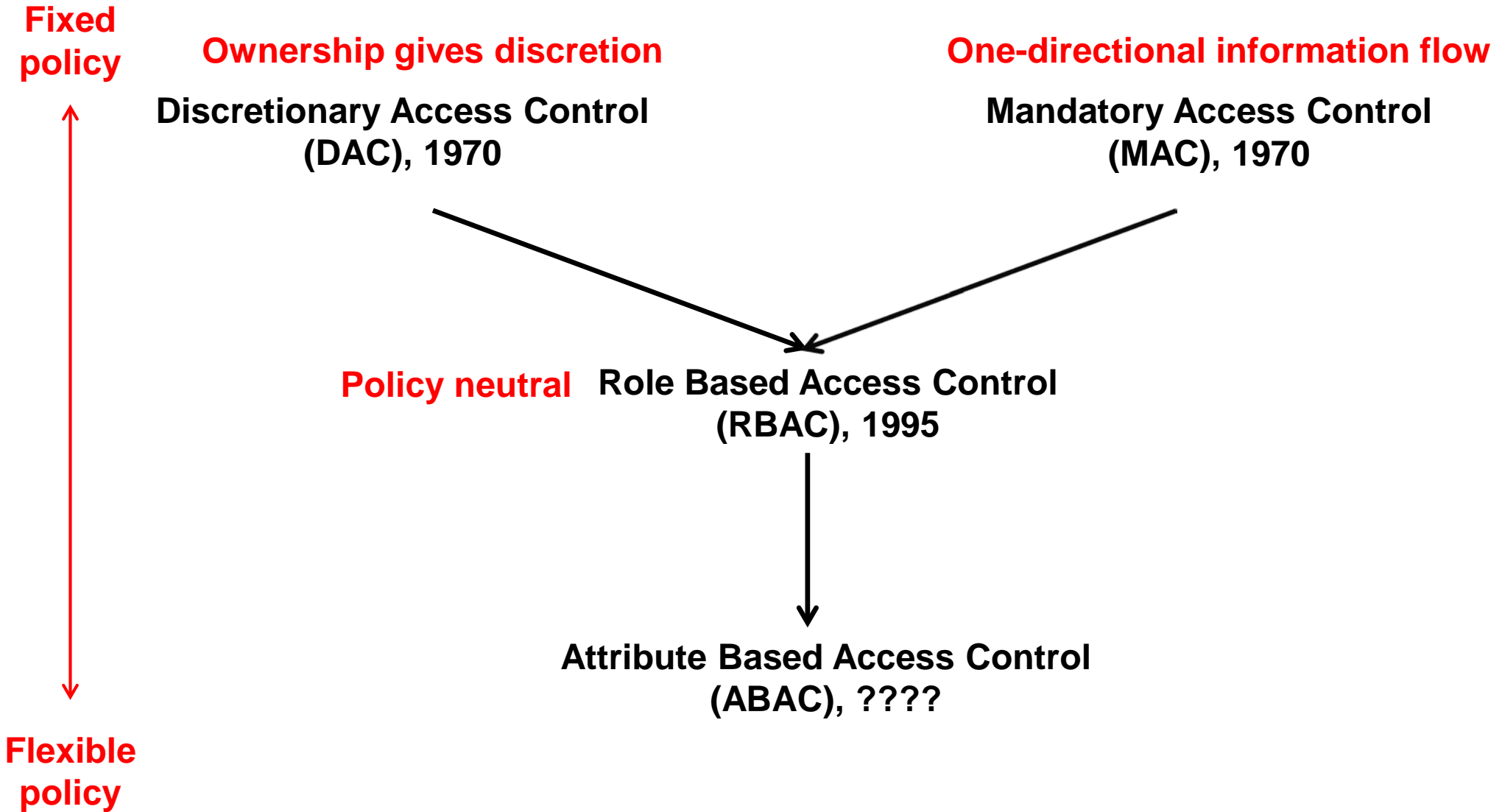


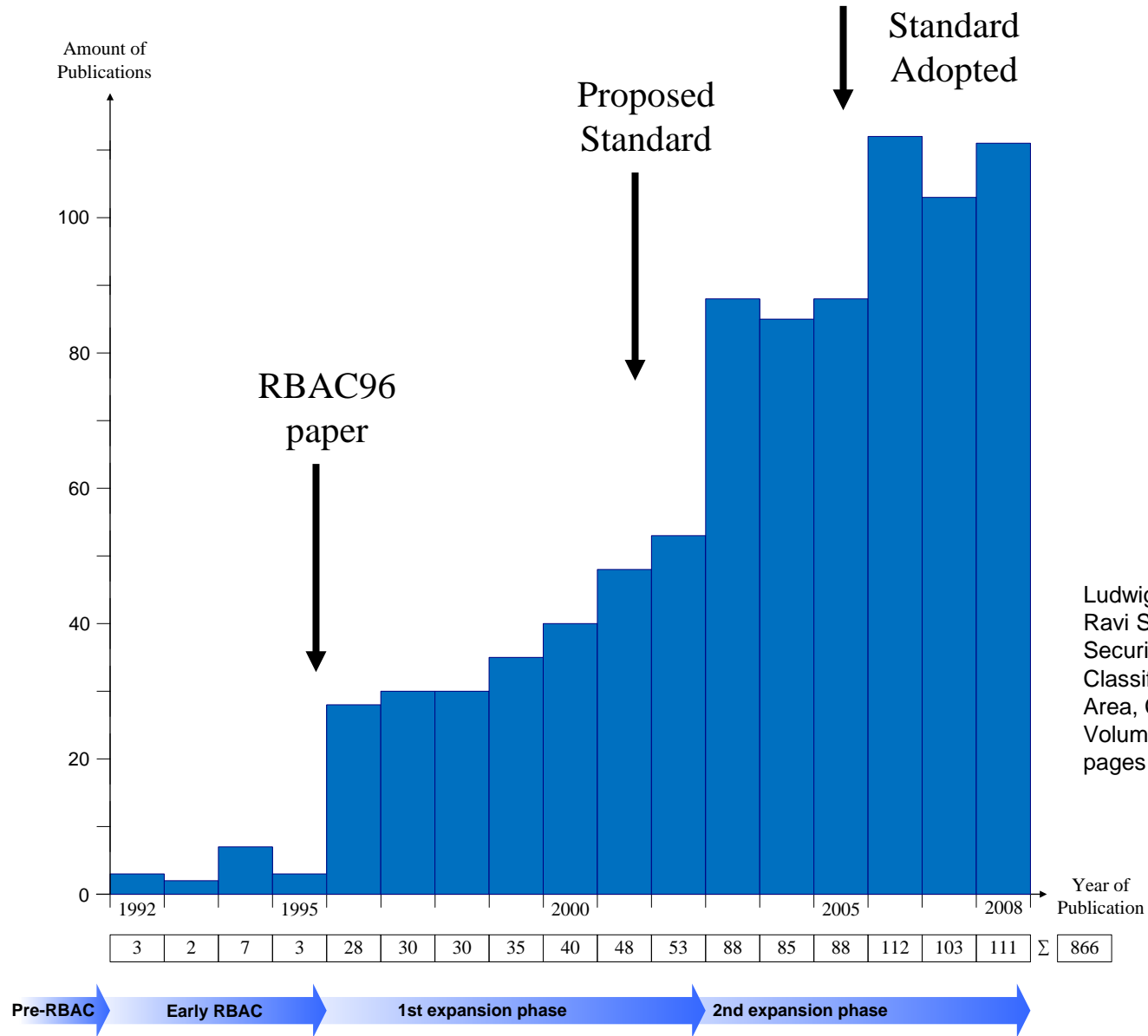
Role-Based Access Control (RBAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 3-1

ravi.utsa@gmail.com
www.profsandhu.com





Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

- Access is determined by roles
- A user's roles are assigned by security administrators
- A role's permissions are assigned by security administrators

First emerged: mid 1970s
First models: mid 1990s

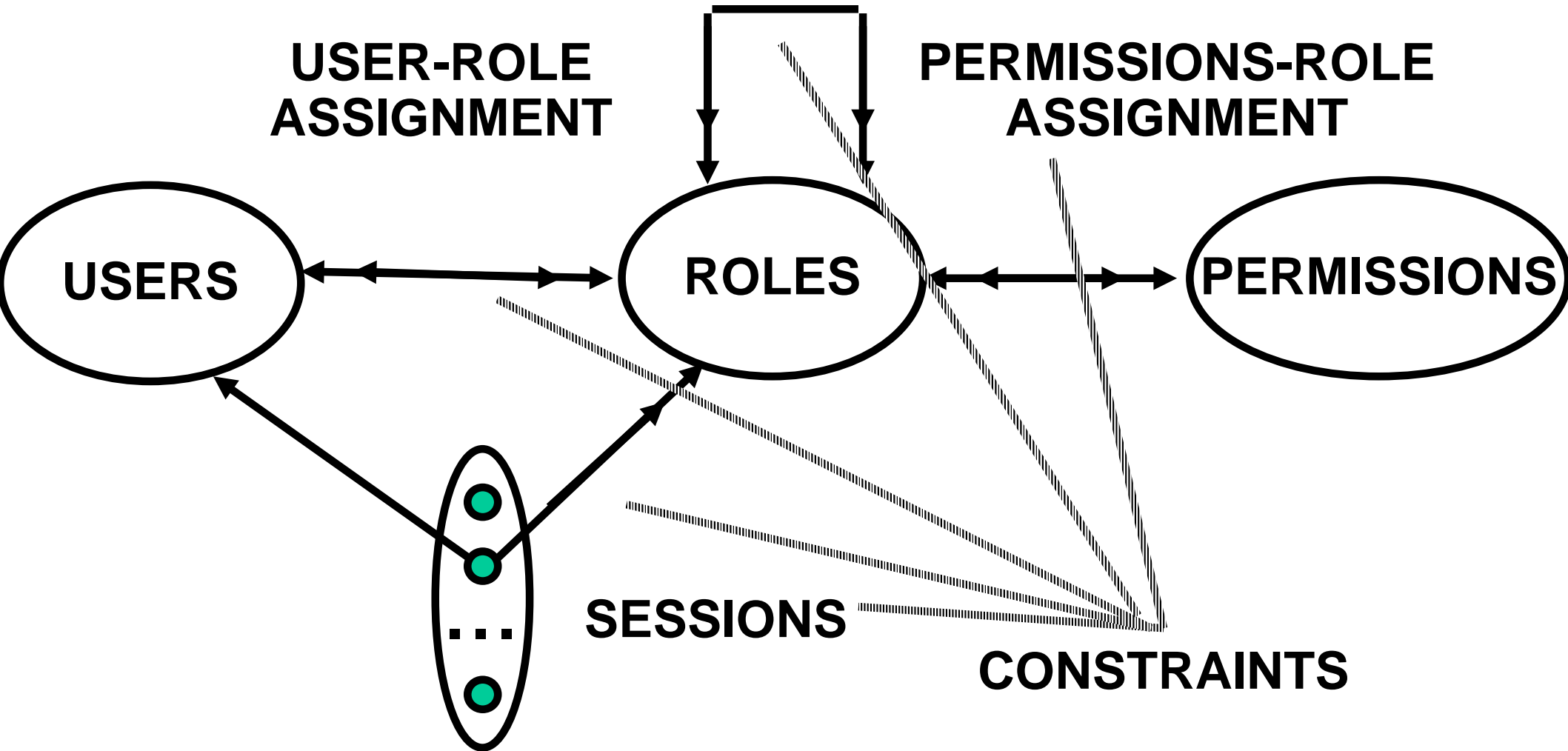
Is RBAC MAC or DAC or neither?

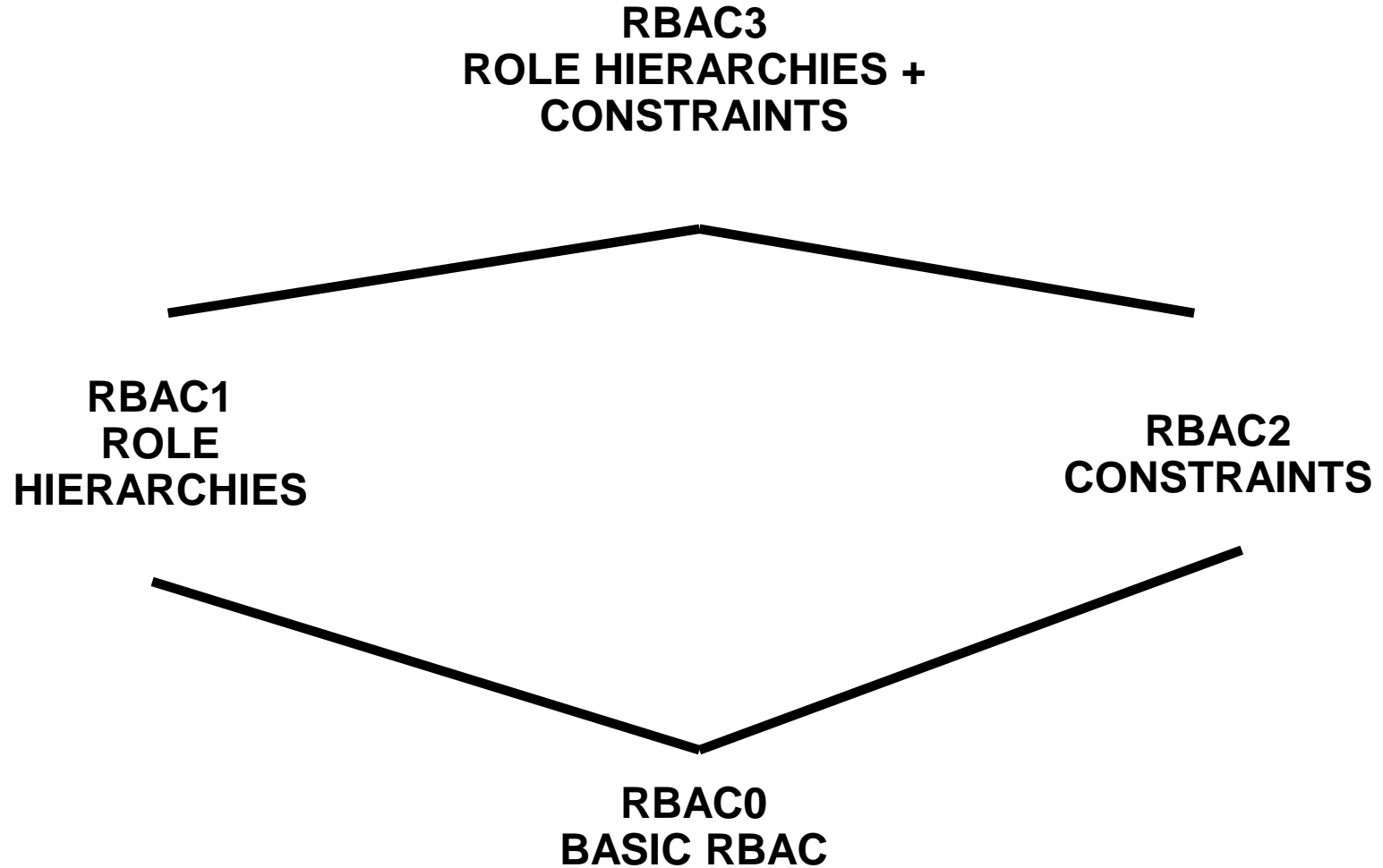
- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

RBAC is neither MAC nor DAC!

RBAC96 Model

ROLE HIERARCHIES





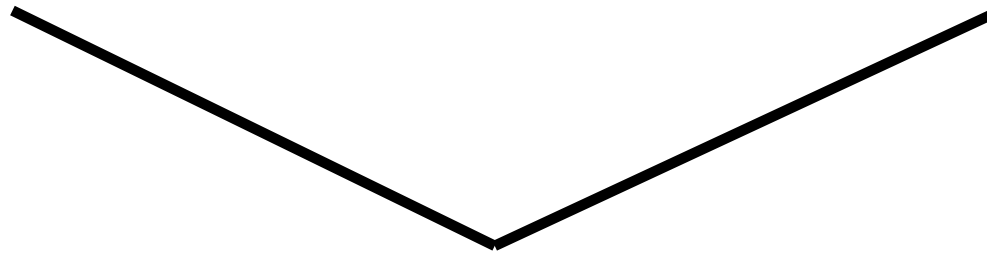
- **Abstraction** of Privileges
 - Credit is different from Debit even though both require read and write
- **Separation** of Administrative Functions
 - Separation of user-role assignment from role-permission assignment
- **Least Privilege**
 - Right-size the roles
 - Don't activate all roles all the time
 - Limit roles of a user
 - Limit users in a role
- **Separation of Duty**
 - Static separation: purchasing manager versus accounts payable manager
 - Dynamic separation: cash-register clerk versus cash-register manager

- A role brings together
 - a collection of users and
 - a collection of permissions
- These collections will vary over time
 - A role has significance and meaning beyond the particular users and permissions brought together at any moment

- Groups are often defined as
 - a collection of users
- A role is
 - a collection of users and
 - a collection of permissions
- Some authors define role as
 - a collection of permissions
- Most Operating Systems support groups
 - BUT do not support selective activation of groups
- Selective activation conflicts with negative groups (or roles)

**Primary-Care
Physician**

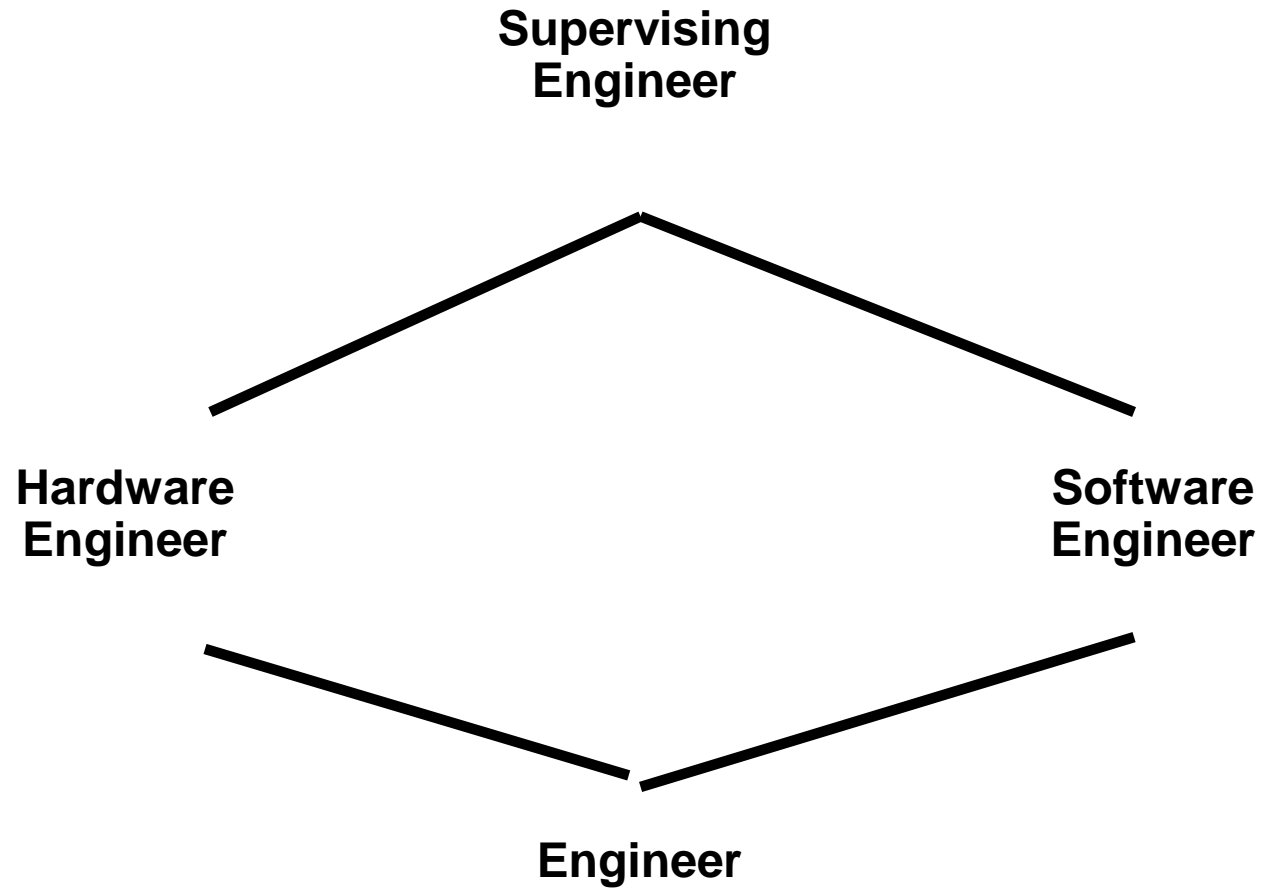
**Specialist
Physician**



Physician



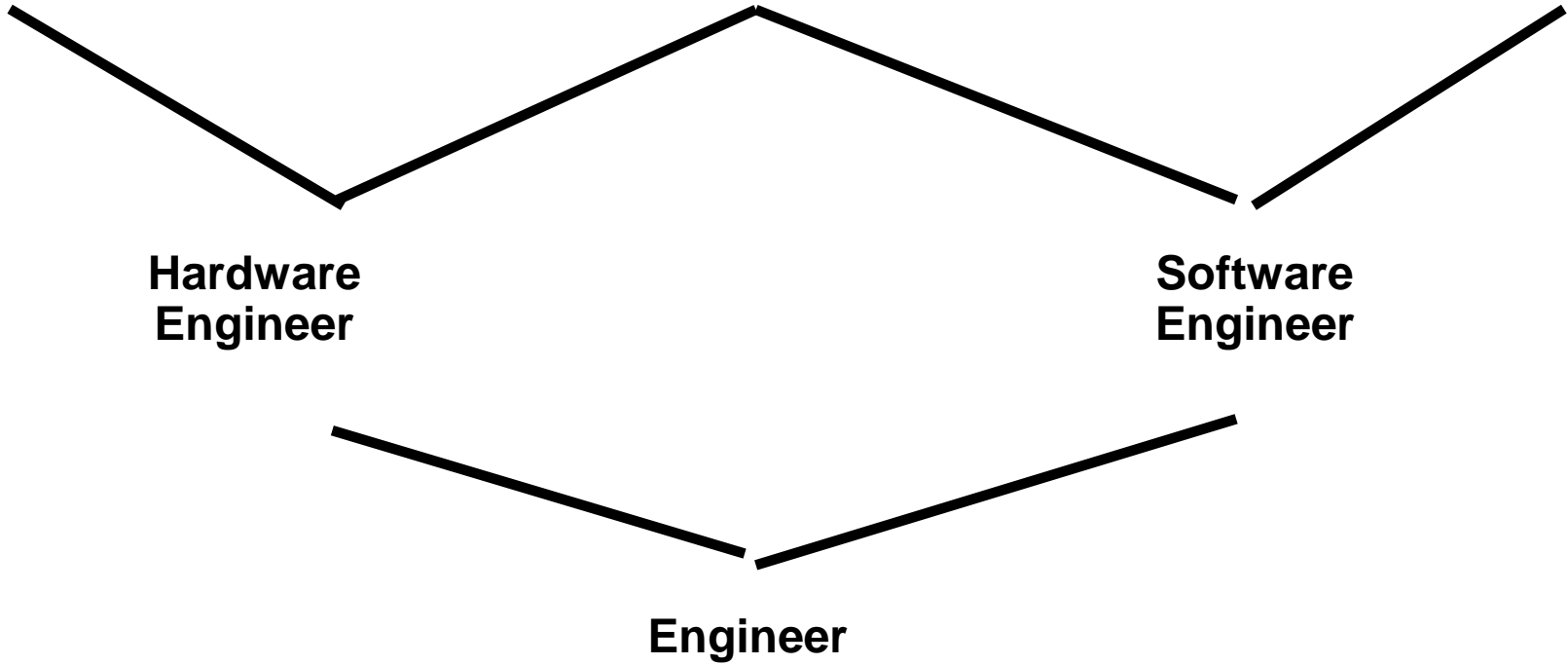
Health-Care Provider

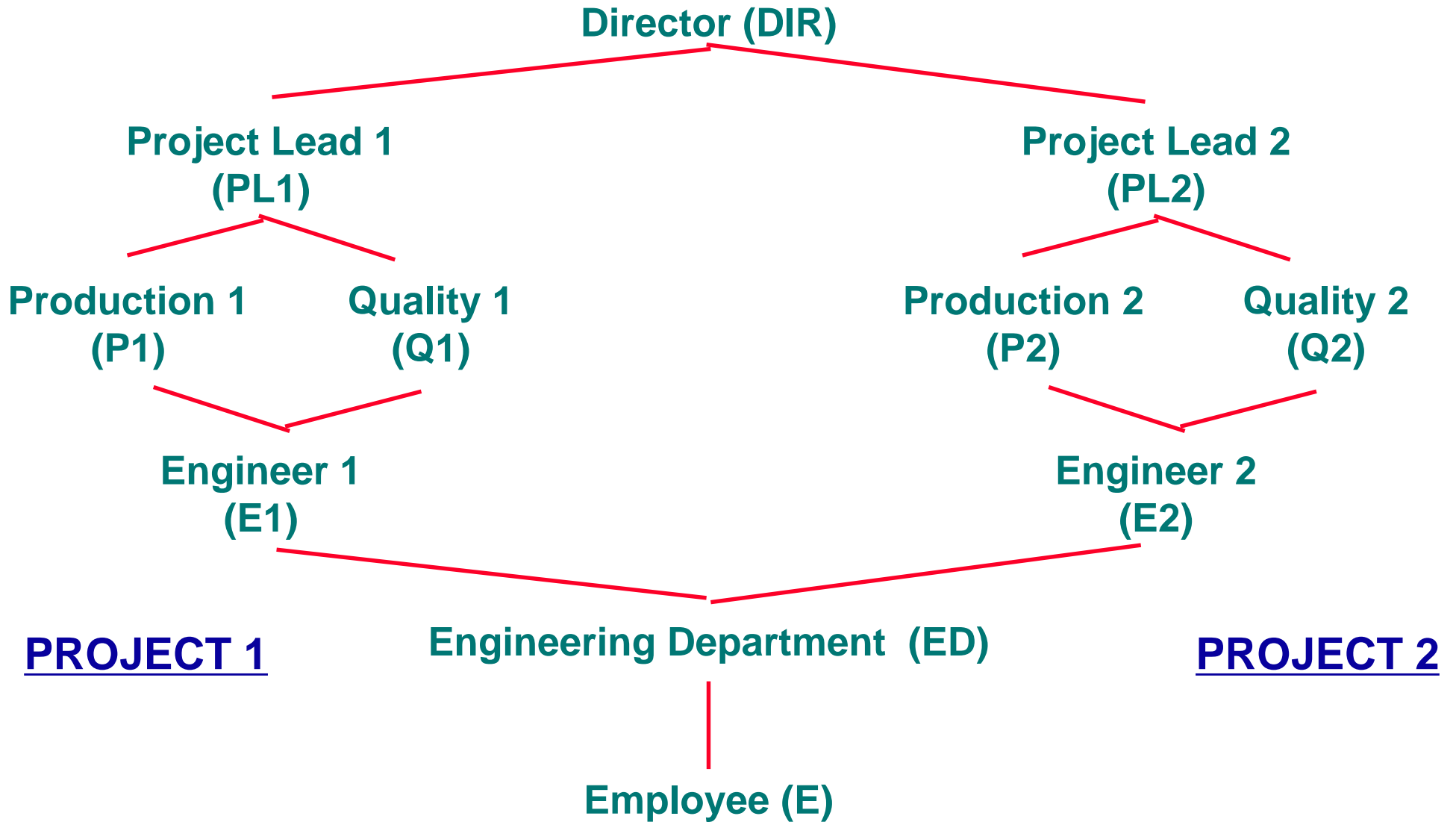


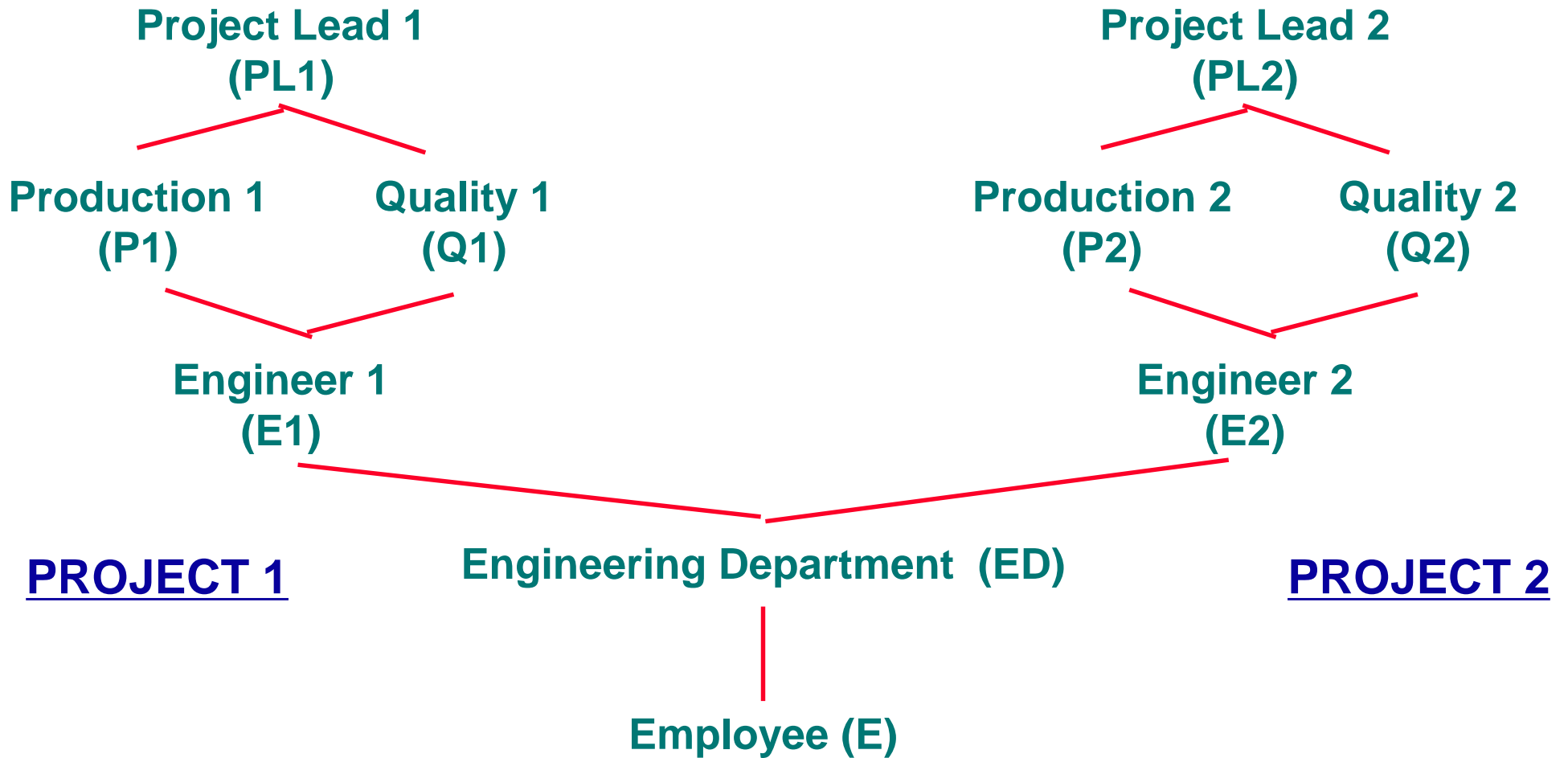
**Hardware
Engineer'**

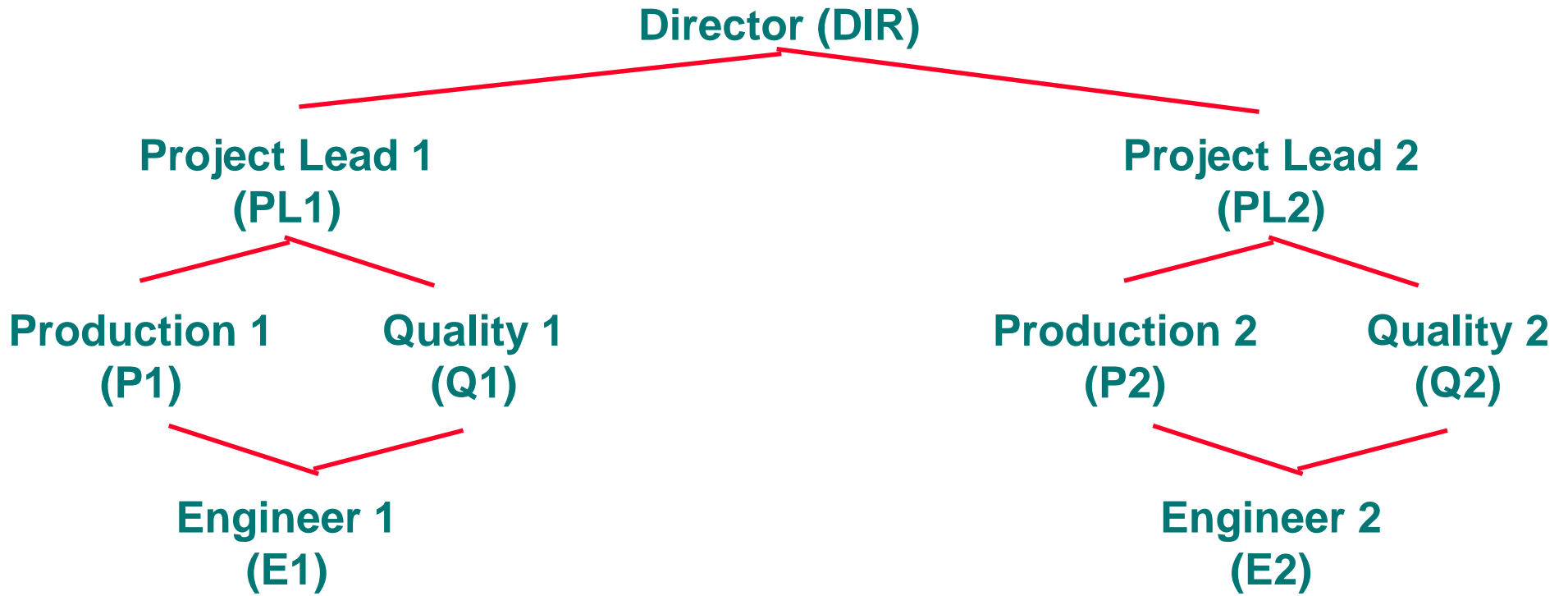
**Supervising
Engineer**

**Software
Engineer'**



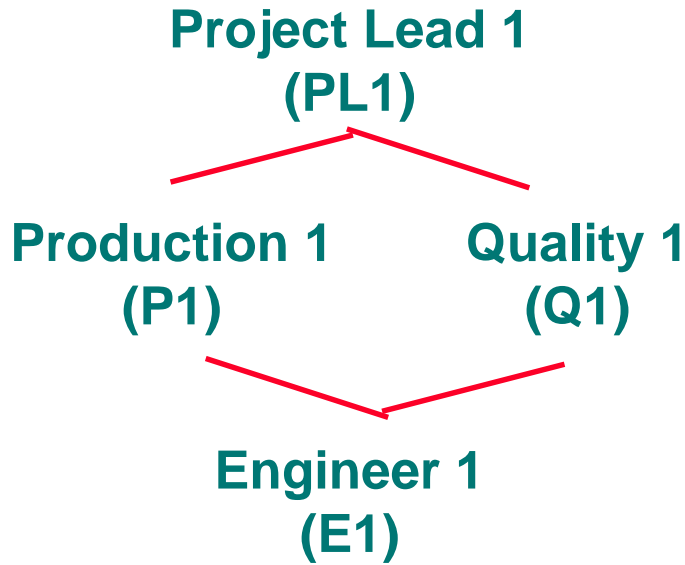




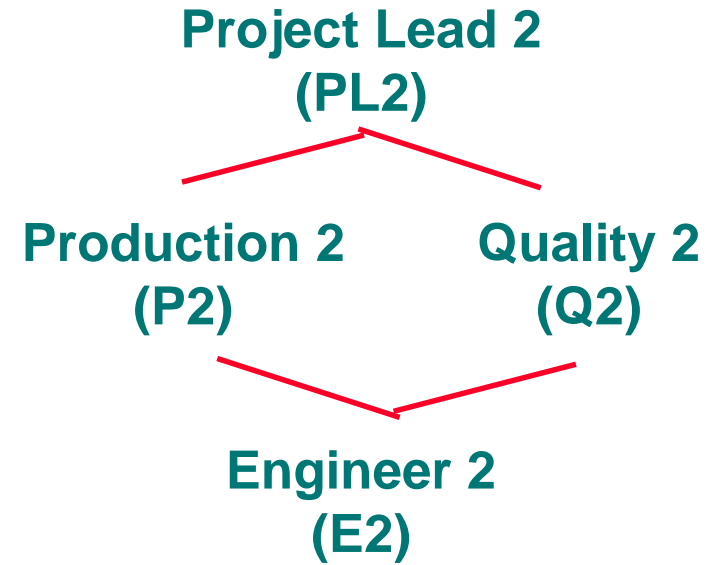


PROJECT 1

PROJECT 2



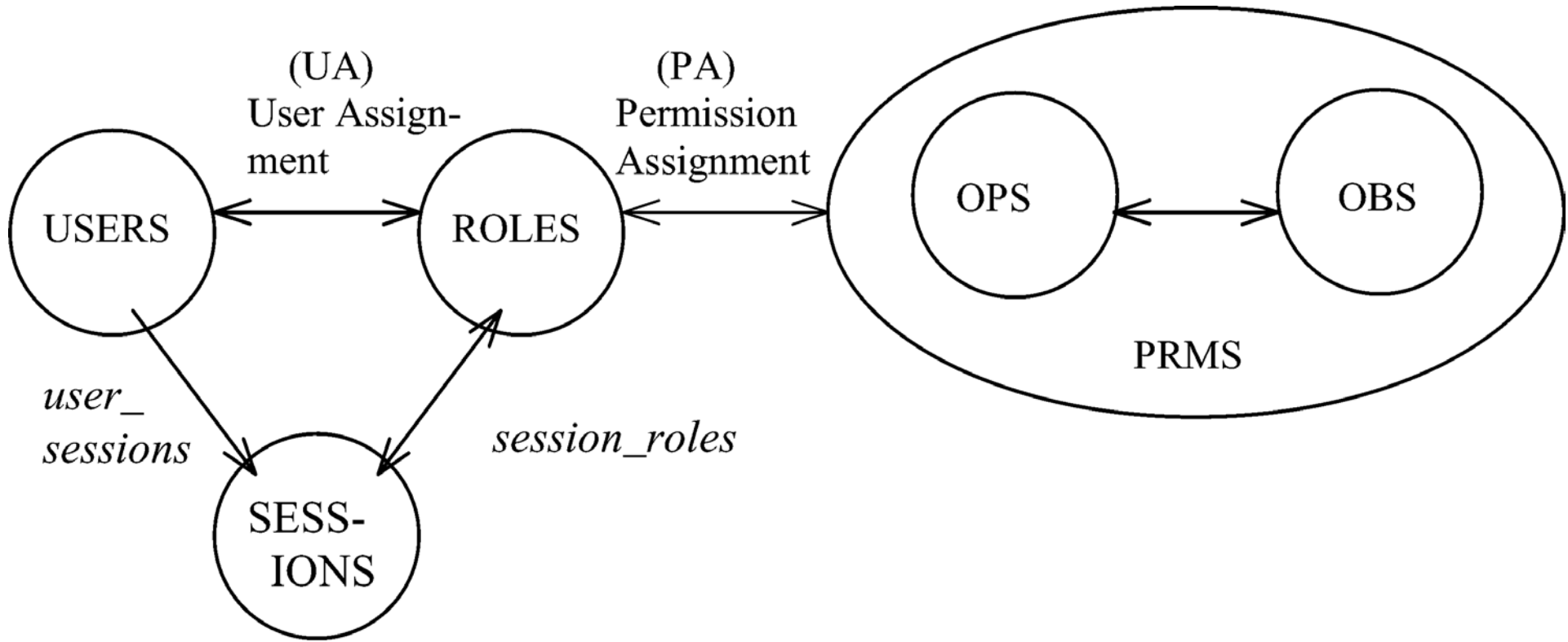
PROJECT 1

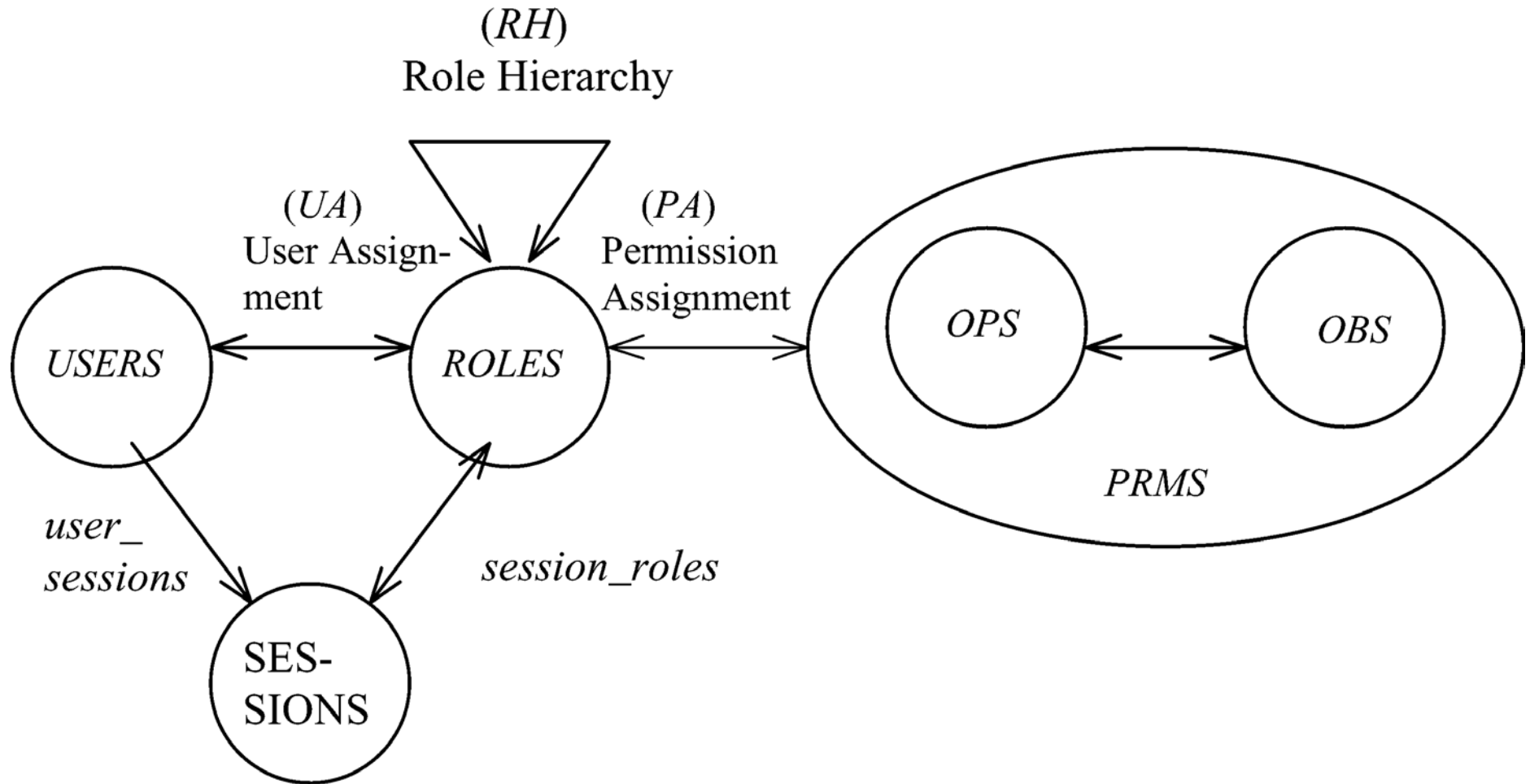


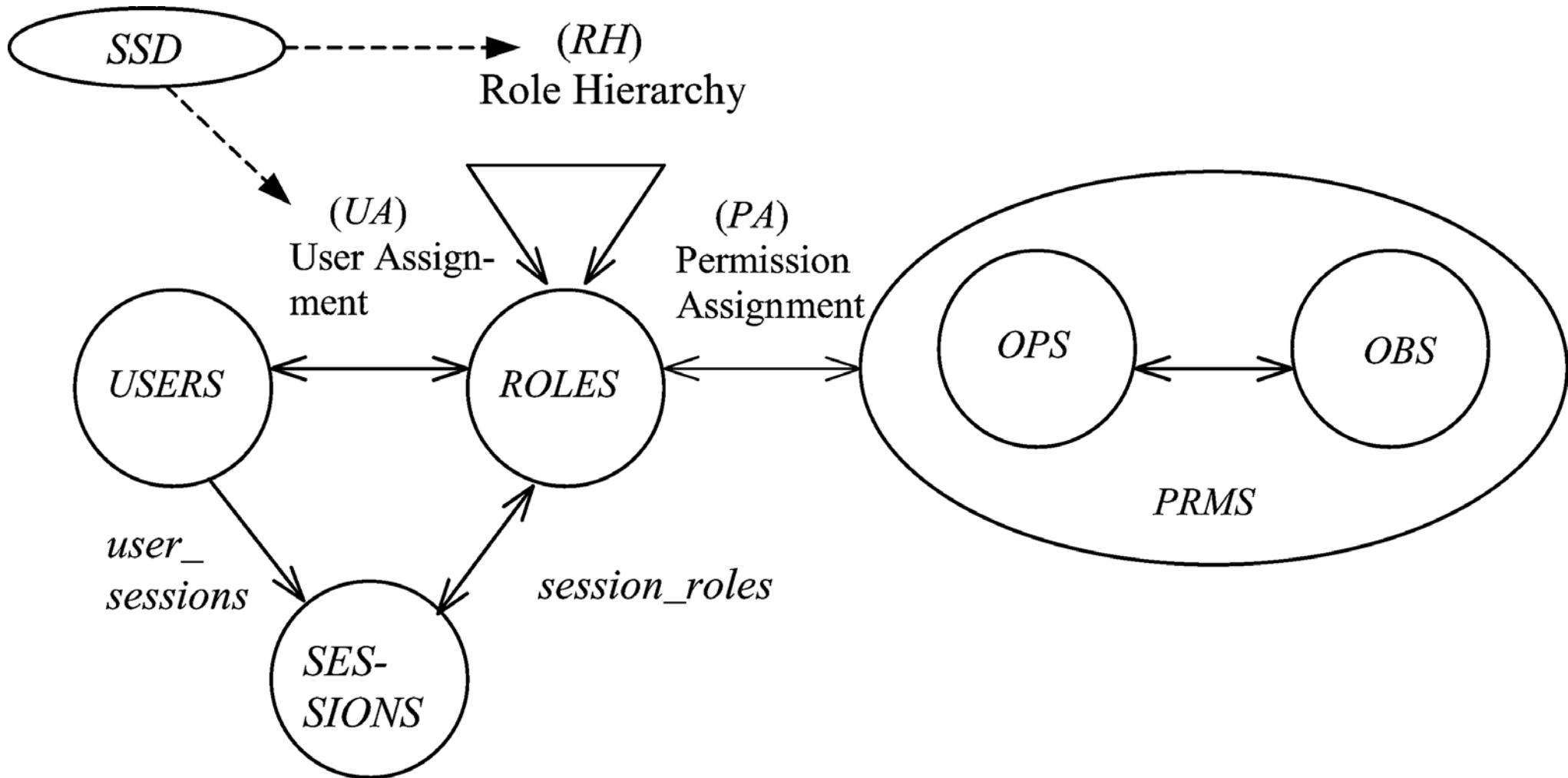
PROJECT 2

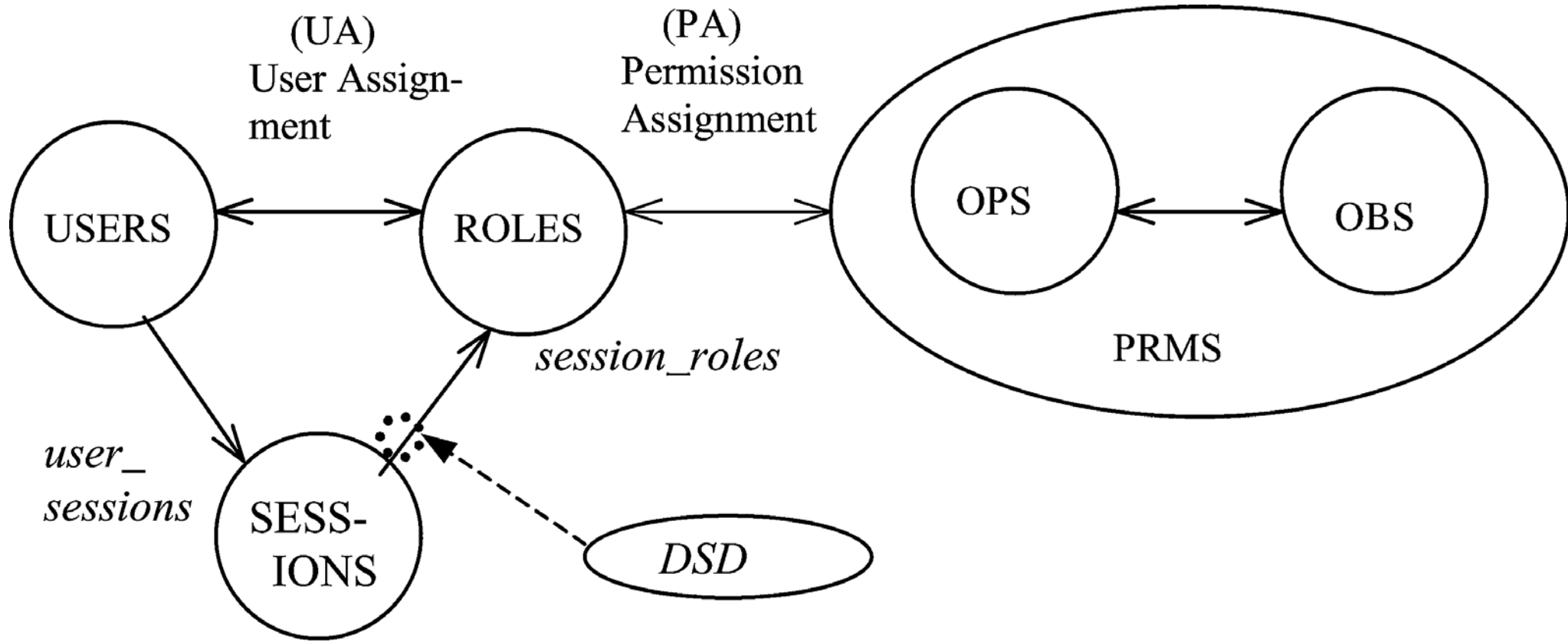
- **Mutually Exclusive Roles**
 - Static Exclusion: The same individual can never hold both roles
 - Dynamic Exclusion: The same individual can never hold both roles in the same context
- **Mutually Exclusive Permissions**
 - Static Exclusion: The same role should never be assigned both permissions
 - Dynamic Exclusion: The same role can never hold both permissions in the same context
- **Cardinality Constraints on User-Role Assignment**
 - At most k users can belong to the role
 - At least k users must belong to the role
 - Exactly k users must belong to the role
- **Cardinality Constraints on Permissions-Role Assignment**
 - At most k roles can get the permission
 - At least k roles must get the permission
 - Exactly k roles must get the permission

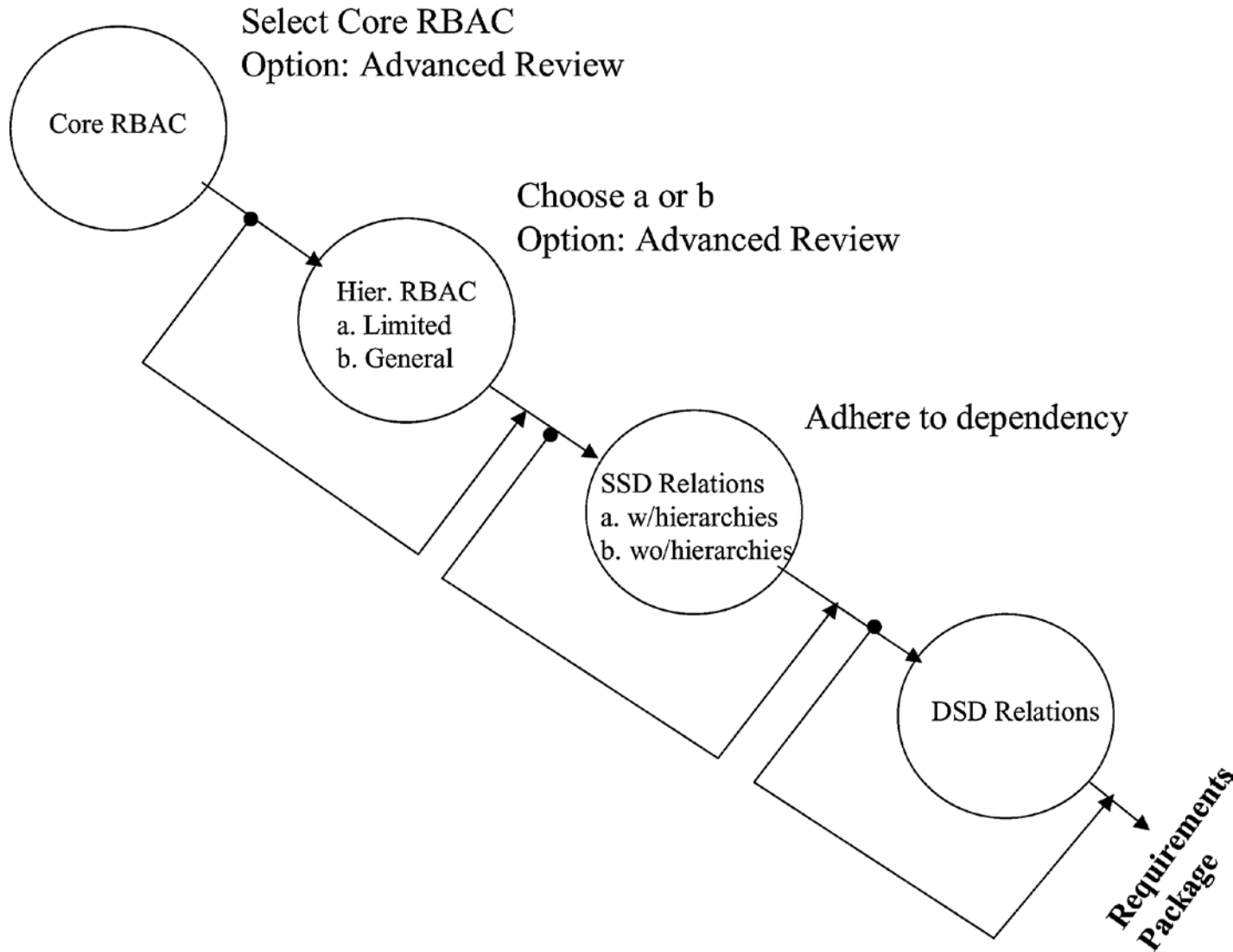
NIST RBAC Model

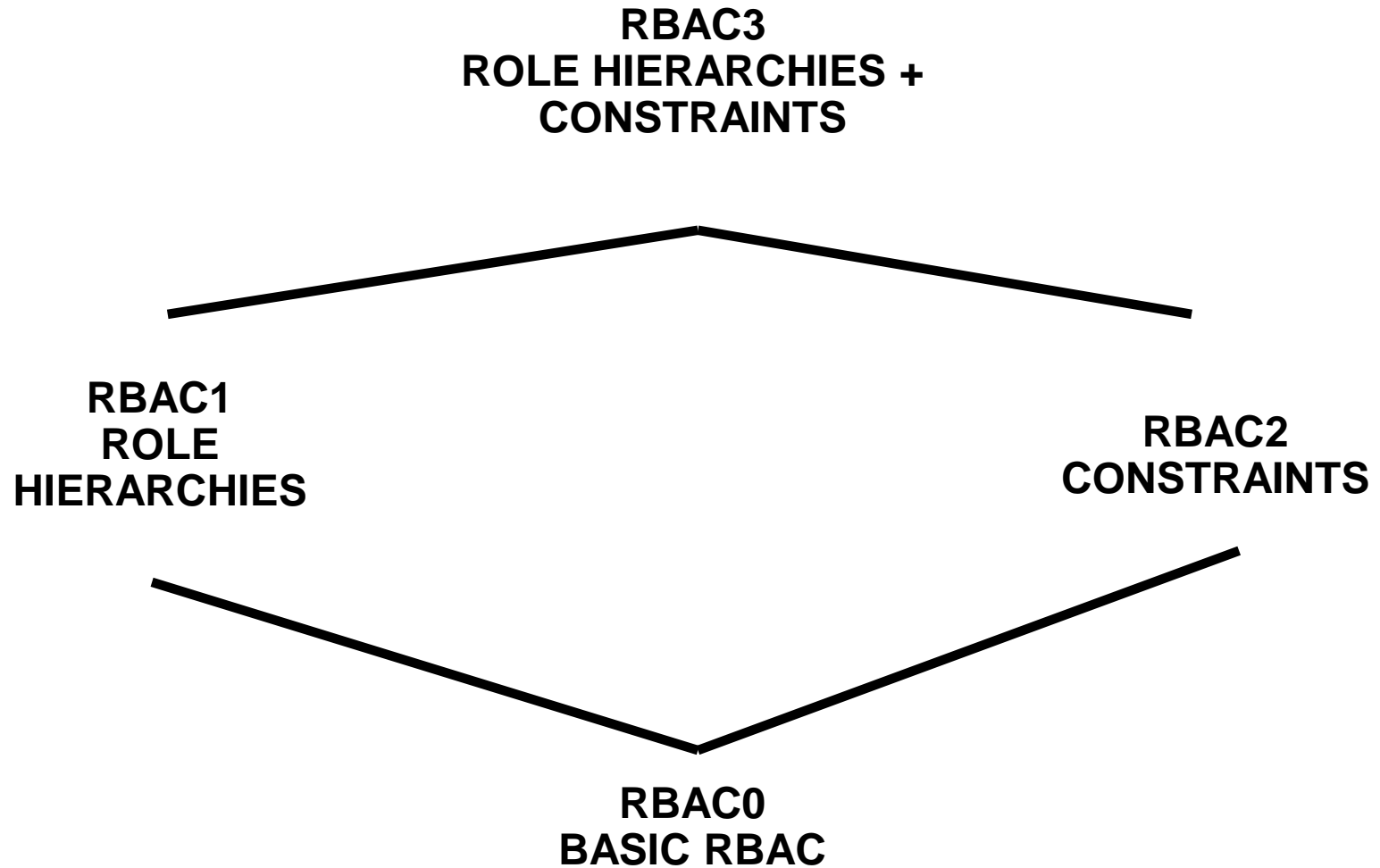












RBAC Administration

ROLE HIERARCHIES

