical tool. We develop Privacy Enhancing Technologies such as dynamic masking and encrypted metadata databases to actively detect and mitigate biases and privacy risks.
6. A **technology roadmap** to introduce this kind of technology in your organisation should address policies, work processes, user interfaces, analytics and ICT infrastructure.

Roadmap



TNO Offer

- To let you share in the accumulation of knowledge of deviant behaviour in the context of public transport (modi operandi and test datasets);
- To describe a realistic roadmap for the introduction of advanced video analytics in your organisation(s);
- To develop high end video analytics for the prevention of incidents;

References

Selected papers

- Bouma, Henri, et al. "Real-time tracking and fast retrieval of persons in multiple surveillance cameras of a shopping mall." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.
- Sanromà, Gerard, Gertjan Burghouts, and Klammer Schutte. "Recognition of long-term behaviors by parsing sequences of short-term actions with a stochastic regular grammar." *Structural, Syntactic, and Statistical Pattern Recognition*. Springer Berlin Heidelberg, 2012. 225-233.
- Burghouts, Gertjan J., and J-W. Marck. "Reasoning about threats: From observables to situation assessment." *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 41.5 (2011): 608-616.
- Bouma, Henri, et al. "Recognition and localization of relevant human behavior in videos." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.
- Burghouts, Gertjan J., and Klammer Schutte. "Correlations between 48 human actions improve their detection." *Pattern Recognition (ICPR)*, 2012 21st International Conference on. IEEE, 2012.
- Burghouts, G. J., et al. "Selection of negative samples and two-stage combination of multiple features for action detection in thousands of videos." *Machine Vision and Applications* 25.1 (2014): 85-98.
- Bouma, Henri, et al. "WPSS: Watching people security services." *SPIE Security+ Defence*. International Society for Optics and Photonics, 2013.
- Bouma, Henri, et al. "Re-identification of persons in multi-camera surveillance under varying viewpoints and illumination." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2012.
- Rest, J., et al. "Sensors and tracking crossing borders." *In Proceedings of the 4th Conference on Safety and Security Systems in Europe*. 2009.
- van Rest, Jeroen, et al. "Designing Privacy-by-Design." *Privacy Technologies and Policy*. Springer Berlin Heidelberg, 2014. 55-72.
- Burghouts, Gertjan J., and J-W. Marck. "Reasoning about threats: From observables to situation assessment." *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 41.5 (2011): 608-616.
- Lefter, I., L. J. M. Rothkrantz, and G. J. Burghouts. "A comparative study on automatic audio-visual fusion for aggression detection using meta-information." *Pattern Recognition Letters* 34.15 (2013): 1953-1963.
- Andersson, Maria, et al. "Activity recognition and localization on a truck parking lot." *Advanced Video and Signal Based Surveillance (AVSS)*, 2013 10th IEEE International Conference on. IEEE, 2013.
- Bouma, Henri, et al. "Behavioral profiling in CCTV cameras by combining multiple subtle suspicious observations of different surveillance operators." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.
- van Rest, J., et al. "Requirements for multimedia metadata schemes in surveillance applications for security." *Multimedia Tools and Applications* (2013): 1-26.
- Bouma, H. et al, (2014) Integrated roadmap towards fast finding and tracking people at large airports (*in review*)
- Rest, et al (2014) *Deviant Behaviour*, TNO Report (*in re view*)

Selected patents

- [System and method for identifying image locations showing the same person in different images](#)
- [US2013163819 \(A1\) - SYSTEM AND METHOD FOR IDENTIFYING IMAGE LOCATIONS SHOWING THE SAME PERSON IN DIFFERENT IMAGES](#)

Reserve slides

Nine definitions of deviant behaviour (1-4): threat based

- Behaviour which may lead to dangerous and/ or undesired situations, i.e. which threaten the continuity of the processes at the location;
- Behaviour which correlates significantly with incidents;
- Behaviour which is part of the modus operandi of a criminal act;
- Behaviour which has as purpose to gain an advantage for one self at the cost of someone else: unethical behaviour;

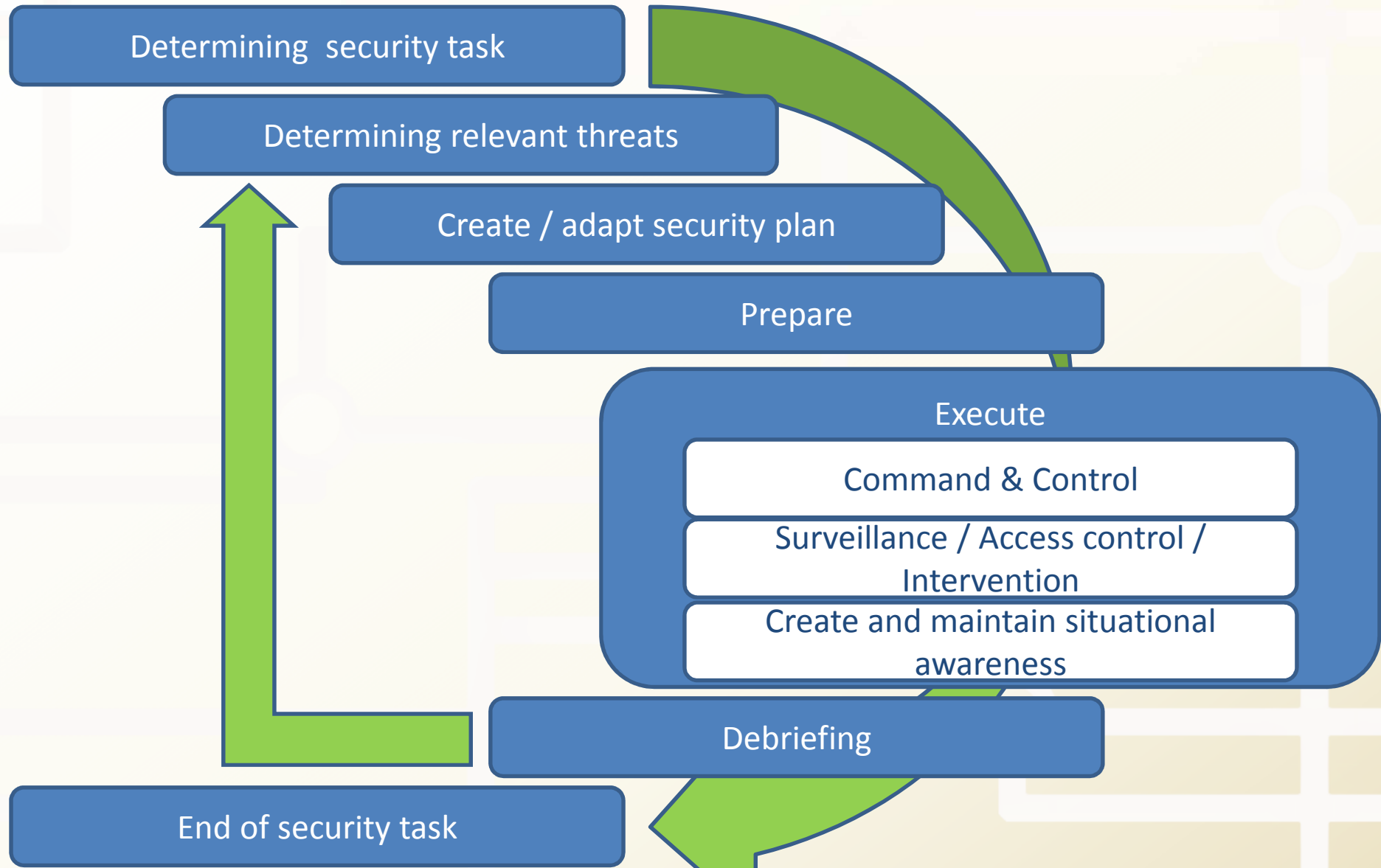
Nine definitions of deviant behaviour (5-9): continuity based

- Behaviour which is not part of any of the allowed (work-)processes which occur at the respective location or object;
- A reaction which does not fit to the stimulus if the intent of the subject were benign;
- Behaviour which falls outside the normal distribution of behaviour at the respective location;
- Behaviour which is unwillingly displayed due to high cognitive pressure;
- Behaviour which does not fit the local social norms, including anti-social behaviour and culturally abnormal behaviour.

Inequal definitions

- either threat-based, or continuity-based;
➔ fighting crime and public order management;
- the efficacy of applying some of these definitions (6-9) has not been thoroughly validated. Their application should therefore not be done lightly.
 - E.g. USA TSA SPOT Program

Concept of Operations



Deviant behaviour in ConOps

ConOps Step	Application of knowledge of deviant behaviour
Determining security task	Specify the object of security, its context and environment; Specify relevant normal behaviour, among them, but not limited to, the work processes of which the continuity must be protected; Specify levels of transparency, accountability, efficacy en efficiency;
Determining relevant threats	Specification of threats in specific modus operandi
Create or adapt security plan	Selection of definitions of deviant behaviour; Selection of methodology for specifying deviant behaviour (profiles); Specify deviant behaviour (e.g. with the help of local observation), including validation of this specification in the respective environment and contact; Creation of a security plan which can monitor, detect, recognize and identify these behaviours with satisfactory accuracy, in the desired phases of security (prevention, in-the-act, investigation).
Prepare(implementation of security plan, training)	Training of personnel in face to face behavioural profiling; Install security measures;
Execute	Secure the object of security on an operational level
Command & control	Introduce real life training simulations (“red teaming”, etc.); Periodic management reporting about efficacy, costs and impact on the liberty of the object of security;
Surveillance, Access control, intervention	Detection of normal and deviant behaviour; When intervening, take inaccuracy of surveillance into account with regard to the intentions of subjects;
Create and maintain situational awareness	Detection of relevant new normal and deviant behaviours; Determining that a certain threat is occurring;
Evaluation (debriefing)	Update knowledge of normal behaviour and processes, and of known modus operandi; Identify flaws in security plan;
End of security task	Transfer and store knowledge w.r.t. actual incidents and discovered modus operandi for next security task, i.e. facilitate learning;

Biases in surveillance

Bias name	Description
Funding bias	The tendency of scientists (and of police and intelligence officers?) to prevail the outcome of studies which support the interest of (financial) sponsors.
Law of the instrument	Too much trust in a specific tool or resource
Positive feedback	A self-influencing effect in a system.
Recall bias	The systematic error that people make when remembering events.
Reporting bias	The error that people make when reporting events.
Surveillance bias	The phenomenon where people pay more attention to a specific selection of people than to others.
Conformity bias	The tendency of people to let prevail information which confirms their believe (case building).
Exclusion bias	The systematic exclusion of certain (types of) subjects.

Finding people

Who left the luggage?

The screenshot displays a video analysis software interface. The top section shows a large video feed of a train platform with the text "Who left the luggage?" overlaid. To the right of this feed are five smaller camera feeds labeled "cam 1" through "cam 5". The bottom section is a timeline labeled "WPS Detection Inspection" with a time range from 13:15 to 13:45. The timeline shows a series of small video frames representing detected people, with a vertical line indicating the current time. The interface includes various control buttons and a legend for the timeline.