

# Authorisation Frameworks for Airports of the Future

- Professor Emeritus Ed Dawson
- School of Electrical Engineering and Computer Science
- Institute for Future Environments
- Queensland University of Technology



# Overview

- Airports of the Future Project
- Role Based Access Control
- XACML
- Integrated Access Control for Smart Buildings using Building Information Models
- Authorisation Management in Business Process Environments
- Acknowledgement: Jason Reid, Farzad Salim, Nimal Skandhakumar, Khalid Alissa and Others

# Australian Research Council Linkage Project



## Airports of the Future

**Queensland University of Technology**

University of Technology Sydney, University of Melbourne, Edith Cowan University,  
Massachusetts Institute of Technology, Delft University of Technology.



a university for the **real** world<sup>®</sup>

regenerate engage experiment





08:50	Cornaca	BA662	Cancelled
08:50	Berlin	AA6594	Cancelled
08:50	Glasgow	GF5222	Cancelled
08:50	Palma Mallorca	LH6639	Go to Gate
08:55	Prague	CX7121	Cancelled
08:55	Moscow	BA872	Cancelled
08:55	Nice	BD193	Go to Depart
08:55	Manchester	GF5280	Cancelled
09:05	Dublin	BA5953	Cancelled
09:10	Edinburgh	AA6562	Cancelled
09:10	Rome	BA548	Cancelled
09:10	Belfast City	LH6690	Cancelled
09:10	Munich	QF3565	Cancelled
09:10	Dublin	SK9757	Cancelled
09:10	Barcelona	BA484	Cancelled
09:10	Madrid	BA458	Cancelled

# Observations

- Fuzzy requirements - Practical trialling.
- Trends:
  - Self service
  - Next generation airplanes
  - e-borders
  - Technology innovation
  - Emerging non-security technologies (mobile phone check-in, hotel check-in).
- Sweating assets.
- Despite investments, we still face seemingly trivial events with enormous repercussions.

- More recently @ Melbourne Airport, Apr 8<sup>th</sup> 2011



Travellers queue to get back through security screening at Melbourne's Tullamarine airport. Picture: Aaron Francis *Source: The Australian*

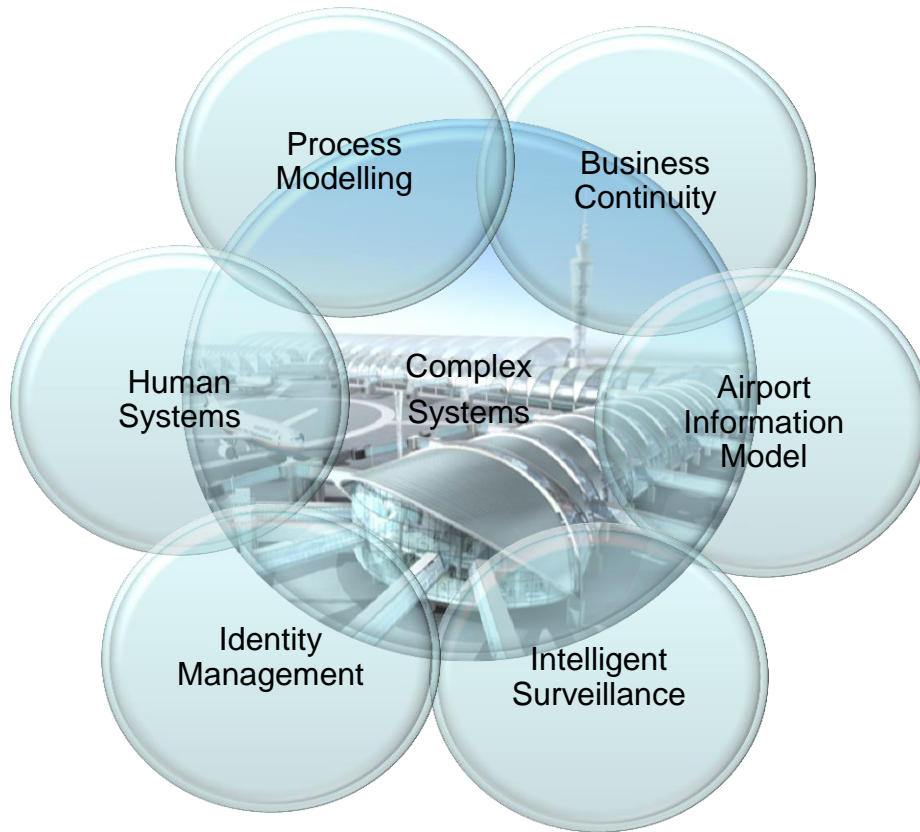
# Project Vision

...“To develop a complex systems approach for the integrated design, engineering, management and operation of airport systems” ...





# The Airport as a Complex System



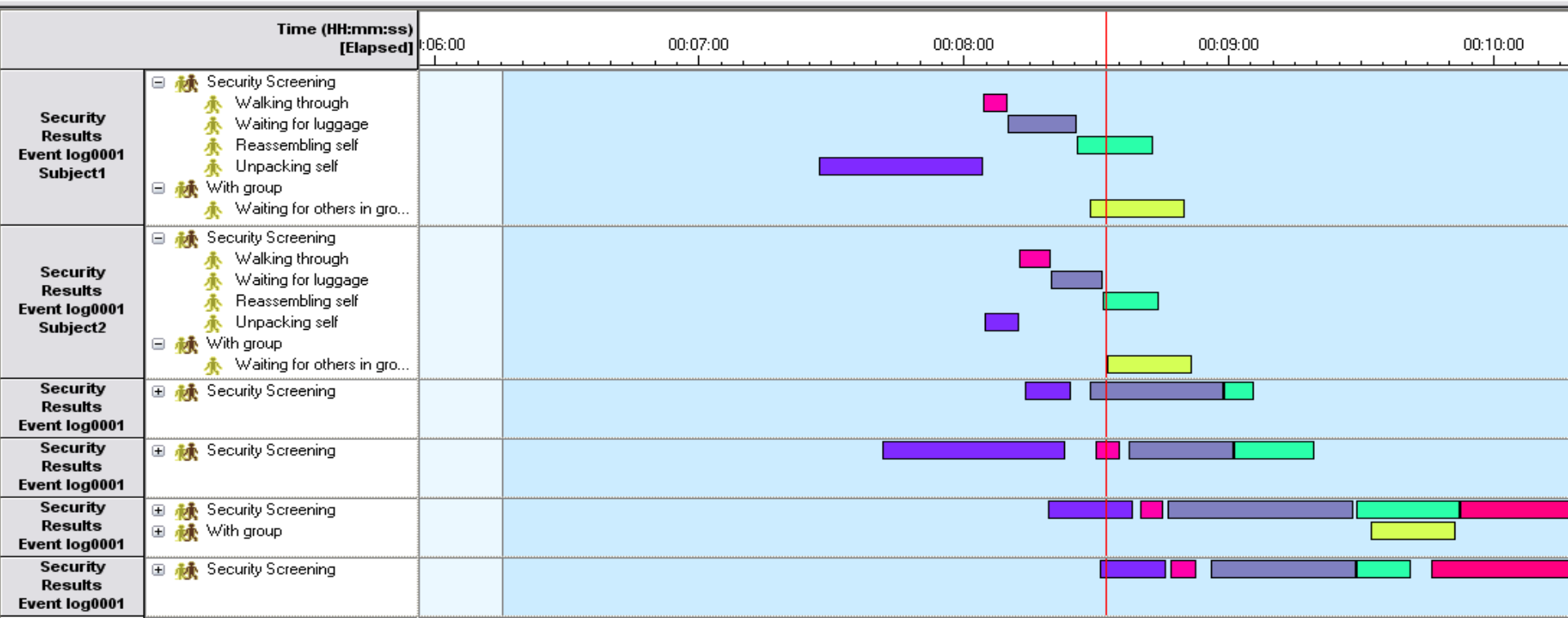
Complex, Large-Scale, Multi-stakeholder, Integrated, Open, Socio-technical System.

# Business Continuity

- Continuity planning in security-concerned complex systems.
  - Impediments to flexible business continuity management.
  - Risk-based flexible security policies.
- Emergency Response Planning
  - Correlation of emergent properties and methodologies for emergency response / recovery.
  - Alignment of emergency response and business continuity needs with transport security planning requirements.
  - Scalable Incident Response Management system.

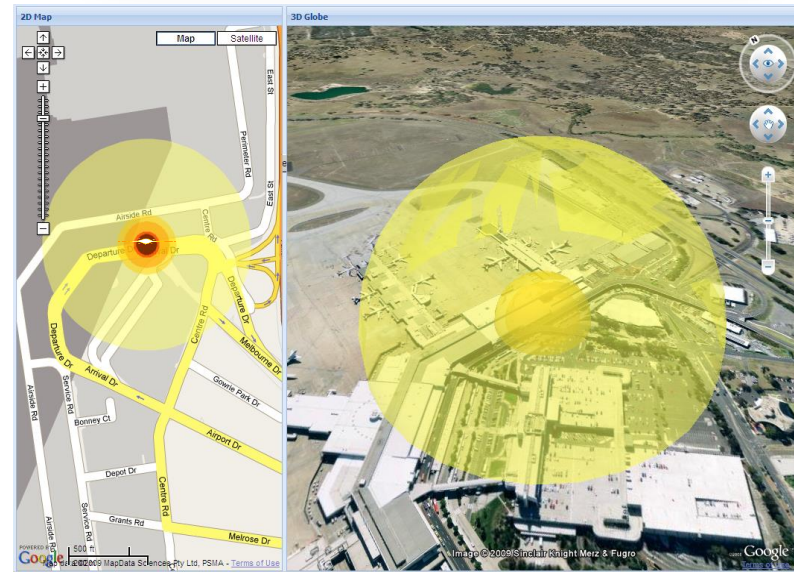
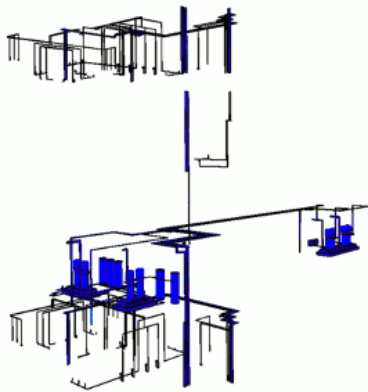
# Human Systems

- Qualitative and quantitative study of the interactions within the actors and with other system components in complex systems
- passengers' experiences and interactions at both system and domain levels



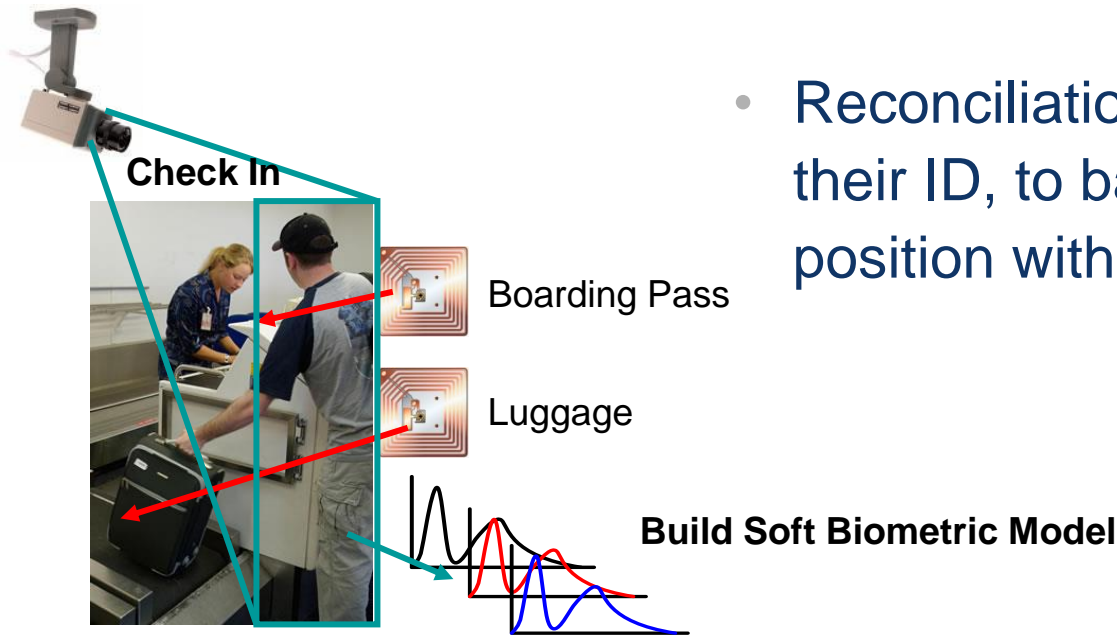
# Airport Information Model

- New platform for airport management, visualisation, operating decision support systems.
- Physical Infrastructure Protection.



# Identity Management

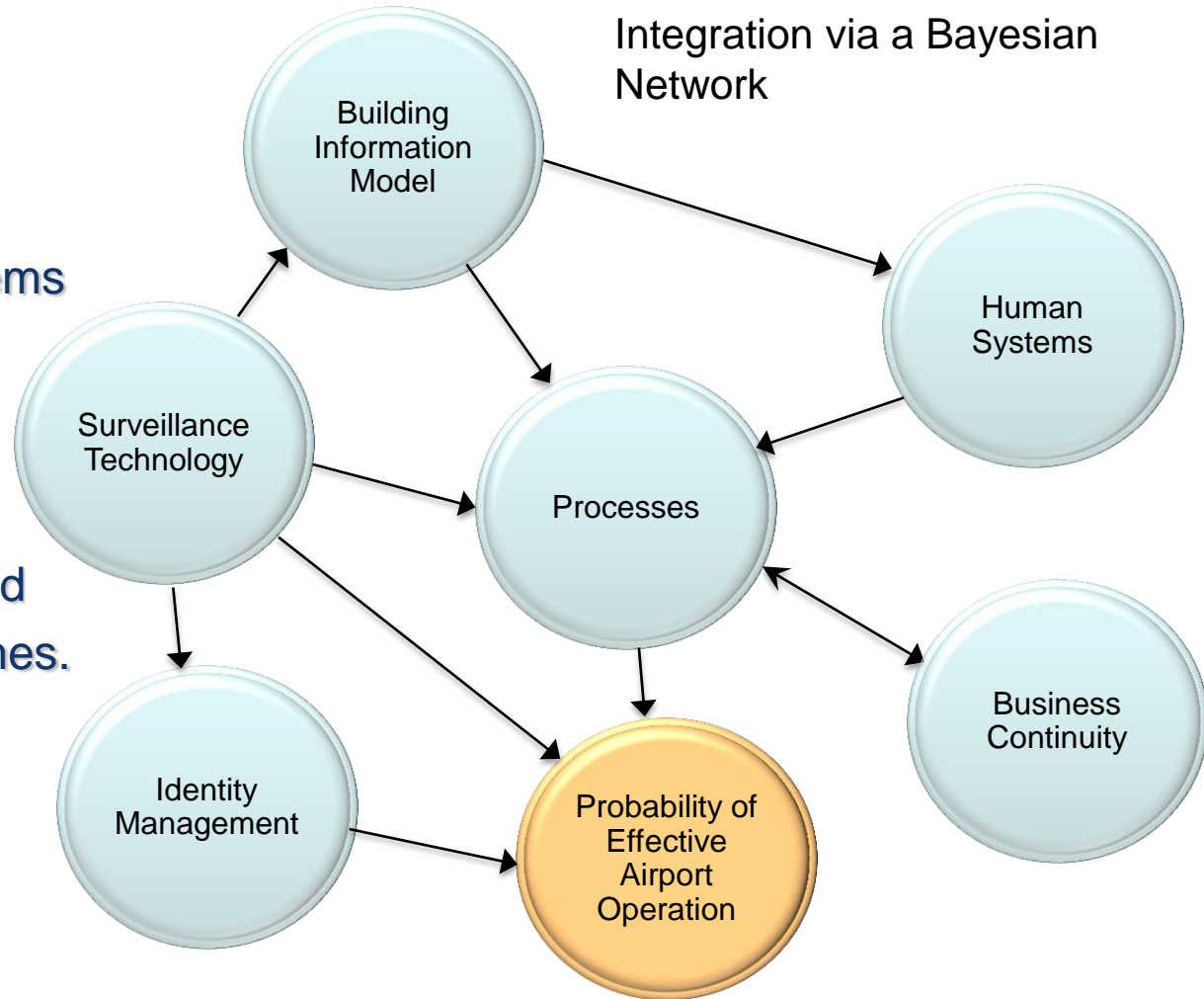
- Federated identity management systems & reference architecture for next-generation integrated airport identity management systems.



- Reconciliation to link passengers to their ID, to baggage, to physical position within terminal.

# Complex Systems

- Bayesian hierarchical models & Decision Networks to model systems and inter-dependencies.
- Cross-scale tradeoffs and shape enterprise outcomes.

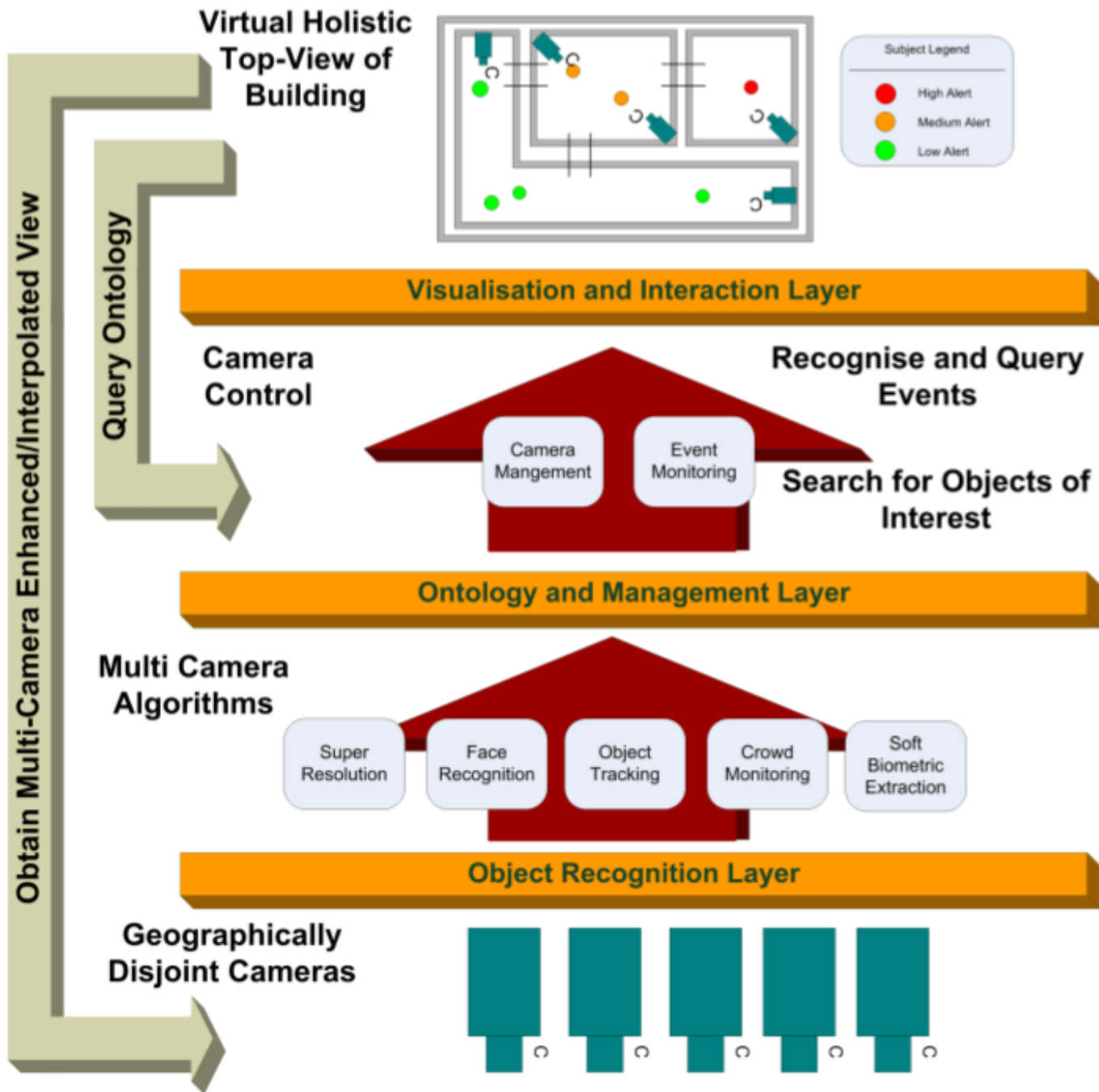


# Intelligent Surveillance



- Camera management, multi-view tracking, crowd analysis and activity recognition for screening.
- Monitoring airport effectiveness; emergent properties.





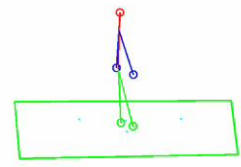
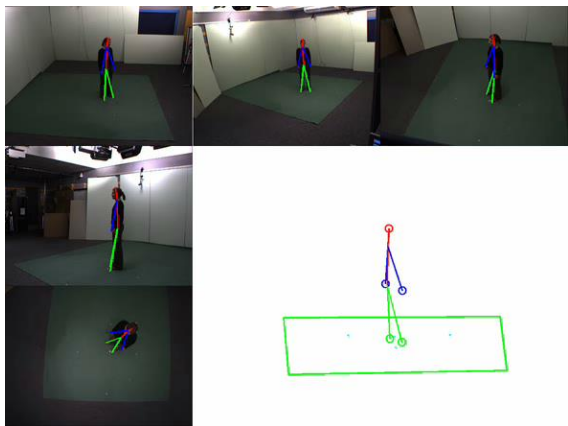
Semi-Supervised Visual Surveillance System



# Abnormal Crowd Event Detection

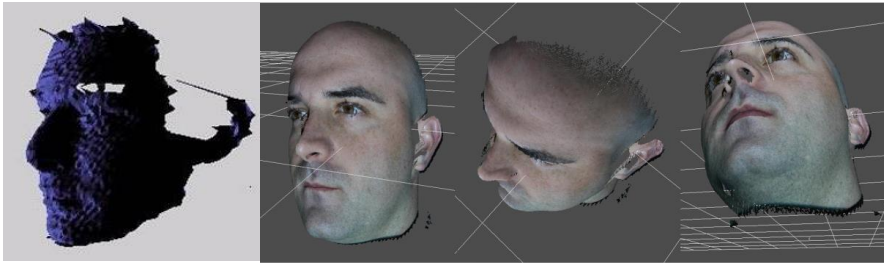


# Action recognition

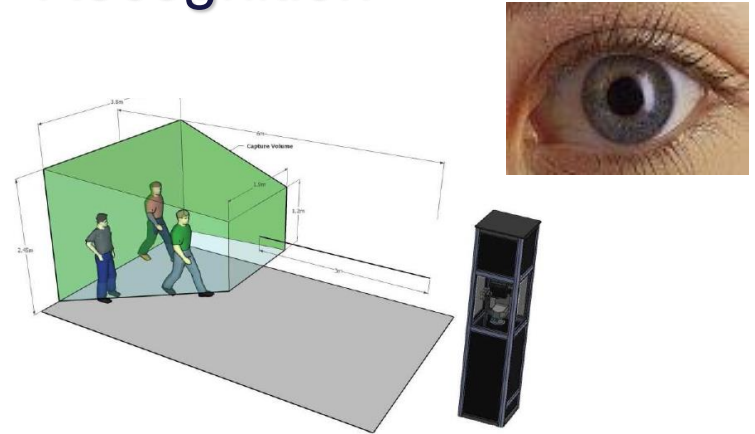


# Recognition - Biometrics

- Multi-view Face Recognition 2D & 3D



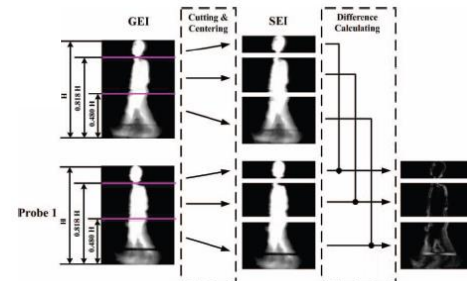
- Unconstrained Iris Recognition



- Super-Resolution

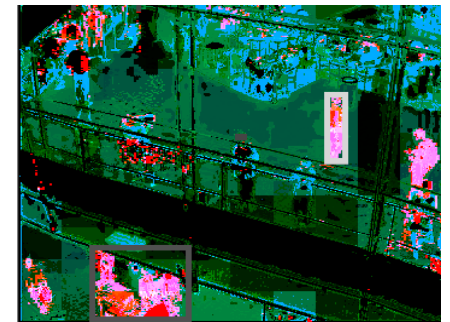
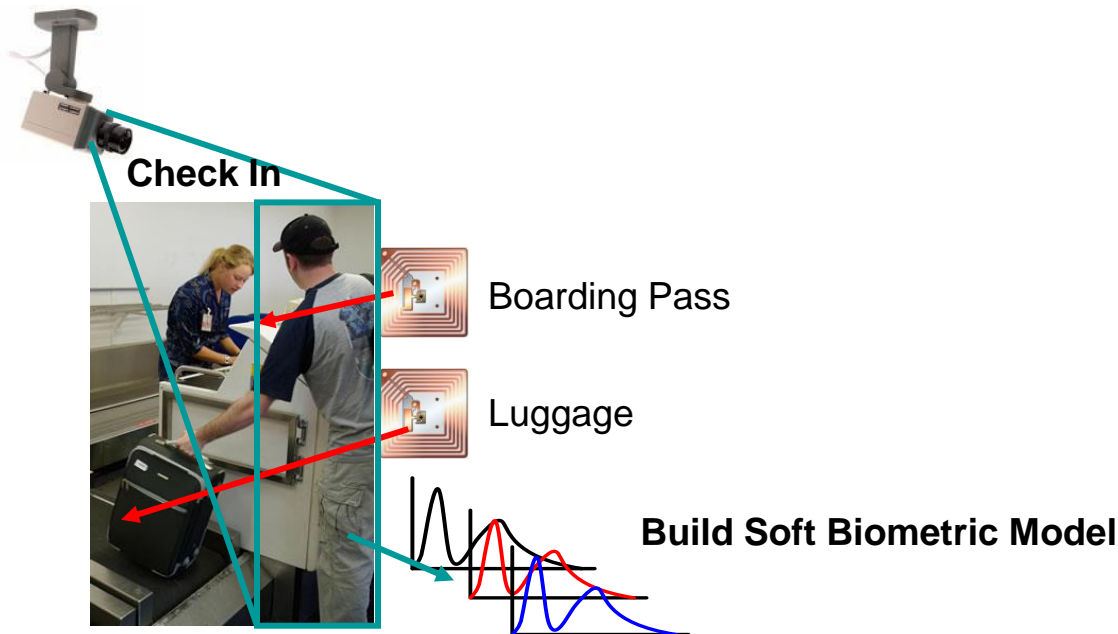


- Gait Recognition



# Soft Biometrics

- Soft Biometrics – Height, weight, hair / skin, colour, clothes.
  - Security & operational monitoring



# Operational Analytics

Operations analytics aim to extract information about the system they are observing from video footage

- No alarm generation
  - No false alarms, missed events
- Still useful even if not 100% accurate
  - Trends and changes in performance still visible

Presently, most commercial systems are focused on security rather than operations



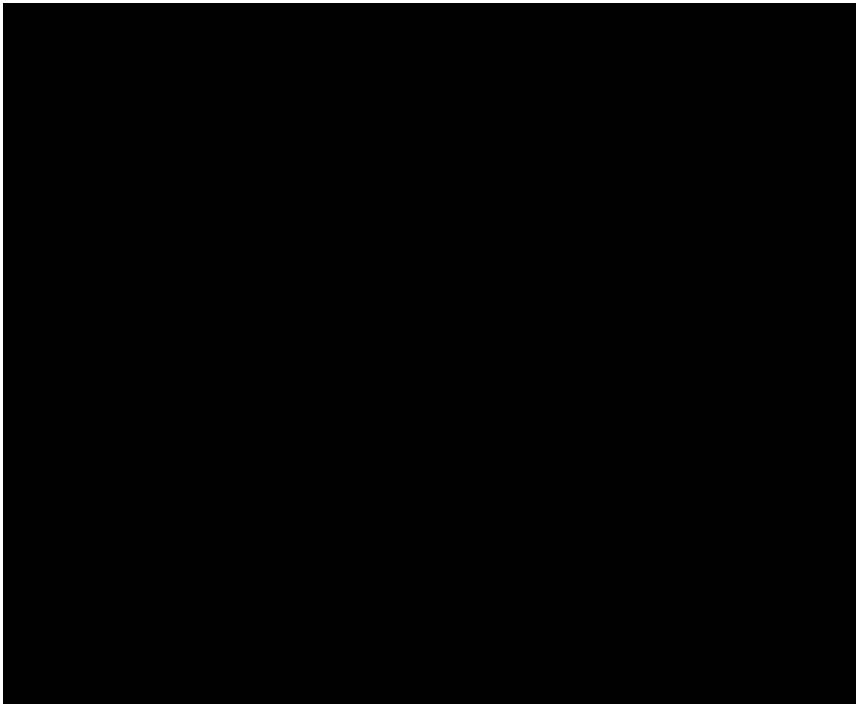
# Crowd Surveillance

- Not possible to track everyone in large open areas
- Monitor the crowd as an entity instead



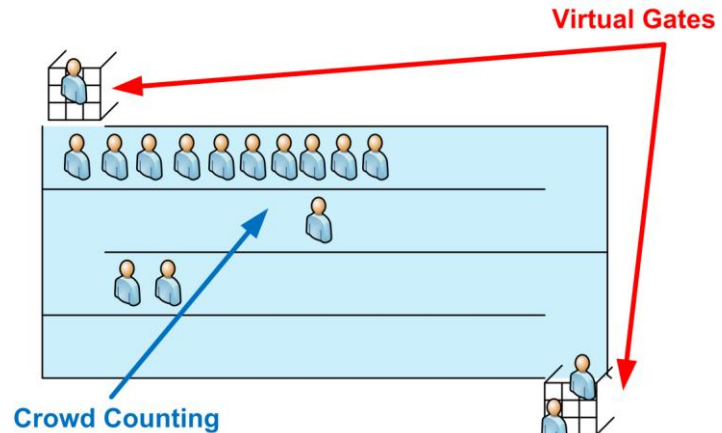
# Operational Analytics

- Measuring Throughput: Pedestrian Flow Analysis – “Virtual Gates”
  - Monitor bidirectional pedestrian traffic through a gate
  - Integrates optical flow over time & exploit calibration info to capture optical flow in relevant direction.

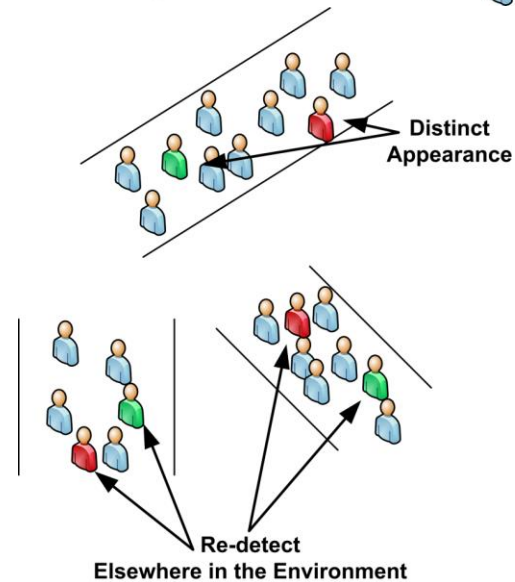


# Operational Analytics

- Monitoring Queues



- Determining Travel Times



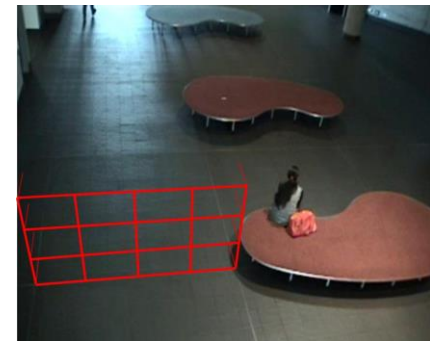
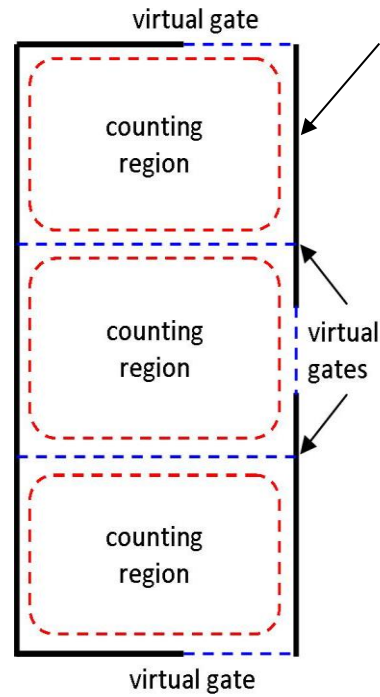
# Whole-of-Airport Performance Model



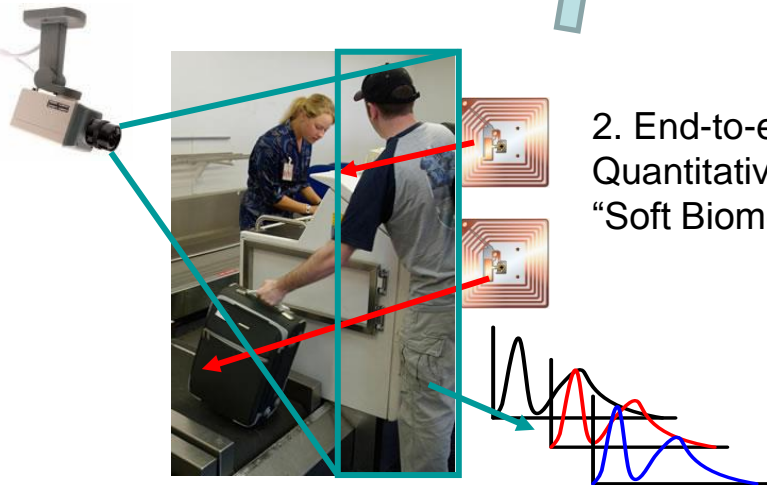
Statistical Model of Airport Performance  
"Complex System Model"

Intelligent Surveillance

1. Module-specific Quantitative data



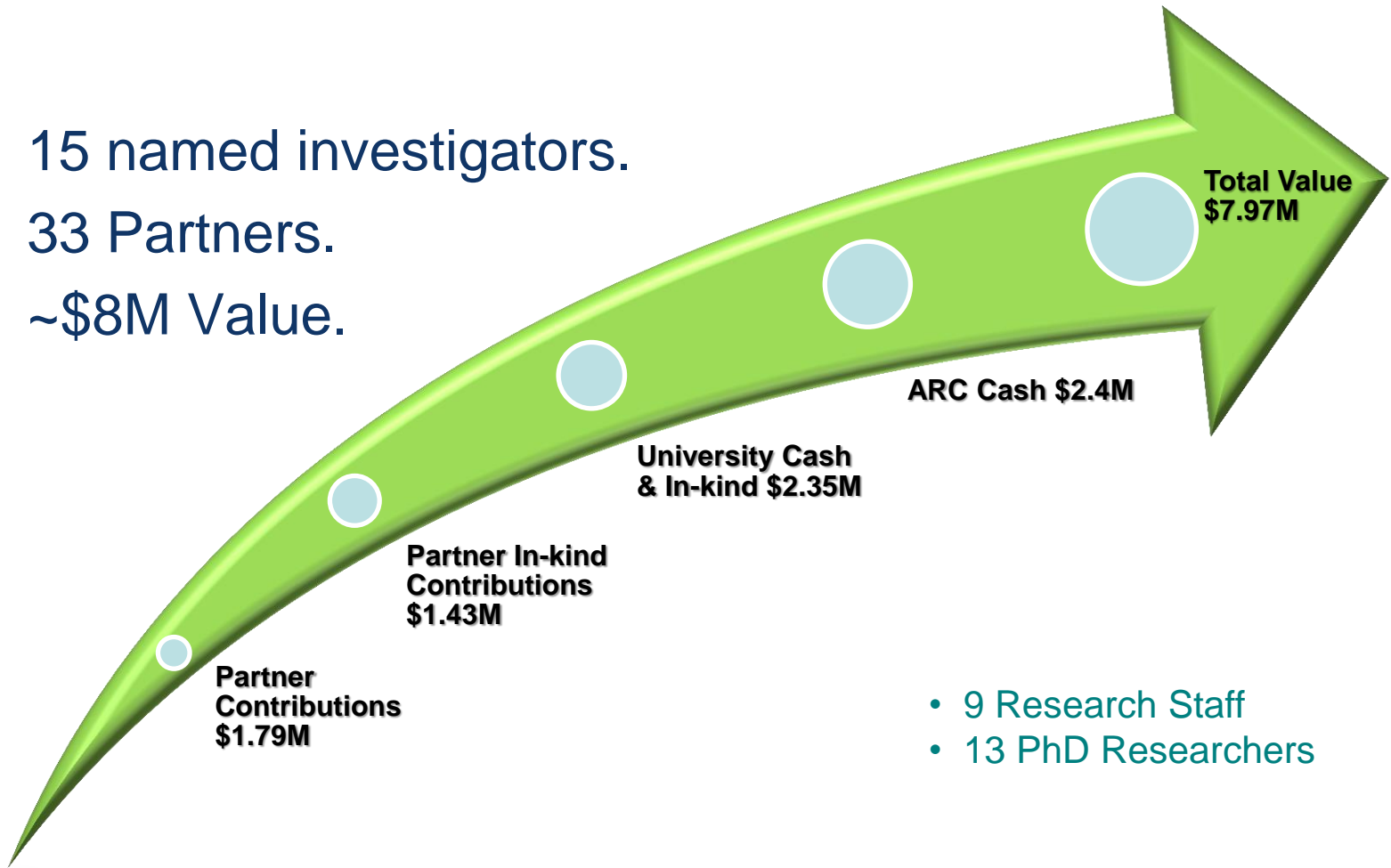
2. End-to-end Quantitative data  
"Soft Biometrics"





# Grant Structure

- 15 named investigators.
- 33 Partners.
- ~\$8M Value.



- 9 Research Staff
- 13 PhD Researchers



Australian Government

Department of Infrastructure, Transport,  
Regional Development and Local Government



Australian Government

Australian Customs and  
Border Protection Service



Australian Government

Department of Immigration  
and Citizenship



**AFP**  
AUSTRALIAN FEDERAL POLICE



Australian Government

Australian Quarantine and Inspection Service



- A WORLD OF SERVICE



AUSTRALIA

Tourism & Transport Forum



Emirates  
Group Security

Centre of Aviation & Security Studies



**SIEMENS**

# AotF Big Picture

Queensland University of Technology



Brisbane Airport



Australian airports

[Airports in general]

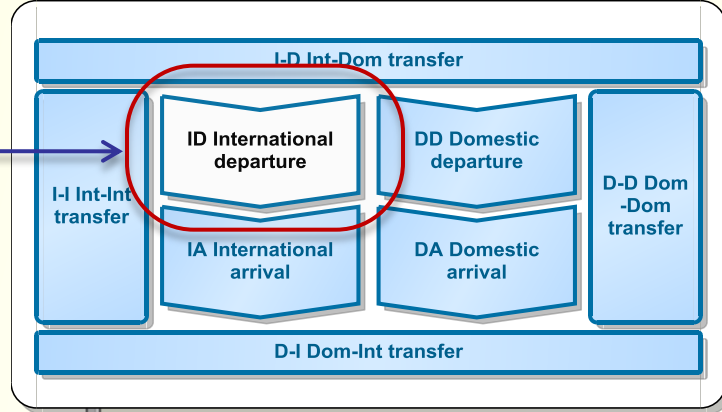
Pilot Team

Business Continuity Planning

Business Process Management

Human & Systems Interaction

Intelligent Surveillance



Pilot Team

Business Continuity Planning

Business Process Management

Human & Systems Interaction

Intelligent Surveillance

Extended Team

Complex Systems

Identity Management

Building Information Model





# Airports of the future

## ABOUT THE PROJECT

*The Airports of the Future – a multi-disciplinary international collaborative research project exploring the complexity of modern airports and addressing conflicts between aviation security and the passenger experience.*

This project draws upon diverse strengths through a university-industry-government partnership to develop tools to manage airport effectiveness and balance conflicting security, economic and passenger-driven pressures.

The project is funded under the Australian Research Council Linkage Projects Scheme LP0990135 and brings together a large consortium of stakeholders in the aviation industry including airports, airlines, and government agencies.

## NEWS AND EVENTS

- ➔ International Conference 9 - 11 February 2011
- ➔ Airports of the Future to feature on Stateline this Friday, 30th April at 7.30pm
- ➔ QUT responds to the Australian Government's Aviation Issues Paper (PDF, 558KB)

[More news »](#)



# Summary

- Outcomes of the research aim to enhance capabilities of Australian airports:
  1. Improve efficiency, security, and the passenger experience.
  2. Support strategic decision making.
  3. Balance performance criteria of a system that are mutually contradictory. (e.g. security and facilitation).
  4. Identify emergent properties of airports and interdependencies.
  5. Increase situational awareness and data mining of airport information.
  6. Inform legislation, policy and management, best practice guidelines.

# Access Control

- Exerting control over who can interact with a resource
- Two components
  - Authentication: Entity has the right to claim a unique identity within a domain
  - Authorisation: Granting or denying permission to an authenticated entity to access a resource in a particular way
- Main access control model in business, RBAC

# Why RBAC?

- NIST Standard
- Ease of administration
  - Move users in and out of roles
  - Move access rights in and out of roles
  - Very flexible
- Roles match business model
  - Roles define access
  - Role captures- function, responsibility, trust qualifications

# RBAC Elements

- Five elements
  - User: entity requesting access to object, has access in role
  - Role: package of permissions, assigned to users
  - Permission: grants access to objects
  - Operation: specific functions depending on object
  - Object: anything containing information that a user may need to access or an application



# Associations in RBAC

- Many to many user to role assignment allowed
- Many to many permission to role assignment allowed

# RBAC System

- Administrative Operations
  - Create, delete, maintain elements and operations
- \* Administrative Reviews: Query operations
- System level functions
  - Creation of users
  - Role activation/deactivation
  - Constraint enforcement
  - Access decision calculation

# Privilege

- Roles are assigned base on the principle of least privileged
- A role contains the minimum a mount of permissions to instantiate an object
- A user is assigned to a role that allows him to perform only what is required for that role
- No single role is given more permissions than the same role for another user

# Hierarchy and Inheritance

- Roles related in hierarchical structure
- Subordinate roles inherit rights from above
- Rights added as role becomes more specific
- Allows assignment of users to fewer roles

# Separation of Duties (SoD)

- Enforces conflict of interest policies
- Ensures that failures of omission or commission can be caused only as a result of collusion
- Two types
  - Static Separation of Duties
  - Dynamic Separation of Duties

# Static SoD

- Places restrictions on the set of roles
- No user is assigned to n or more roles which may conflict with each other
- A user may be in one role but not another
- Prevents a person from submitting and approving their own request

# Dynamic SoD

- Places constraints on the users that can be assigned to a set of roles
- Constraints are across or within a user's session
- No user may activate n or more roles from the roles set in each session
- Timely revocation of trust ensures that permissions do not persist beyond the time that they are required for performance of duty

# XACML

- Dialect of XML used to specify and enforce authorization policies (OASIS standard)
- XACML provides
  - Interchangeable policy format
  - Support for fine grained and coarse authorization policies
  - Policy combination and conflict resolution
  - Independency from implementation
  - Can be extended



# XACML Policy Evaluation

- Attribute based access control
- Attributes associated with Subject, Action, Resource or Environment
- Attributes may represent static or dynamic properties
- Policies contain Boolean expressions
  - False: Policy not applicable
  - True: Permit or deny is returned
  - Indeterminate: Error or some value missing

# XACML Policy Evaluation

- Combining algorithms resolve conflicting policy results
- Typical: Deny overrides
- Obligations which are associated with final effect are also returned
- Policies are tree structured to simplify management

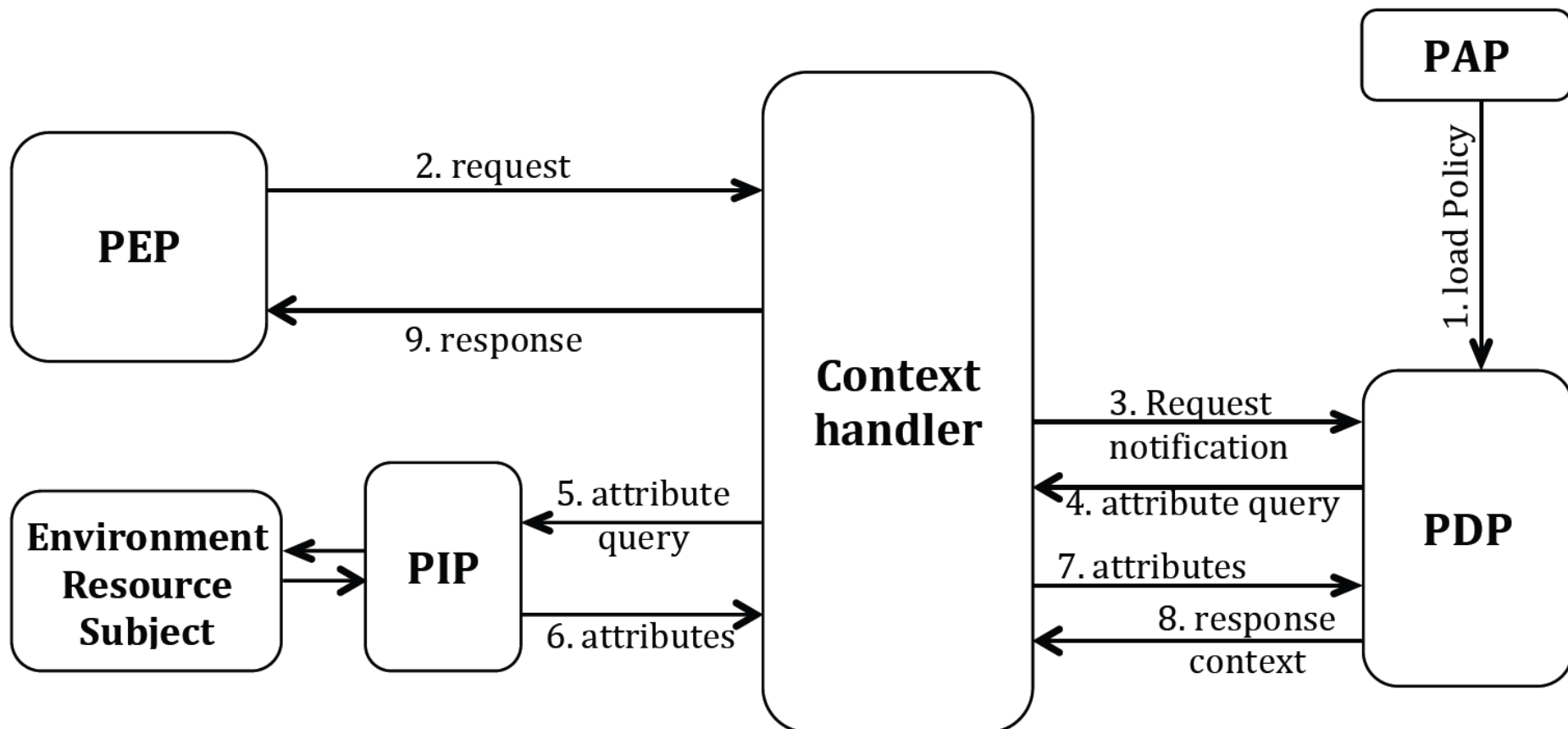
# XACML Major Actors

- Policy Decision Point (PDP)
  - Select those policies that are applicable to an access request
  - Make decision whether the request should be allowed or denied
- Policy Enforcement Point (PEP)
  - Initiates a request in response to user's access attempt
  - Enforces decision returned by PDP

# XACML Major Actors

- Context handler (CH)
  - Translates between PDP, PEP and other systems
- Policy Administration Point (PAP)
  - Responsible for administering and managing the policies
- Policy Information Point (PIP)
  - Communication with other systems in case extra information is needed in making a decision

# XACML major actors



# RBAC-XACML

- Extension (2005) of XACML to include RBAC
- Adds an additional type of decision point namely a Role Enablement Authority (REA)
  - Deals with requests on role activation decisions
  - Supports role hierarchy
  - Does not support SoD