Astronomy ESFRI & Research Infrastructure
Cluster ASTERICS - 653477

A&A Cherenkov Telescope Array User Requirements

Alessandro Costa[1], Eva Sciacca[1]

on behalf of the CTA Consortium

[1] INAF Catania

INTRODUCTION & Outline

*CTA: "operated as an observatory **open** to the astronomy community"*

*This is a fundamental **Constraint** and drives the A&A Infrastructure development*

A&A WG in CTA Data Management team:

Identify a solution to provision and manage electronic identity for every individual seeking to access CTA resources

Use Case	Collection
User Requirement	Elicitation
A&A	**Architecture Overview**

Use Case Collection

The A&A working group outlined a collection of use cases:

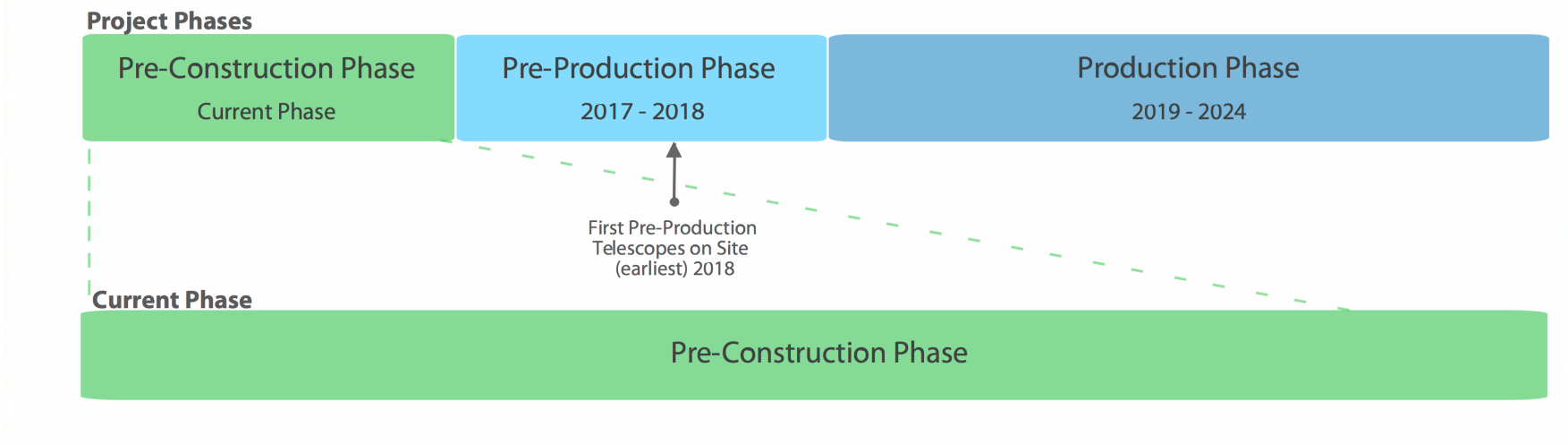
Use Cases: representative set of activities corresponding to **Constraints** and **Scenarios**.

- **Constraints** describe real-world *limits or boundaries* around what we want to happen
- **Scenarios** are used to analyse the operation of the system in its intended environment.

Use Case Collection -> to identify requirements that may not have been (yet) formally specified.

Requirements describe what we *want* to happen

Constraints and UR: an Example



CONSTRAINT: **Production Phase until 2024**

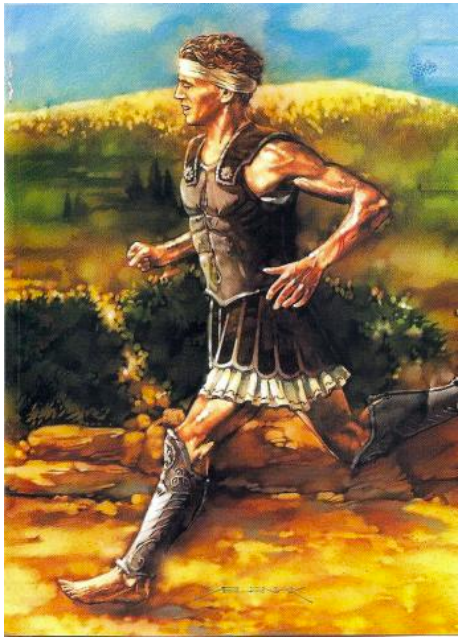
USER REQUIREMENT "Portability": **UR-A&A-1000** The A&A system must be portable enough to be maintained over the period of operations and 10 years after CTA decommissioning.

Time Scale and the Impact on Technology

10 years after CTA decommissioning -> **2034**

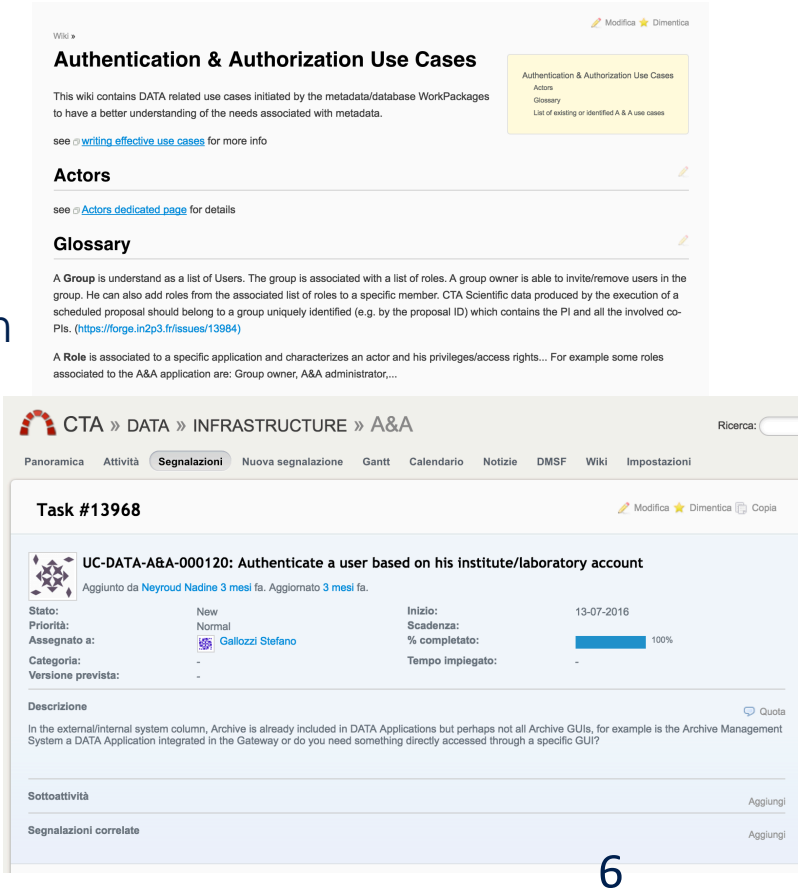
Time scale for CTA is definitely a **long distance running**

Technology must **follow requirement** with **simplicity** in the correct priority; giving furthermore a field test of its **sustainability**



Use Case Collection

- **ACTOR Definition**
  - Human
    - name, role, description
  - System
    - name, description, Sub-System
- **USE CASES Definition**
  - name, description, ID
- **Redmine Issue Tracking**



Actor Definition

Actor	Description
Observer	An astronomer that can submit proposals to **perform observations**.
Guest Observer	A member of the scientific community who is granted access to a specific subset of CTA data, associated with a successful proposal to the Observatory.
CTA Consortium Observer	An observer that is a member of the CTA Consortium. A privileged user.
Archive User	A scientific user of the CTA observatory who makes use of archival data, as opposed to data associated with a specific proposal.

A&A Use Case Collection

Some of the defined Use Cases:

- **Authenticate an already registered CTA Consortium user**
- **Authenticate a user based on his institute/laboratory account**

- **Lost password management**
  - User with a local A&A login/password must be able to ask for a new password in case of lost password
- **Group creation**
  - **A&A Administrator or DATA Applications** must be able to create a group, associate roles and define group owner(s)
- **Group management**
  - A group owner is able to manage his group from a central A&A management system or from specific **DATA application** integrated or not in the Gateway: **invite users, remove users**

User Requirement Elicitation

User Requirement are grouped in the following Classes:

- Authentication capabilities
- Authorization capabilities
- Account Management capabilities
- Group Management by users/group owner
- Interfaces
- Availability
- Performance
- Security
- Portability

User Requirement: Authentication Capabilities

- **UR-A&A-0030** A CTA consortium user could be identified using his CTA login/password.

- **UR-A&A-0010** A Guest Observer that cannot be identified by a scientific community must be able to be identified by a local account protected by login/password.

- **UR-A&A-0035** User wants to log in **once** on the CTA applications from the gateway and gains access to his authorized applications and datasets without being prompted to log in again at each of them, so that **user needs to authenticate himself only once per session**.

User Requirement: Authorization Capabilities

- **UR-A&A-0100** The A&A system administrator or an authorized **application** should be able to **create a group**.

- **UR-A&A-0105** The A&A system administrator should be able to **manage the list of roles associated to a group**.

- **UR-A&A-0120** CTA Scientific data produced by the execution of a scheduled proposal should belong to a group uniquely identified (e.g. by **the proposal ID)** which contains the PI and all the involved co-Is.

- **UR-A&A-0130** The A&A system administrator has a tool to **add privileges to any user**.

User Requirement: Group Management

- **UR-A&A-0310** A **group owner** has access to management tools to invite/remove user and manage roles of his group members
- **UR-A&A-0315** A group owner has access to management tools allowing the definition of groups by using **set operations**
- **UR-A&A-0340** A group owner has a tool to easily add or remove list of users as members of his group
- **UR-A&A-0360** A group owner has a tool to **delegate** his group owner rights to another member

User Requirement: Security & Portability

Security

- **UR-A&A-0900** All passwords must be encrypted on network.
- **UR-A&A-0910** A lockdown system must be implemented to block accounts in case of too many connection attempts
- **UR-A&A-0920** The user must be sure that the A&A system will guarantee privacy of user information with an **explicit user consent**.
- **UR-A&A-0975** **A Persistent ID** must be assigned to a User
- **UR-A&A-0980** **Persistent ID** will not be reassigned to another user

Portability

- **UR-A&A-1000** The A&A system must be portable enough to be maintained over the period of operations and 10 years after CTA decommissioning.

User Requirement: Interfaces

- **UR-A&A-0410** **A central GUI** is provided to the A&A system administrator and Group owners to perform all management activities
- **UR-A&A-0420** An **API** is provided by the A&A system to perform group management/provisioning activities

A&A Architecture

- **Consortium member**
- **Observatory member North Site**
- **Observatory member South Site**
- **Observatory member Central**

(CTA Local Access)

Authentication

is the process of identifying an individual using the credentials of that individual.

- **Guest Observer**

(Local account)

- **Guest Observer**

(Federated Access)

+

Authorization

Authorization is the process of determining whether an authenticated individual is allowed to access a resource or perform a task

=

Role-Based Authorization

When a user or group is added to a role, the user or group automatically inherits the various security permissions

Acknowledgement

H2020-Astronomy ESFRI and Research Infrastructure Cluster (Grant Agreement number: 653477).

Questions ?