pilar

PILAR
Asset dependencies

José A. Mañas <jmanas@pilar-tools.com>

October 2020

SRA > method > assets

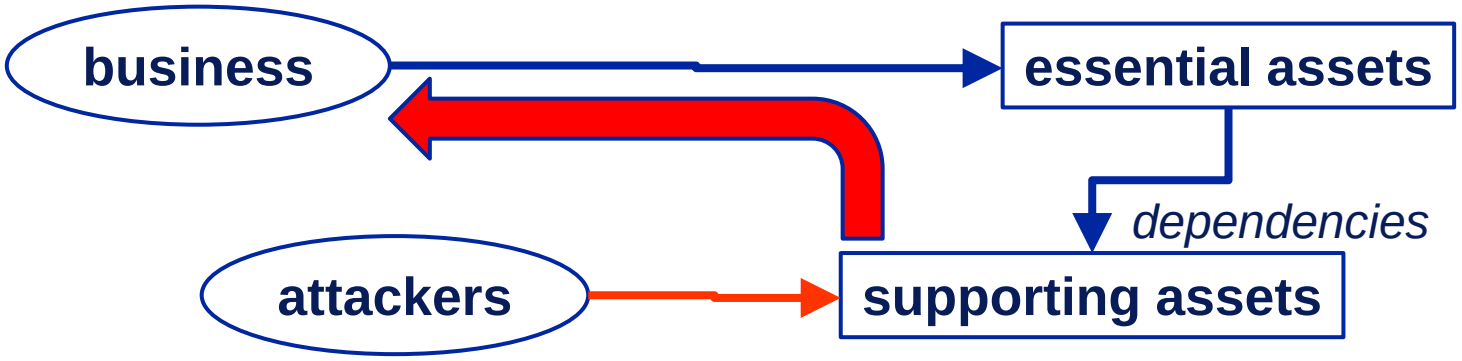
- Magerit
  - resources of the information system, or related to it, necessary so that the organisation works correctly and reaches the objectives proposed by its direction
- ISO
  - Asset. Anything that has value to the organization

SRA > method > assets

- essential assets
  - information and services
  - have a value for the business → security requirements
- supporting assets
  - equipment, communications, media, facilities and personnel
  - have no value by themselves,
    but the value inherited from the business they support (i.e. essential assets)
  - may be subject to incidents
    - accidental
    - deliberate

SRA > method > requirements & consequences

1. business requirements are used as essential assets value
2. value is transferred to supporting assets



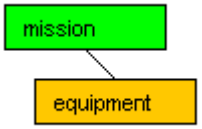
3. attackers act on supporting assets
4. consequences are transferred back onto business impact

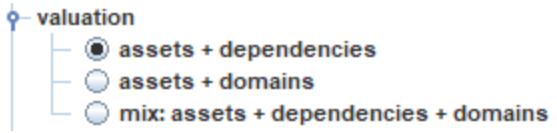
SRA > method > assets

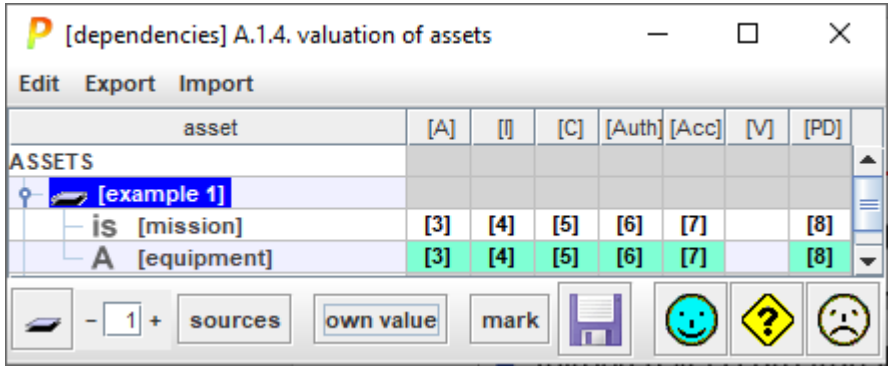
- what is an asset?
  how to identify assets?
- formal: an asset is anything that has value for the organization
  - direct value: essential assets
  - indirect value: supporting assets
- heterodox
  - an asset is anything that may be subject to attack / incident
  - a [structuring] asset is a node that helps to model the transfer of value between assets
  - an asset is a grouping of assets that provide a service
    - i.e. a Service Access Point (e.g. a vpn)

dependencies

- Asset A depends on asset B
  - The security requirements on A are transferred onto B
  - [direct] risks B are transferred onto deflected (indirect) risks on A

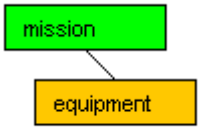






dependencies

- Asset A depends on asset B
  - [direct] risks B are transferred onto deflected (indirect) risks on A



[dependencies] impact & risk > risk.down

View Export

potential | current | target | PILAR

asset	[A]	[I]	[C]	[Aut...	[Acc]	[V]	[PD]
ASSETS	{3.6}	{3.9}	{3.9}	{4.5}			{6.5}
[example 1]	{3.6}	{3.9}	{3.9}	{4.5}			{6.5}
is [mission]							{6.5}
A [equipment]	{3.6}	{3.9}	{3.9}	{4.5}			

1 +1 domain source manage legend

[dependencies] impact & risk > risk.up

Export

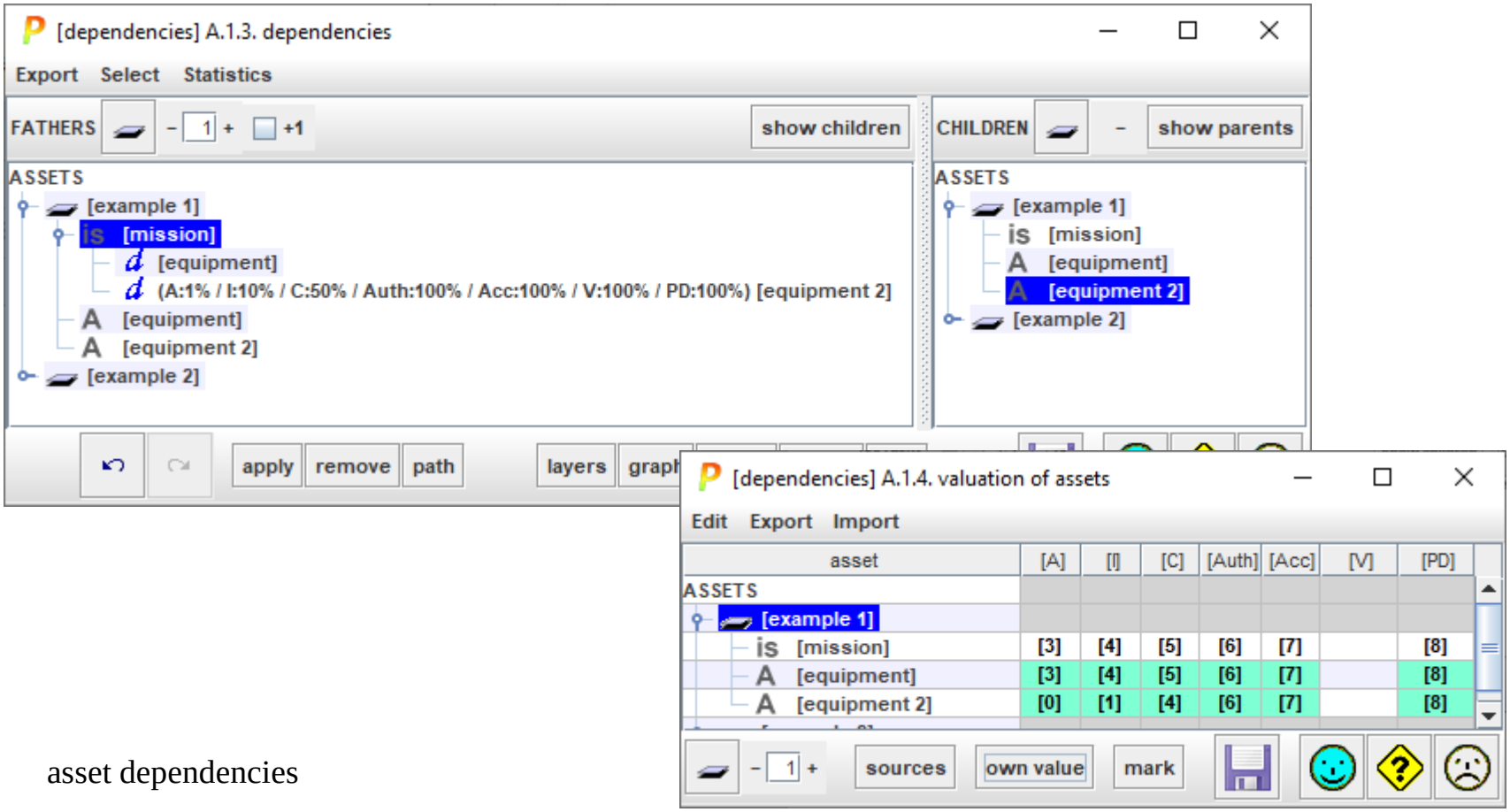
potential | current | target | PILAR

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
ASSETS	{3.6}	{3.9}	{3.9}	{4.5}			{6.5}
is [mission]	{3.6}	{3.9}	{3.9}	{4.5}			{6.5}
[A] Availability	{3.6}						
[equipment]	{3.6}						
[I] Integrity		{3.9}					
[equipment]		{3.9}					
[C] Confidentiality			{3.9}				
[equipment]			{3.9}				
[Auth] Authenticity of users and information				{4.5}			
[Acc] Accountability of service and data							
[PD] Personal data							{6.5}
[mission]							{6.5}

1 manage legend

transfer tuning

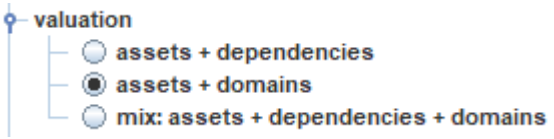
- Asset A depends on asset B
  - you may tune the transfer of values per dimension



asset dependencies

domain valuation

- In each security domain,
  - the aggregated requirements of all essential assets
  - is assigned to every asset in the domain



[dependencies] A.1.4. valuation of assets

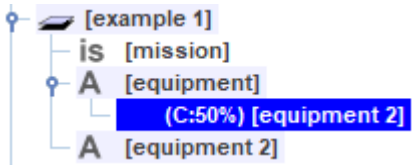
Edit Export Import

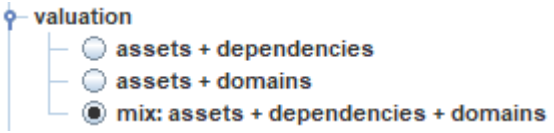
asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
ASSETS							
[example 1]							
IS [mission]	[3]	[4]	[5]	[6]	[7]		[8]
A [equipment]	[3]	[4]	[5]	[6]	[7]		[8]
[example 2]							
I [essential.info]							
A [D.conf]							

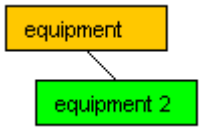
- 1 + sources own value mark

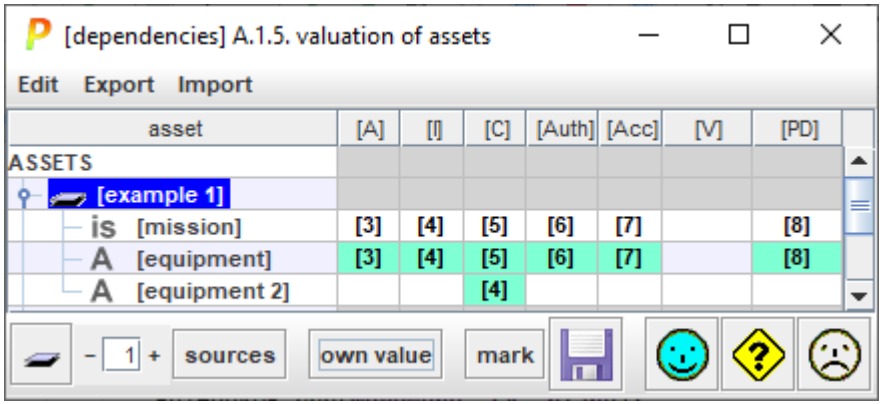
mix valuation

- In each security domain,
  - the aggregated requirements of all essential assets
  - are assigned to every asset in the domain
  - unless the asset has incoming dependencies,
    in which case the dependencies have priority



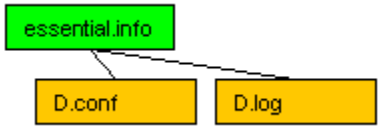


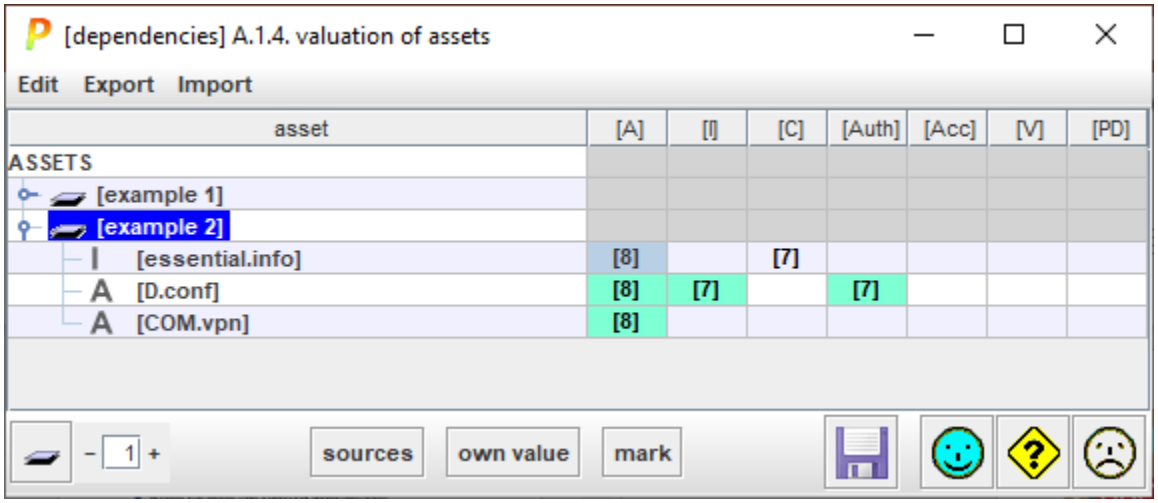




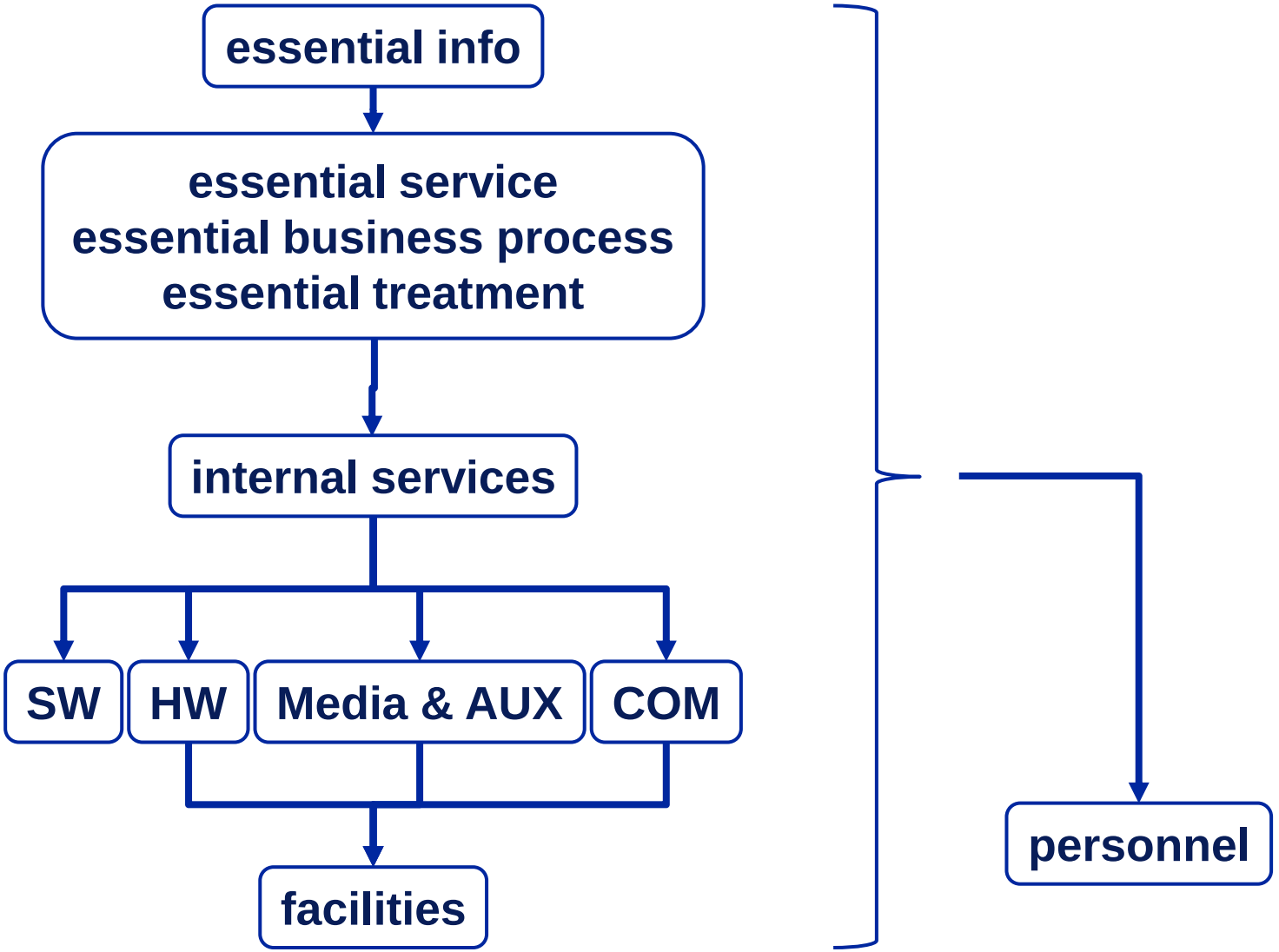
cross-dimension propagation

- The classes of the asset below may condition the transfer of value to protect above





standard dependencies



asset dependencies

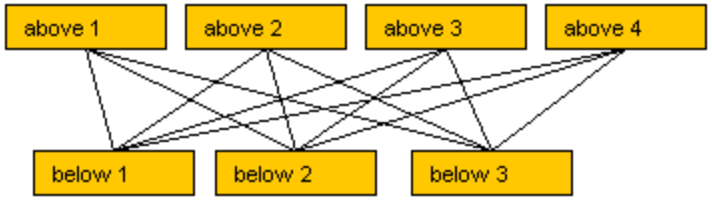
personnel

- essential info → internal users
- services, sw, hw, media, com

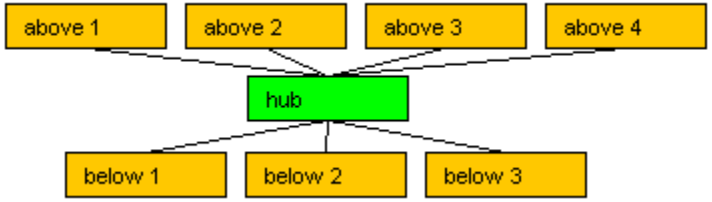
  → system operators and administrators
- sw → developers
- facilities → guards

value distributors

- When there are many-to-many dependencies, the graph is a mess



- You may simplify using service access points



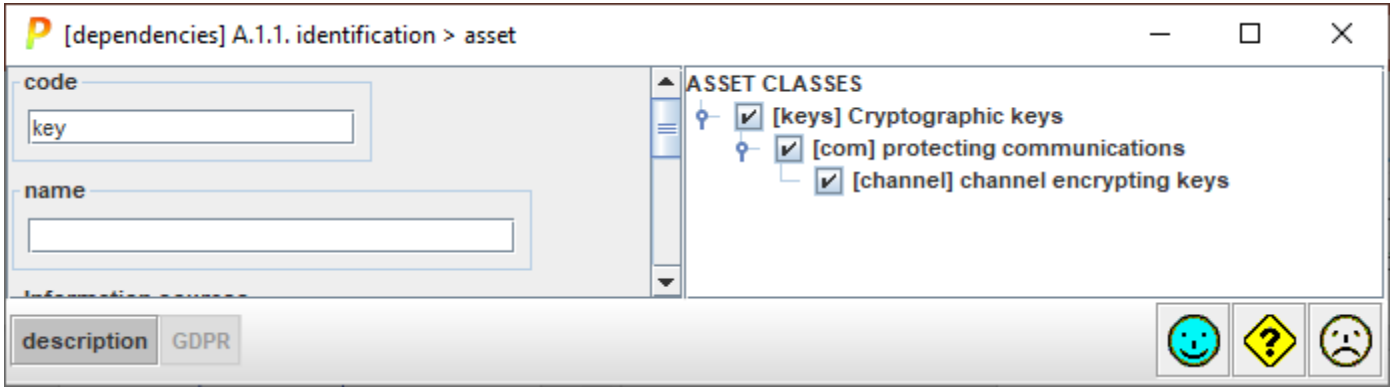
- Now, you may add / remove easily new clients above or new servers below
- It is called object-oriented assets

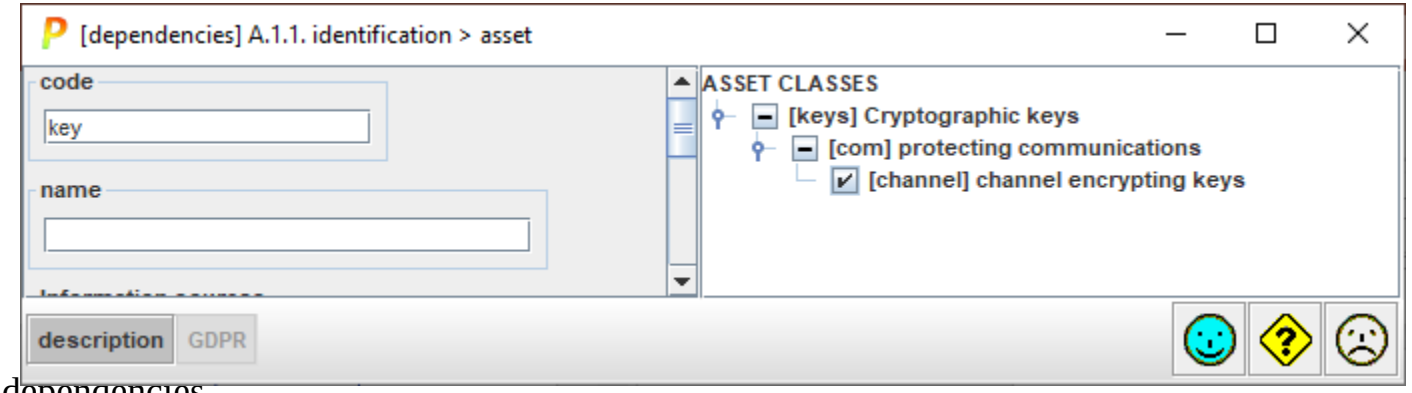
FAQ

- Can I double check that dependencies are right?
- In fact, you should!
  - go to asset valuation
  - switch accumulated values on
  - revise that every supporting asset has a valid value
- Trick
  - is the accumulated value makes sense, it does not matter if the dependencies are right or wrong: the outcome is fine
  - however, poor dependencies may become a nightmare for project maintenance in the future
- Trick
  - if an asset is not valuated, it means it has no security requirements; most likely you forgot some dependency

FAQ

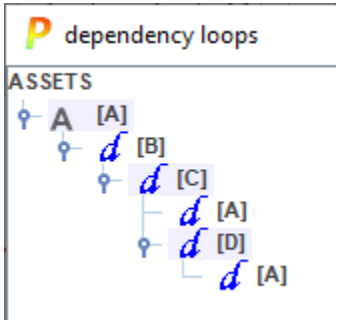
- Marking both general and detail
  - it makes no semantics difference
  - marking only leaves looks cleaner (recommended)

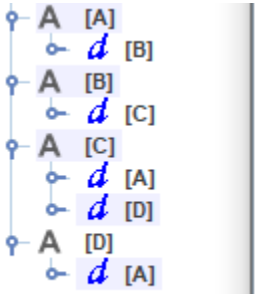


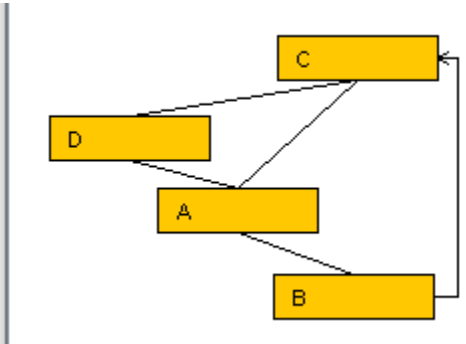


FAQ

- Loops
  - you can set circular loops
  - it is easy to be confused with circular loops
- You can specify behavior of PILAR w.r.t. loops
  - EDIT > options > advanced > ...
    - allow – default in early versions
    - warn – still the loop is allowed
    - no – you cannot set up a circular dependency
- If the model has loops, you identify and edit
  - SELECT > loops







any question?

support@pilar-tools.com