



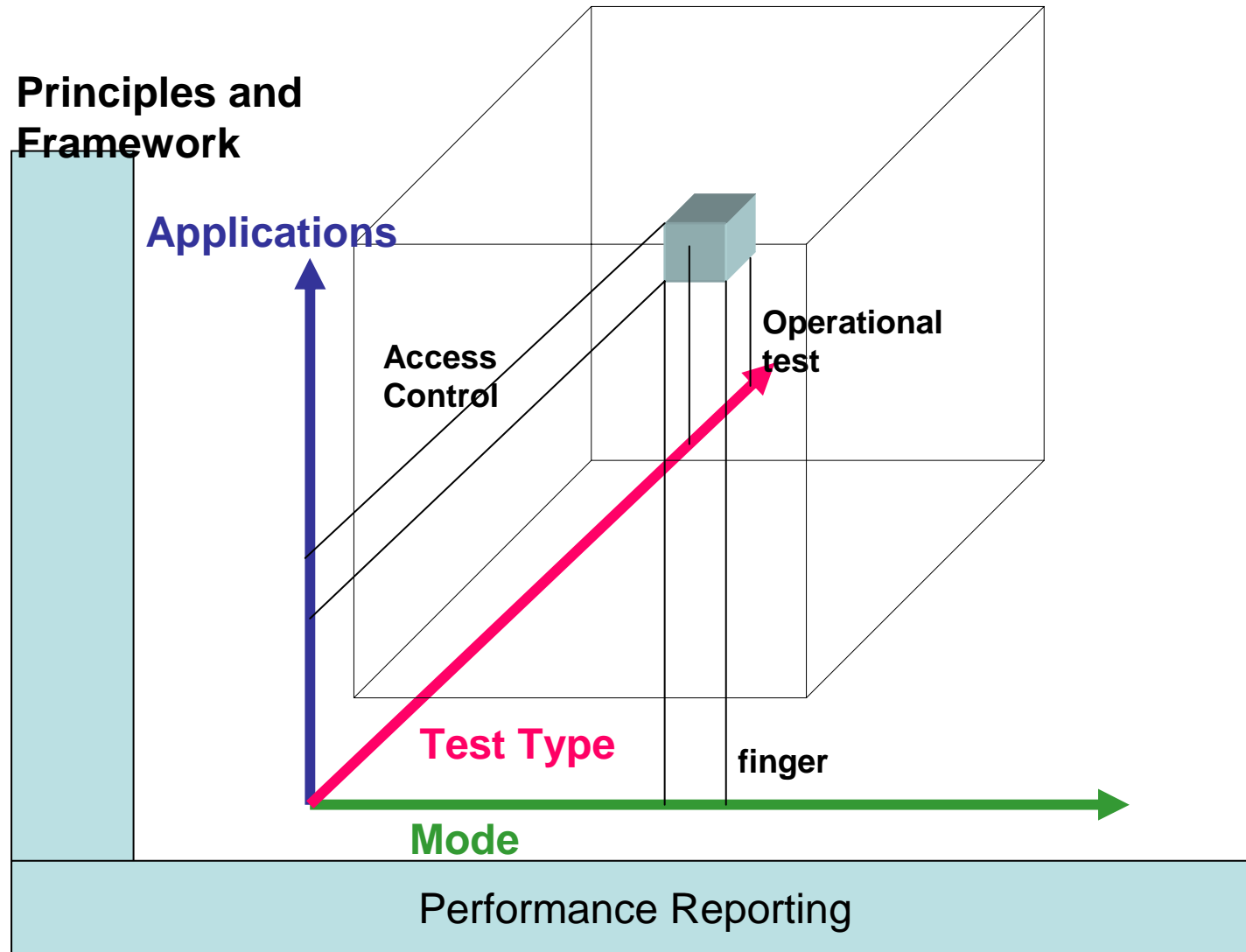
Development of Standard Taxonomy for defining Biometric Applications

Dr. Craig M. Arndt
Mitretek Systems

Why is a Standard Taxonomy Important

- Test Definition
- System Requirements Definition
- Cross mode / Product comparisons
- Evaluating Research
- Defining New Development

Testing Standards



Current Application of the Application Taxonomy

- ISO, JTC1, SC 37 on Biometrics Test and Evaluation Standard
- BIOVISION Roadmap

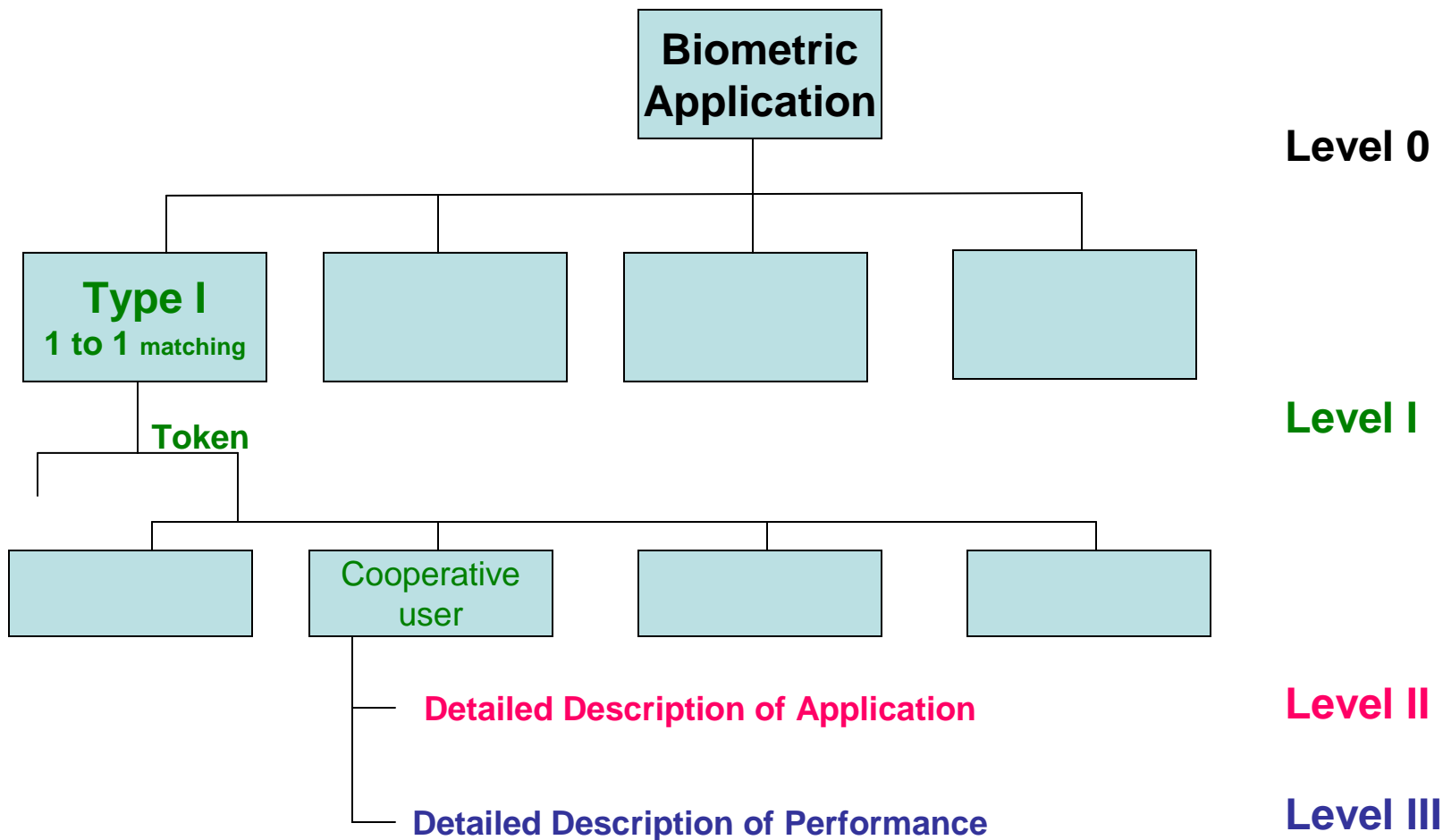
Applications

- Each application also has unique features which affect how a system will operate and therefore be tested
- Applications require a more complex method of definition than the other parts of a biometric system definition (modality)
- Biometric applications are found across all industries and are not easily enumerated.

Method for classifying applications

- A multilevel taxonomy allows us to divided different applications according to different criteria
- Each of the different levels of the classification method separates different applications according to different parts of an application description
- This method provides a structure to define biometric applications independent of modality in a defined repeatable manner

Classification of Application



Levels of application clarification and Description

- Level 0 Definition of biometric application
- Level I General Class of Matching and Architecture
- Level II System Environment, interactions and user population
- Level III System performance requirements

Level 0 Definition of biometric application

- At level 0, we first determine if an application applies as a Biometric
- Some applications and systems use biometric technology but are not considered biometric applications for the purpose of this standard.
- Non-real time and non-live scan types of biometrics are generally considered not included
- Forensic and DNA are not included for example

Level I General Class of Matching and Architecture

- Type of matching function
 - Type I: 1 to 1 matching, recognition
 - Type II: Positive Identification 1 to many
 - Type III: Negative Identification 1 to many
 - Type IV: 1 to few
- Template Architecture
 - With Token
 - Without Token
- User Type
 - Cooperative
 - Uncooperative
 - Surveillance

Level I Classification

- By combining the different level 1 types we determine a general classification of an application
- Not all combinations are an application of interest
- Example: Type 1 (one to one) matching with a smart card (token) and a corporative user
- This defines a class of applications with similar architectures

Level II System Environment, interactions and user population

- At level II we define the system operating environmental factors which characterize applications
 - Operating Environment
 - Temp
 - Lighting
 - Vibration
 - Contamination (dirt, dust, salt etc.)
 - Noise

Level II (Continued)

- Operational Mode of the System
 - Man in the loop (decision add)
 - Attended operation
 - Un-attended operation
- End User Population
 - Size of user set and search set
 - Population distribution and diversity
 - Location of different parts of the population
 - Characteristics of the population

Level II (Continued)

- Exception handling in the system
 - Alarm procedures
 - Failure to enroll procedures
 - False rejection procedures
 - 508 procedures
 - VIP, not enrolled
- System Interfaces
 - Links to external databases
 - Links to external hardware (security systems)

Level II Application Description

- The process of determining the different factors at level II will define how the system operates and how it will need to be tested
- Example: Airport personnel access door from runway
 - Operating environment
 - 100 to -20 Deg
 - Dust
 - Wide range of lighting
 - High noise
 - Operational Mode
 - Unattended operation

Level II (continued)

- End user population
 - Small group of users for any given door
 - Wide range of use demographics
 - Gloves and hearing protection in use
- Exception handling
 - Local supervisor will determine action for false rejection
 - Airport security will react to alarms
 - Others will be escorted
- System interfaces
 - Interface with electronic lock
 - Reporting and recordkeeping of entries in airport central database

Level III System Performance Requirements

- At level III the biometric application is defined based on how it is expected to perform in operation.
- The system performance requirements complete the description of a biometric application. With this information as well as the descriptions at Level I and II, knowledge of the system test type, and modality of the system we can completely describe a test method for the system.

Level III (continued)

- System performance requirements include both biometric and general system requirements
 - Biometric Performance
 - FRR
 - FAR
 - FTE
 - Throughput
 - Standards Compliance

Level III (continued)

- Other systems requirements
 - Power
 - Reliability
 - Maintainability
 - Etc.
- Example: Airport personnel access door from runway
 - Biometric Performance
 - Less than 2% failure to enroll
 - Fewer than 3 false rejections per shift
 - Less than a 1% chance of false acceptance
 - System operation time of less than 2 sec average, 4 sec max

Level III (continued)

- Standards Compliance
 - BioAPI
 - CBIFF
- Other System Requirements
 - 120 V power
 - Mean time between failure under 24/7 operations of 10,000 hours
 - Mean time to repair of 30 min or less

Biometric Applications

- Different applications will require more or less definition
- Example
 - Technology tests will not require Level II or Level III definition
 - Application testing will require detailed definition of the application

Examples of using the Application Taxonomy

- Requirements Definition
 - Define the nature of the task
 - Define the environment and interfaces
- Test Design
 - Parts of the system to be tested
 - Methods of test
 - Acceptable levels of performance

Requirements Definition

- Requirements Definition is critical to specifying a system for development or requirement.
- A clear definition of the system requirements assures that the system developed will function as expected without over design and added cost.

Requirements for Biometric Application

- Level I General Class of Matching and Architecture
- Level II System Environment, interactions and user population
- Level III System performance requirements

Example



- Access Control system
- Level 1, Architecture
 - Recognition without a token and a cooperative user
 - Class 5 application
- Level 2, System Environment, interactions and user population
 - Operating Ambient Temperature range -40 to +140 deg F
 - Existing population demographics of the US army (active duty)

Example (continued)

- Level 3, System performance requirements
 - False Acceptance rate < than .01 % (1 in 10,000)
 - False Rejection rate < than 1% (1 in 100)
 - Operation time of < 2 sec.
 - Mean Time Between Failure (MTBF) in operation > 10,000 Hours

System test Design

- Each test of a biometric system will require specific definition of the different factors which define the system
- The statistical reliability of the performance data will define the size and makeup of the test data and/or test subject pool
- Each test must produce numeric test results for evaluation

Test Definition

- In order to effectively determine what and how to test a system you must first define how the system is to operate and under what conditions (the application definition)
- An accurate clearly defined test plan requires that each aspect of the system be separately defined and pass / fail conditions be defined in terms of the application functions and level of performance.

Test Process

- Step 1 Define scope of the system to be tested
- Step 2 Define the test Type
- Step 3 Define the system Modality
- *Step 4 Define the Application class and features*
- *Step 5 Define performance requirements and test reliability*
- *Step 6 Determine the sample sizes and distribution of data, and subjects for performance testing*
- *Step 7 Specify other requirements to be verified by testing*
- Step 8 Write test plan
- Step 9 Verify planned test will yield definitive reportable results
- Step 10 Write detailed test procedure
- Step 11 Schedule test facilities and train staff
- Step 12 Execute test
- Step 13 Analyze test results
- Step 14 Repeat test as needed
- Step 15 Write test report

Conclusions

- Biometrics is a quickly developing technology with a wide range of current and emerging applications
- The Application Definition method and taxonomy helps users and developers define application in a specific manner and build better systems
- The development of standards including the application definition method are a key part of the maturity of the industry