Rational Systems and Software Engineering **Symposium**

Using IBM Rational tools to support Evidence-based Development

Jeremy.Dick@integrate.biz

Order of service

- Who are Integrate?
- Evidence-based Development
    - What is it?
    - The “W” model
    - Traceability rationale
    - Progressive Assurance
- An Evidence-based Development scenario
    - Mixing software and other disciplines
    - What is best in DOORS and in DOORS NG
    - Cross-platform linking

Who are Integrate?

We are an independent company delivering professional systems engineering services and products to clients in government and industry

who do we work for?

defence

BAE SYSTEMS, Rolls-Royce, QinetiQ, THALES, de&s

transport

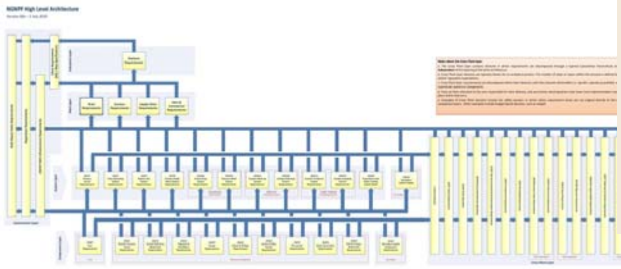
NetworkRail, Department for Transport, NATS, Transport for London, kapsch, EUROTUNNEL

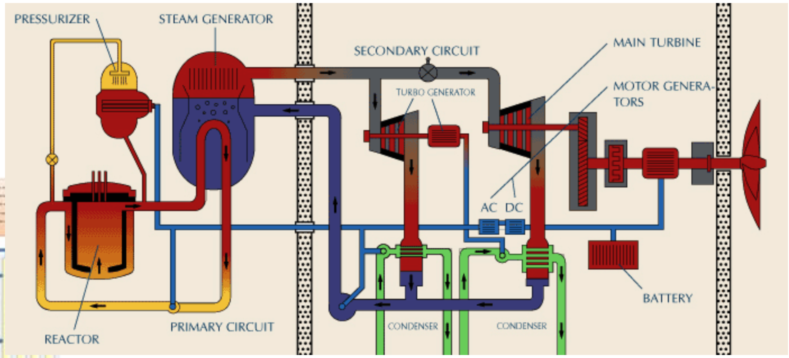
energy

Rolls-Royce, Sellafield Ltd, amec

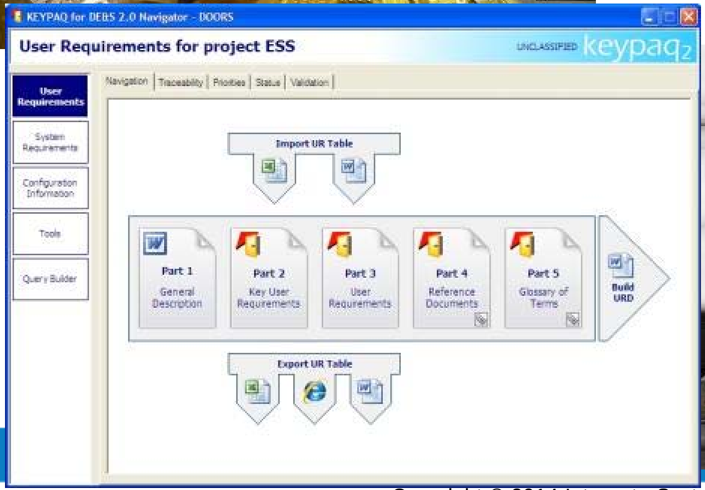
systems engineering of complex systems

- evidence-based development
- e.g. information architecture, processes and tools for managing development of a next generation submarine nuclear propulsion plant





MoD – requirements management



- tools and processes for managing requirements and acceptance information across MoD

Network Rail – systems engineering tools

- software tools for managing requirements and assurance of investment programmes

Relationship with IBM

- IBM is an **Integrate** Premier Business Partner
  - provider of professional services in systems engineering
  - reseller of IBM Rational tools

- **Integrate** employees have over 20 years experience working with DOORS
  - QSS → Telelogic → **Integrate**

IBM Premier Business Partner

Evidence-based Development

EbD – Evidence-based Development

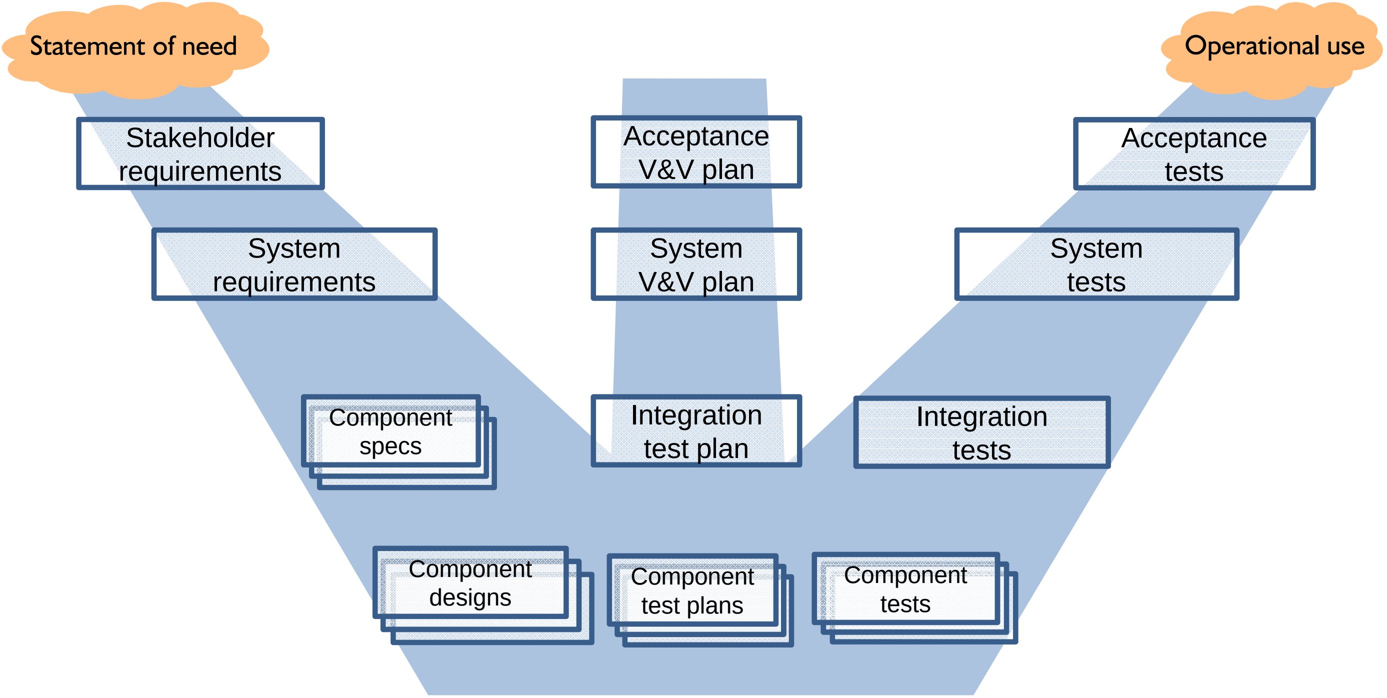
What is it?

- framework for collecting evidence for the correctness of a system as you design the system
- uses requirements traceability as the structure for establishing arguments and supporting evidence
- extends the structured argument paradigm to cover all kinds of requirement – not just safety
- gives ownership of assurance to every engineer

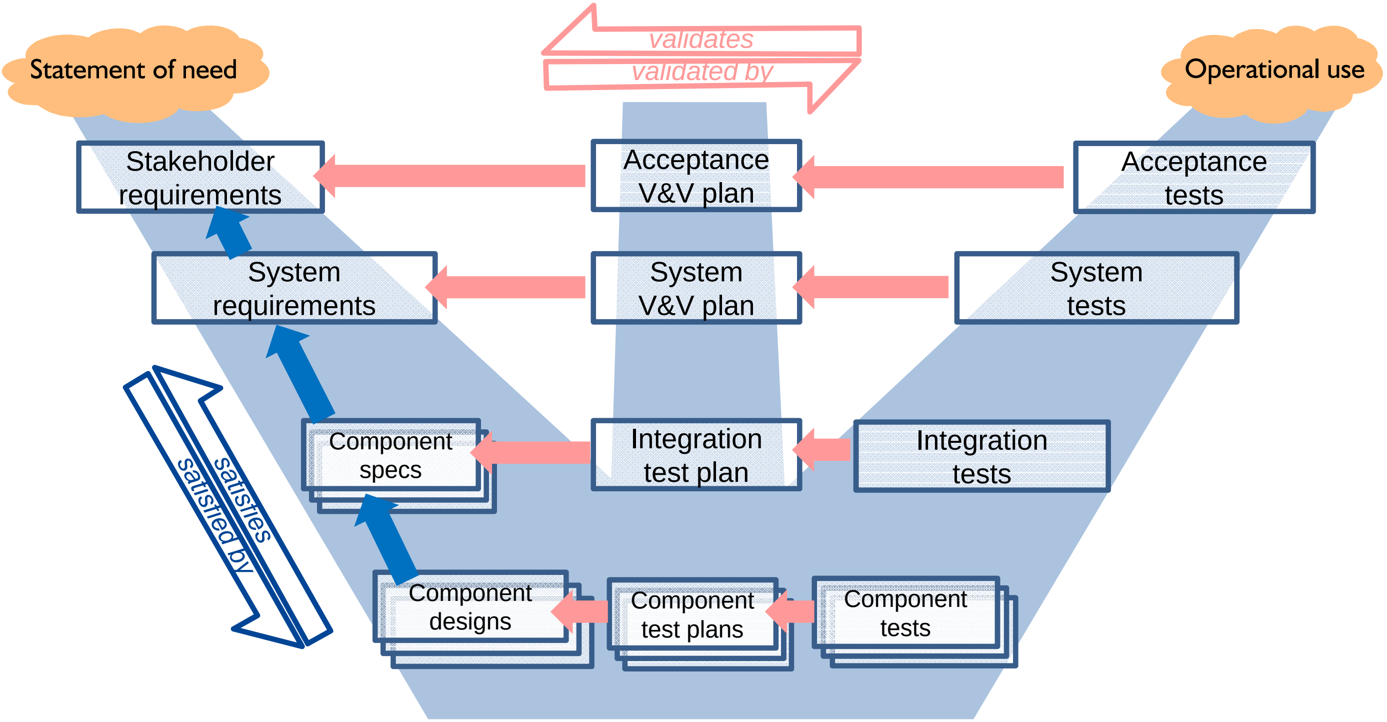
Objectives of EbD

- Connect the assurance case connected to the design
  - the assurance case should not be an “after-thought”
- Develop the assurance case early
  - in time to influence the design
  - in time to save costly rework late in the day
- Apply a uniform approach to all aspects of assurance
  - address all kinds of requirements: function, performance, ease-of-use, reliability, safety, ...
  - have a single point of reference for structured argumentation

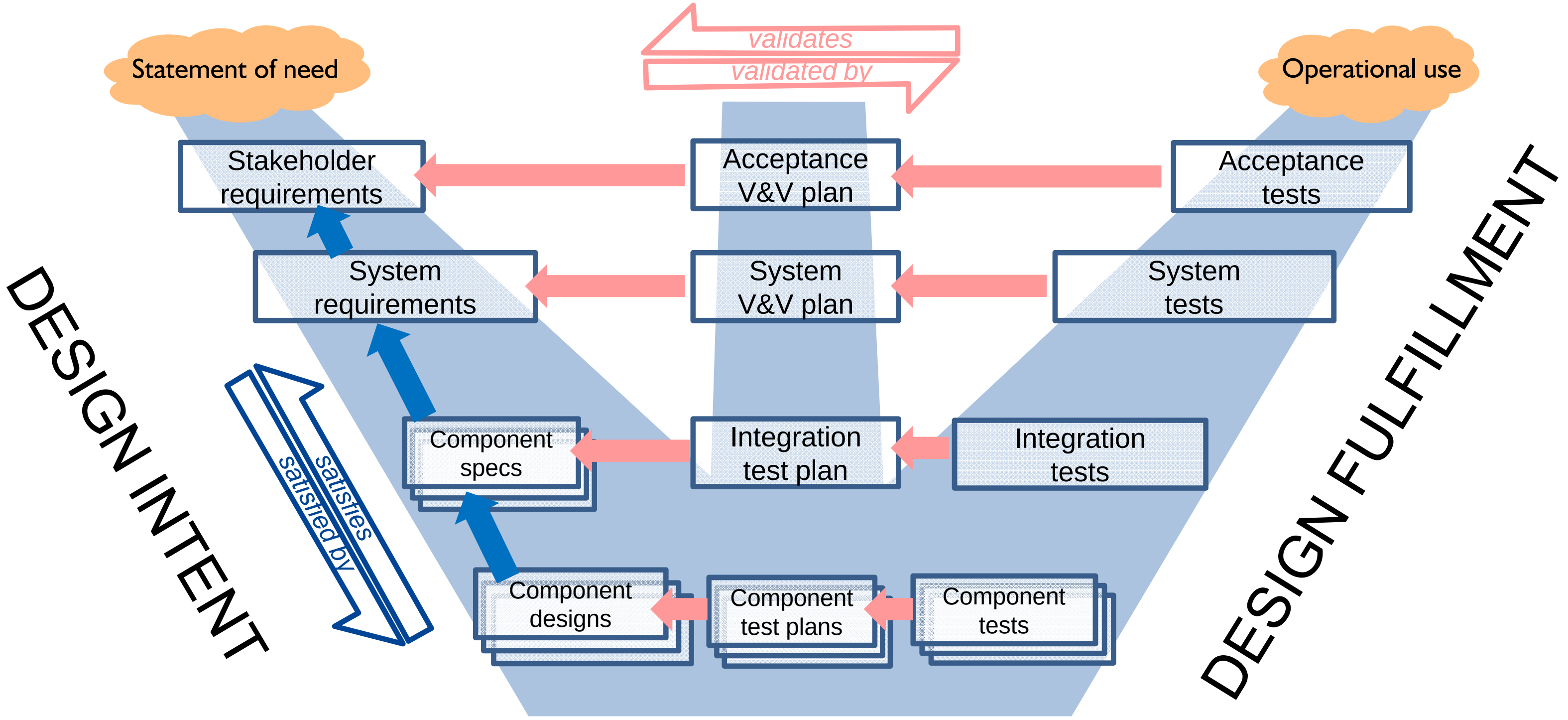
The “W” model


Statement of need
Operational use
Stakeholder requirements
Acceptance V&V plan
Acceptance tests
System requirements
System V&V plan
System tests
Component specs
Integration test plan
Integration tests
Component designs
Component test plans
Component tests

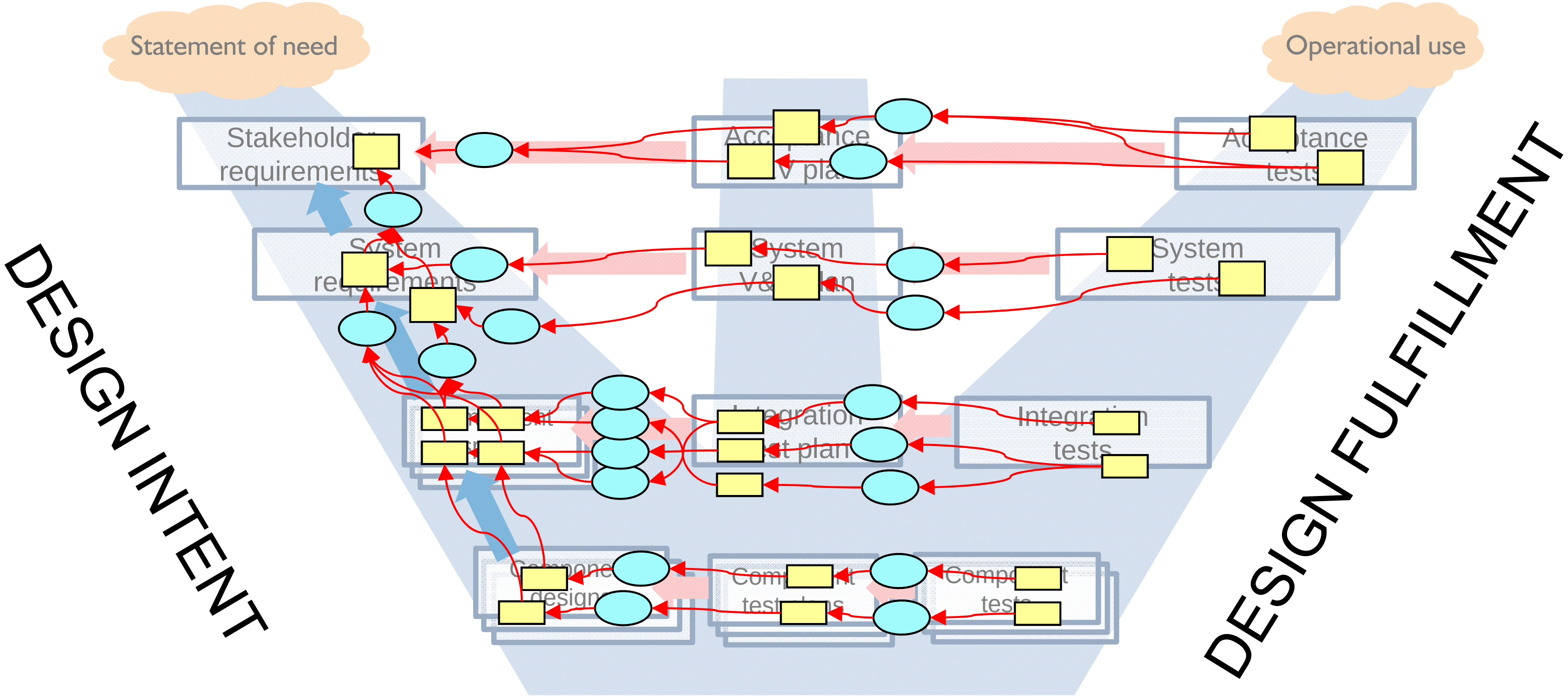
Relationships in the “W” model



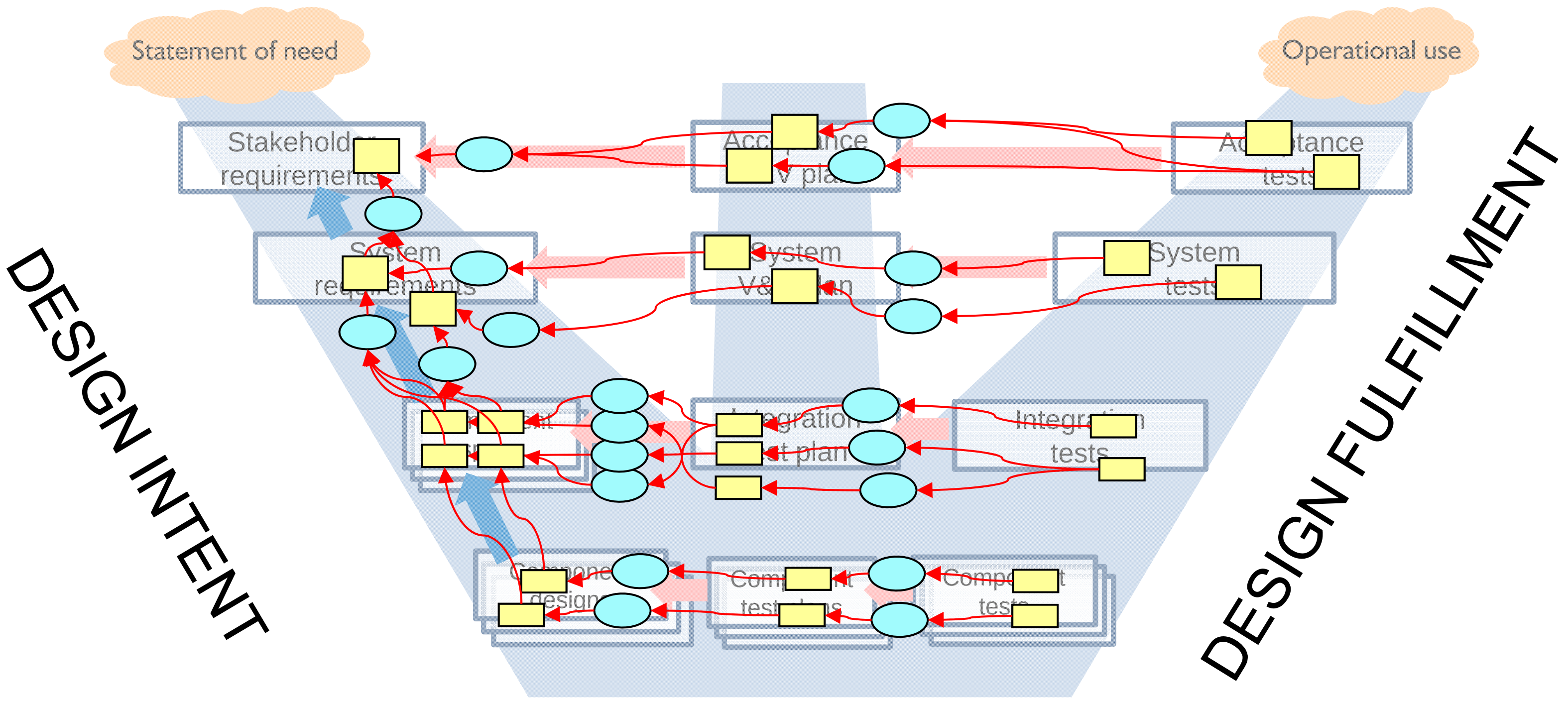
Relationships in the "W" model



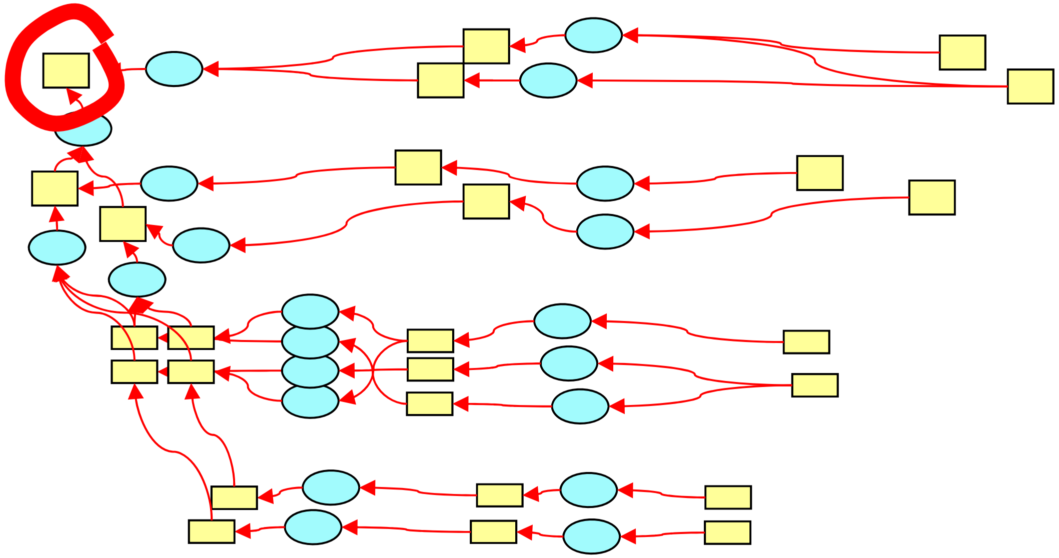
Relationships in the “W” model



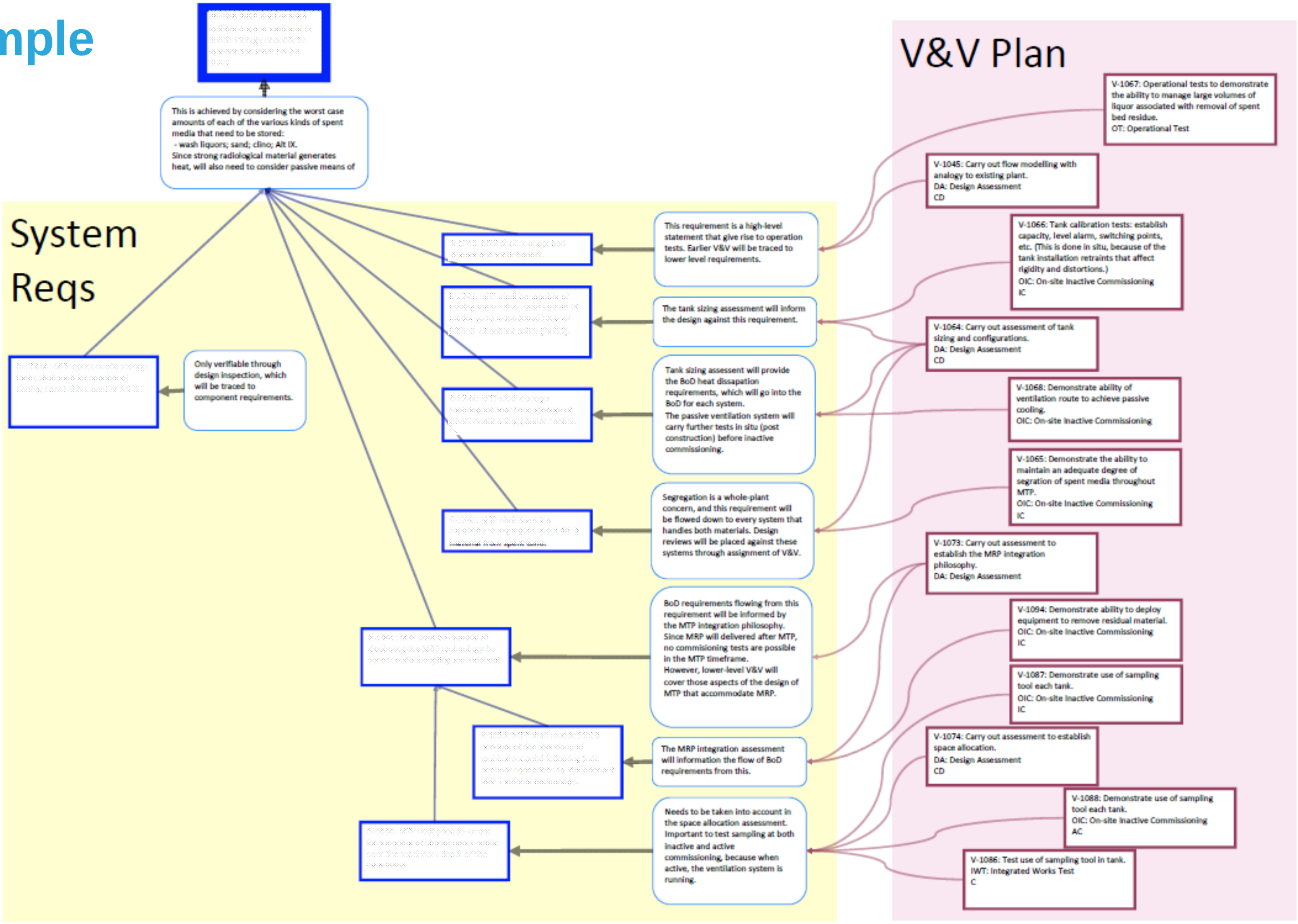
Relationships in the “W” model



Assurance case for one requirement



EbD example



System Reqs

V&V Plan

This is achieved by considering the worst case amounts of each of the various kinds of spent media that need to be stored:
- wash liquors; sand; clino; Alt IX.
Since strong radiological material generates heat, will also need to consider passive means of

Only verifiable through design inspection, which will be traced to component requirements.

This requirement is a high-level statement that give rise to operation tests. Earlier V&V will be traced to lower level requirements.

The tank sizing assessment will inform the design against this requirement.

Tank sizing assessent will provide the BoD heat dissapation requirements, which will go into the BoD for each system.
The passive ventilation system will carry further tests in situ (post construction) before inactive commissioning.

Segregation is a whole-plant concern, and this requirement will be flowed down to every system that handles both materials. Design reviews will be placed against these systems through assignment of V&V.

BoD requirements flowing from this requirement will be informed by the MTP integration philosophy. Since MRP will delivered after MTP, no commisioning tests are possible in the MTP timeframe.
However, lower-level V&V will cover those aspects of the design of MTP that accommodate MRP.

The MRP integration assessment will information the flow of BoD requirements from this.

Needs to be taken into account in the space allocation assessment. Important to test sampling at both inactive and active commissioning, because when active, the ventilation system is running.

V-1067: Operational tests to demonstrate the ability to manage large volumes of liquor associated with removal of spent bed residue.
OT: Operational Test

V-1045: Carry out flow modelling with analogy to existing plant.
DA: Design Assessment
CD

V-1066: Tank calibration tests: establish capacity, level alarm, switching points, etc. (This is done in situ, because of the tank installation retraints that affect rigidity and distortions.)
OIC: On-site Inactive Commissioning
IC

V-1064: Carry out assessment of tank sizing and configurations.
DA: Design Assessment
CD

V-1068: Demonstrate ability of ventilation route to achieve passive cooling.
OIC: On-site Inactive Commissioning

V-1065: Demonstrate the ability to maintain an adequate degree of segration of spent media throughout MTP.
OIC: On-site Inactive Commissioning
IC

V-1073: Carry out assessment to establish the MRP integration philosophy.
DA: Design Assessment

V-1094: Demonstrate ability to deploy equipment to remove residual material.
OIC: On-site Inactive Commissioning
IC

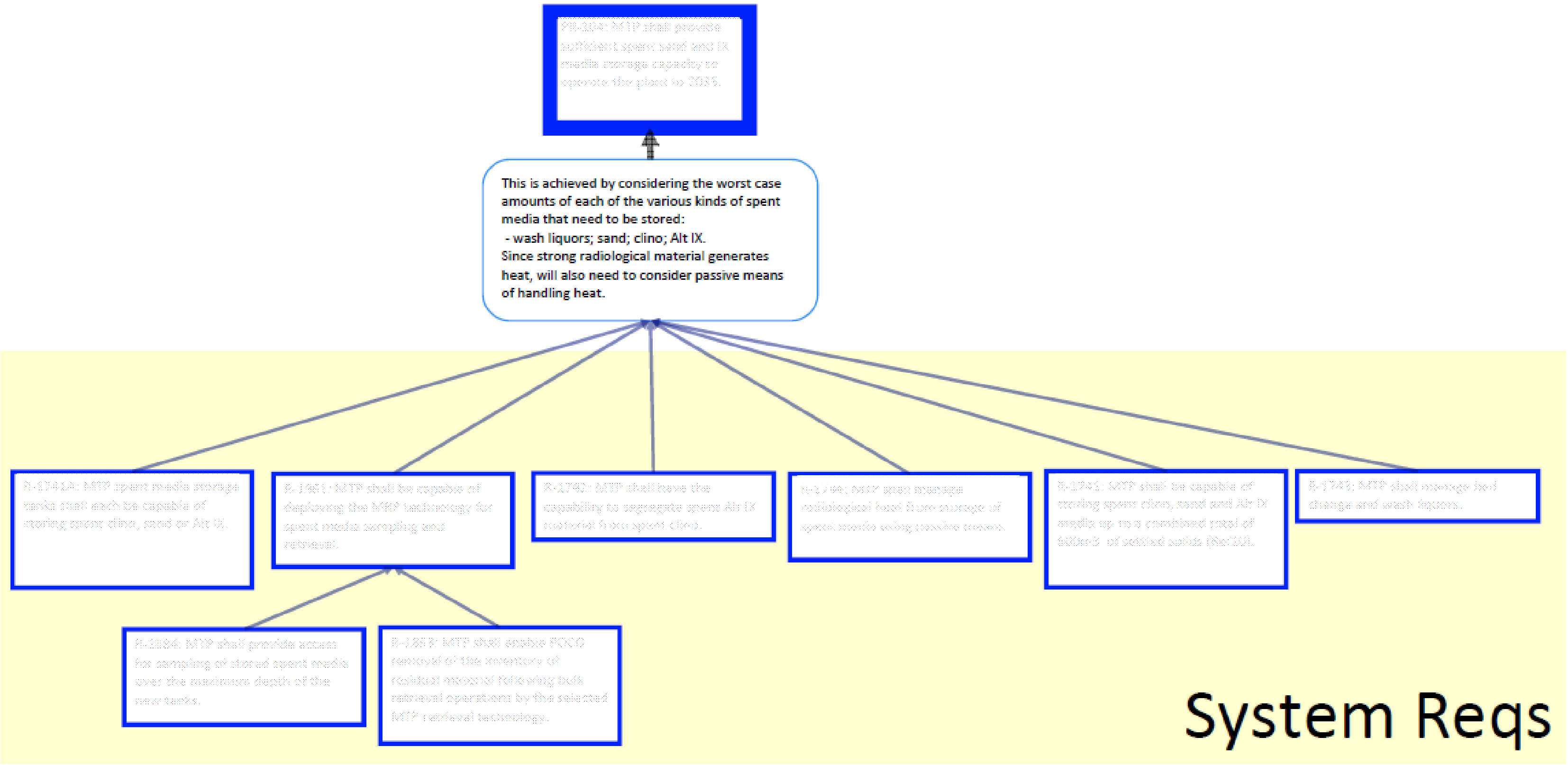
V-1087: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
IC

V-1074: Carry out assessment to establish space allocation.
DA: Design Assessment
CD

V-1088: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
AC

V-1086: Test use of sampling tool in tank.
IWT: Integrated Works Test
C

requirements flow-down



PR-104: MTP shall provide sufficient spent sand and IX media storage capacity to operate the plant to 2055.

This is achieved by considering the worst case amounts of each of the various kinds of spent media that need to be stored:
- wash liquors; sand; clino; Alt IX.
Since strong radiological material generates heat, will also need to consider passive means of handling heat.

R-1741A: MTP spent media storage tanks shall each be capable of storing spent clino, sand or Alt IX.

R-1961: MTP shall be capable of deploying the MRP technology for spent media sampling and retrieval.

R-1742: MTP shall have the capability to segregate spent Alt IX material from spent clino.

R-1744: MTP shall manage radiological heat from storage of spent media using passive means.

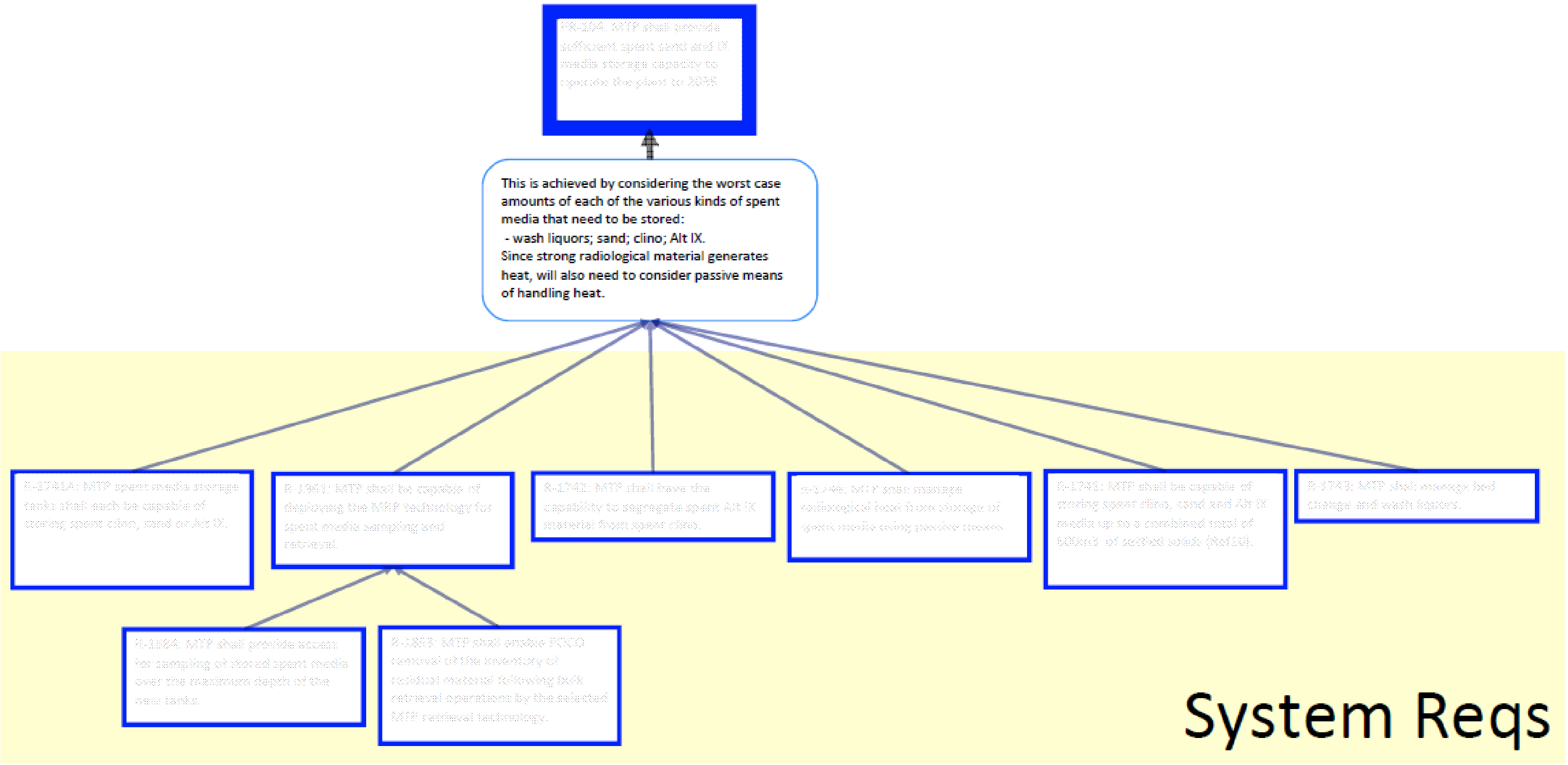
R-1741: MTP shall be capable of storing spent clino, sand and Alt IX media up to a combined total of 600m3 of settled solids (Ref10).

R-1743: MTP shall manage bed change and wash liquors.

R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

R-1853: MTP shall enable POCO removal of the inventory of residual material following bulk retrieval operations by the selected MTP retrieval technology.

requirements flow-down



PR-104: MTP shall provide sufficient spent sand and IX media storage capacity to operate the plant to 2058

This is achieved by considering the worst case amounts of each of the various kinds of spent media that need to be stored:
- wash liquors; sand; clino; Alt IX.
Since strong radiological material generates heat, will also need to consider passive means of handling heat.

R-1741A: MTP spent media storage tanks shall each be capable of storing spent clino, sand or Alt IX.

R-1961: MTP shall be capable of deploying the MRP technology for spent media sampling and retrieval.

R-1742: MTP shall have the capability to segregate spent Alt IX material from spent clino.

R-1744: MTP shall manage radiological heat from storage of spent media using passive means

R-1741: MTP shall be capable of storing spent clino, sand and Alt IX media up to a combined total of 600m3 of settled solids (Ref10).

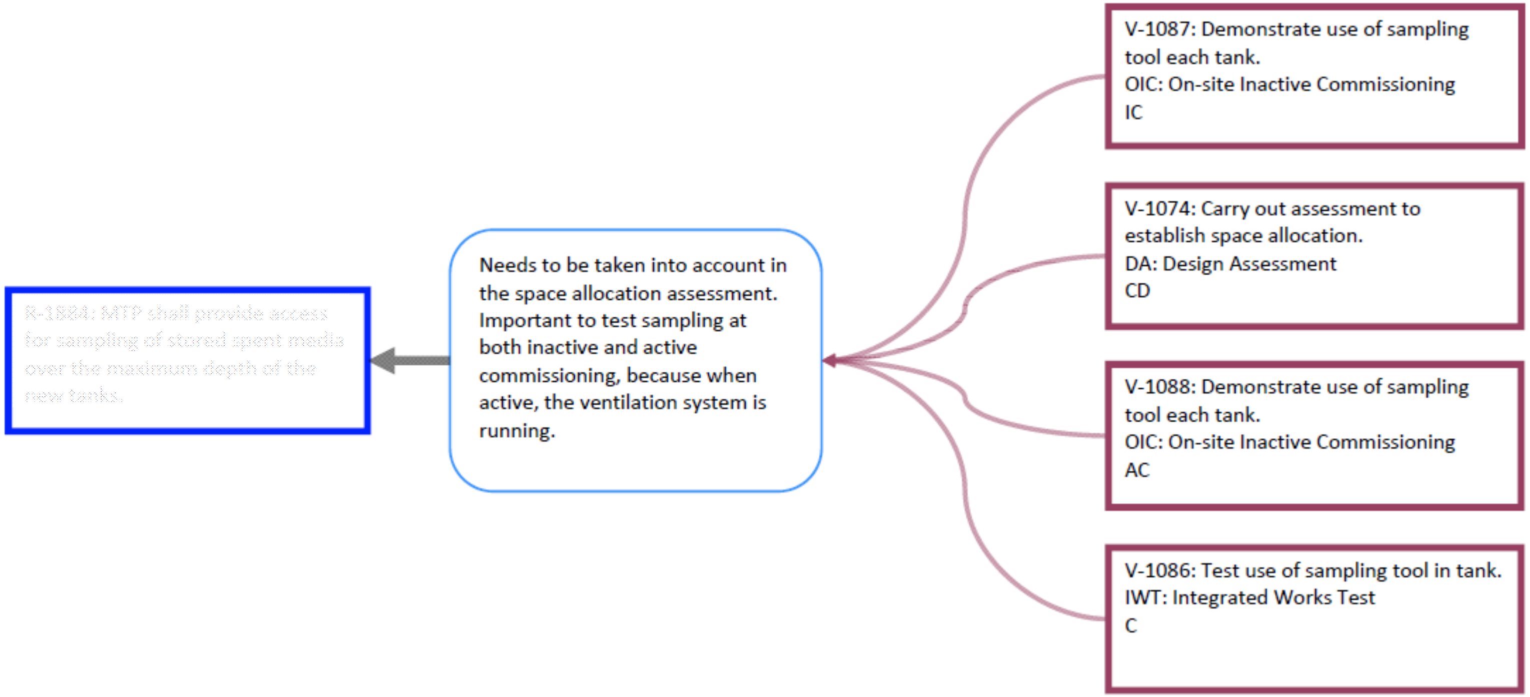
R-1743: MTP shall manage bed change and wash liquors.

R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

R-1883: MTP shall enable POCO removal of the inventory of residual material following bulk retrieval operations by the selected MTP retrieval technology.

System Reqs

validation statement



R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

Needs to be taken into account in the space allocation assessment. Important to test sampling at both inactive and active commissioning, because when active, the ventilation system is running.

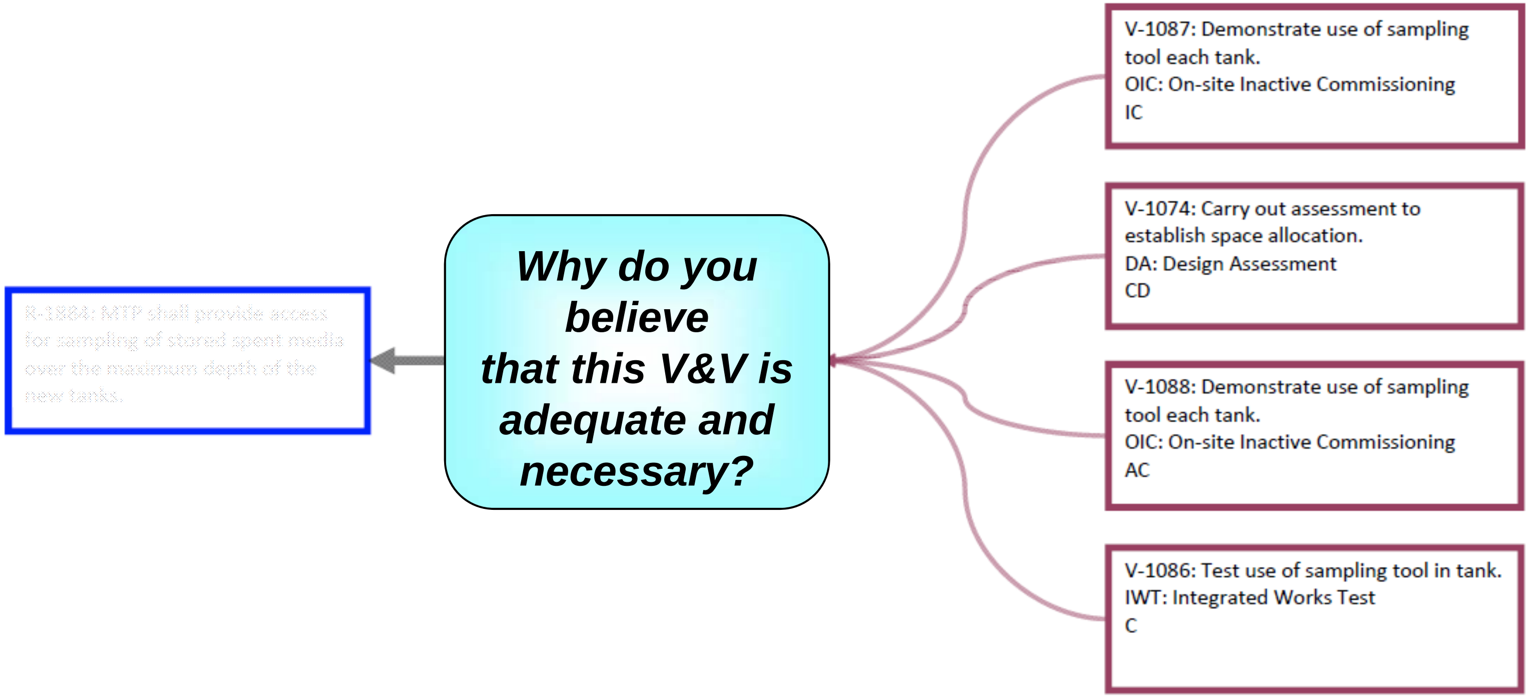
V-1087: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
IC

V-1074: Carry out assessment to establish space allocation.
DA: Design Assessment
CD

V-1088: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
AC

V-1086: Test use of sampling tool in tank.
IWT: Integrated Works Test
C

validation statement



R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

Why do you believe that this V&V is adequate and necessary?

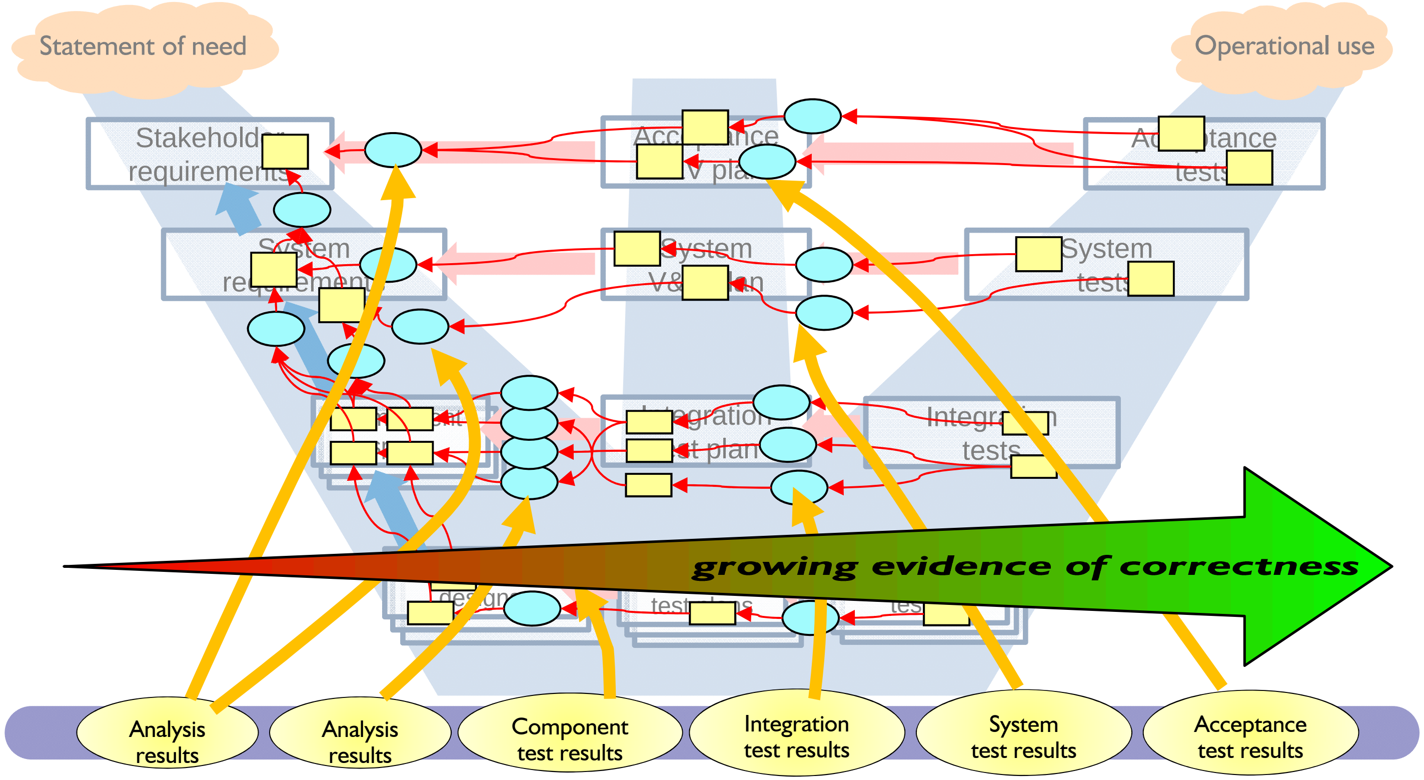
V-1087: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
IC

V-1074: Carry out assessment to establish space allocation.
DA: Design Assessment
CD

V-1088: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
AC

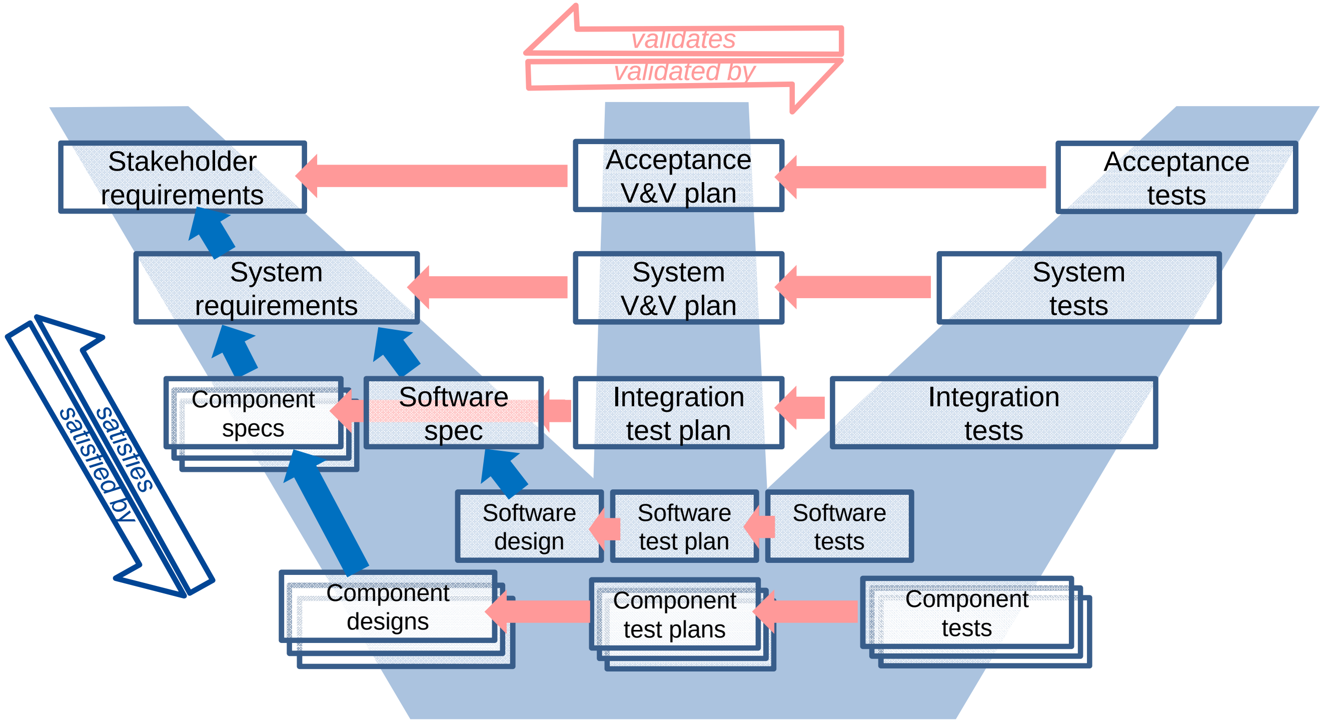
V-1086: Test use of sampling tool in tank.
IWT: Integrated Works Test
C

Relationships in the “W” model

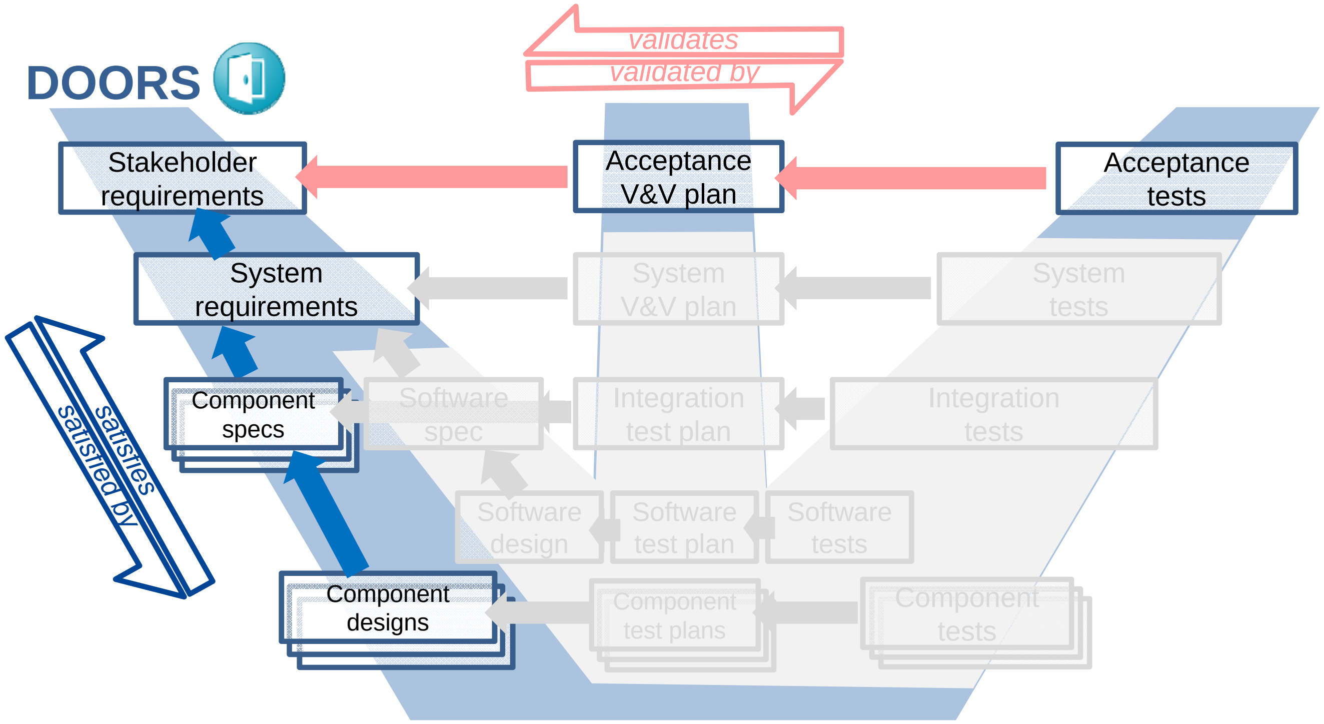


EbD scenario using the IBM Rational toolset

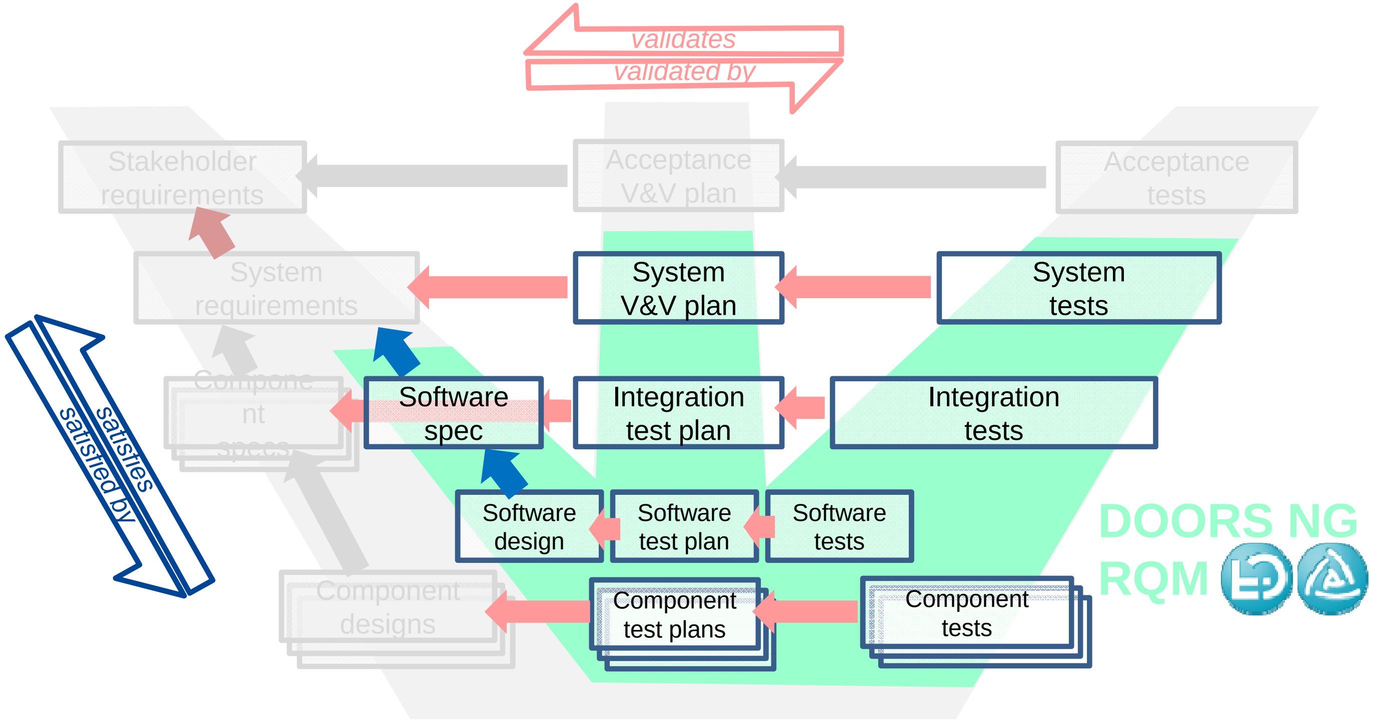
Example scenario: hard components and software



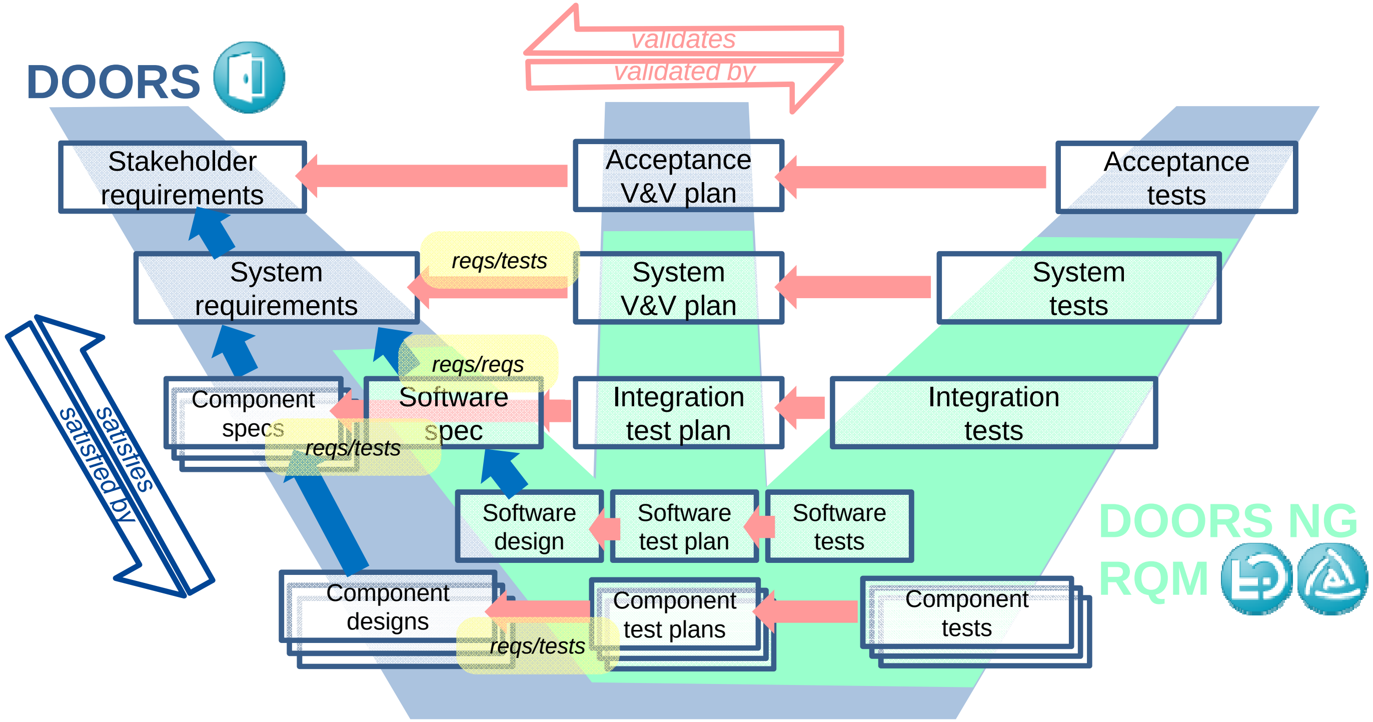
Example scenario: scope of what is managed in DOORS



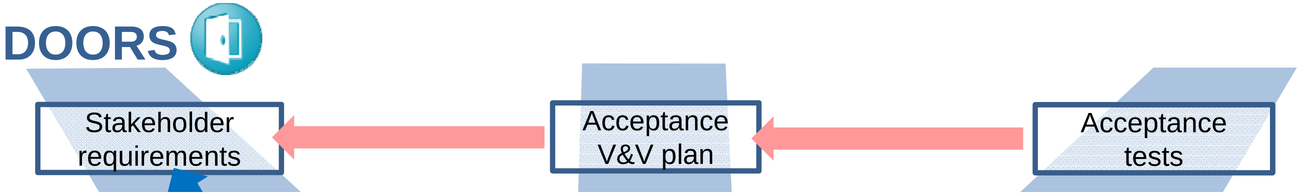
Example scenario: scope of what is managed in DOORS NG/RQM



Example scenario: cross tool linking

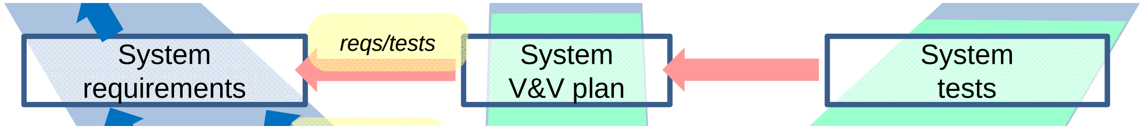


Example scenario: stakeholder layer



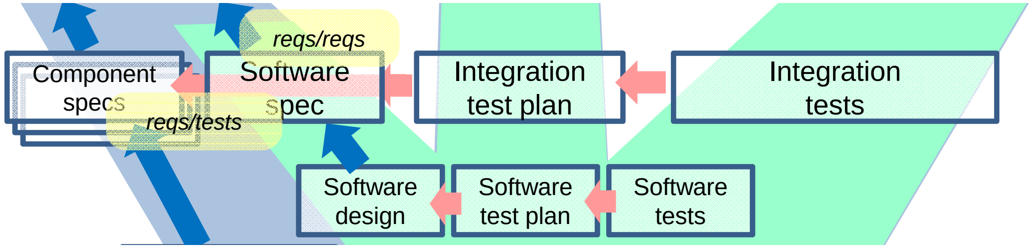
- Acceptance tests are broad-reaching
- No particular benefit in the formality offered by RQM
- Manage the acceptance plan and supporting evidence all in DOORS

Example scenario: system layer



- System test plan is more formal, but not automatable
- Use RQM with manual test scripts
- Use cross-tool linking between DOORS and RQM using OSLC

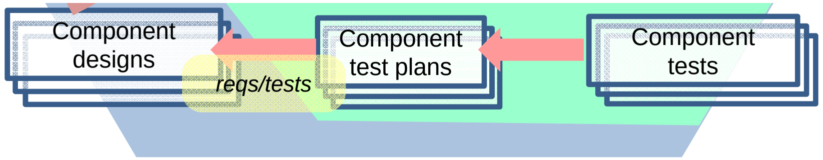
Example scenario: component specification layer



- Software benefits from RTC/RQM life-cycle and automated testing features
- Use DOORS NG and RQM with automated test scripts
- Use linking within Jazz between DOORS NG and RQM

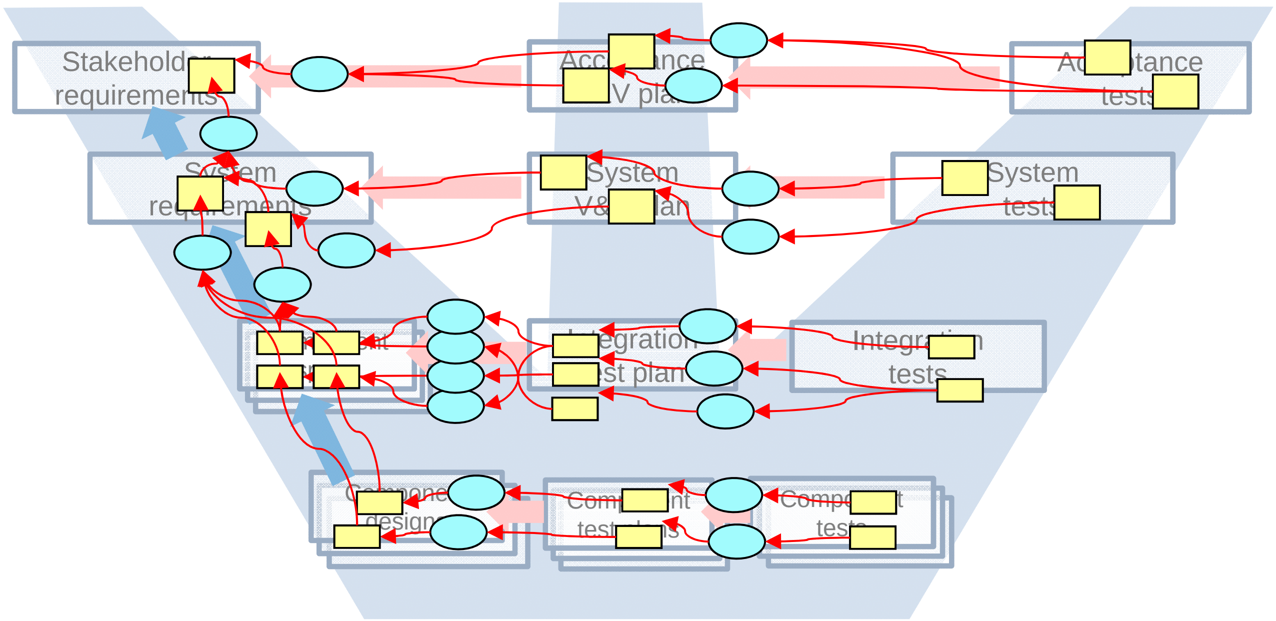
- Non-software component specs in DOORS and RQM, like system tests

Example scenario: component design layer



- Non-software component designs in DOORS and RQM, like system tests

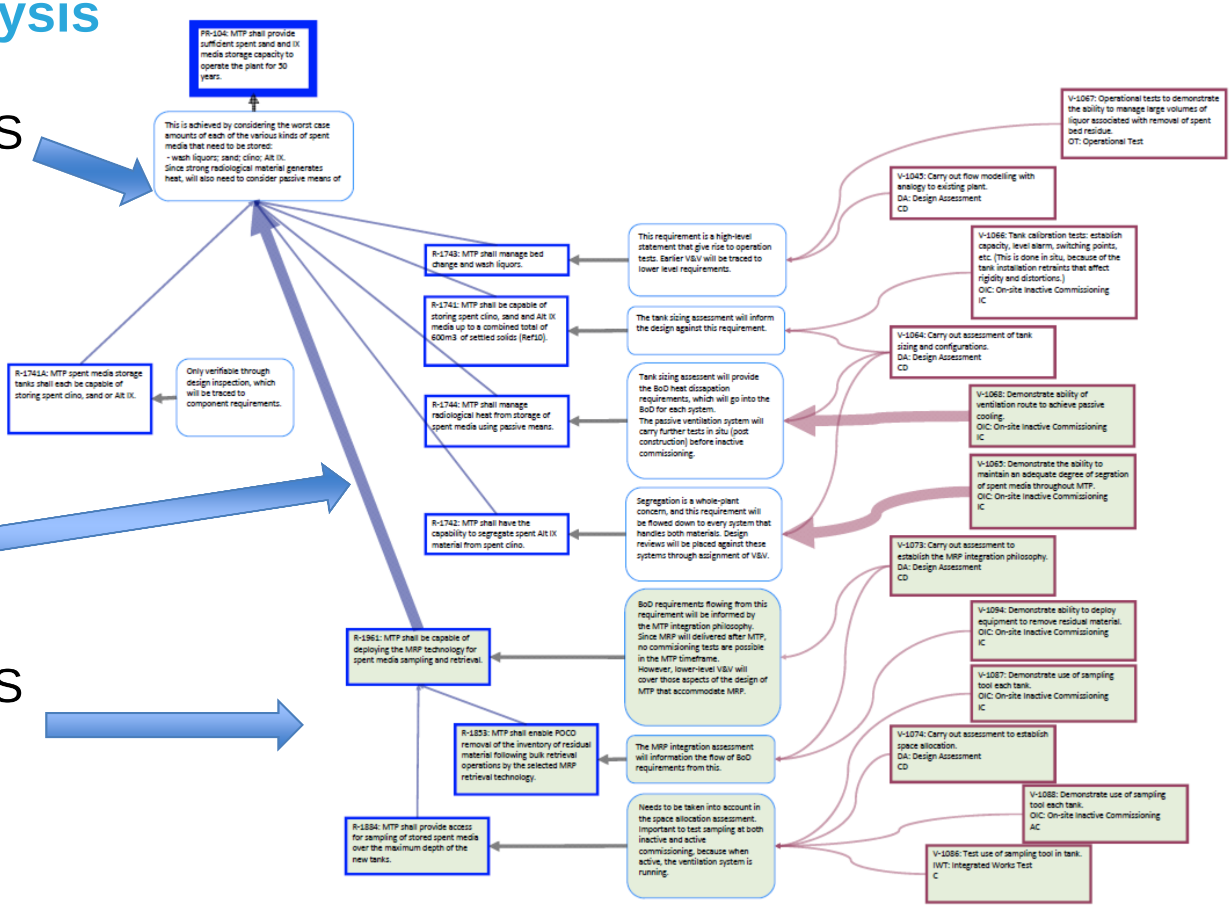
Example scenario: traceability relationale



- Rationale managed as attributes in DOORS and in DOORS NG
- Rationale managed as descriptive text in test cases in RQM

Cross-tool impact analysis

- data managed in DOORS
- cross-platform links
- data managed in DOORS NG and RQM



PR-104: MTP shall provide sufficient spent sand and IX media storage capacity to operate the plant for 50 years.

This is achieved by considering the worst case amounts of each of the various kinds of spent media that need to be stored:
- wash liquors; sand; clino; Alt IX.
Since strong radiological material generates heat, will also need to consider passive means of

R-1741A: MTP spent media storage tanks shall each be capable of storing spent clino, sand or Alt IX.

Only verifiable through design inspection, which will be traced to component requirements.

R-1743: MTP shall manage bed change and wash liquors.

This requirement is a high-level statement that give rise to operation tests. Earlier V&V will be traced to lower level requirements.

R-1741: MTP shall be capable of storing spent clino, sand and Alt IX media up to a combined total of 600m3 of settled solids (Ref10).

The tank sizing assessment will inform the design against this requirement.

R-1744: MTP shall manage radiological heat from storage of spent media using passive means.

Tank sizing assessent will provide the BoD heat dissapation requirements, which will go into the BoD for each system.
The passive ventilation system will carry further tests in situ (post construction) before inactive commissioning.

R-1742: MTP shall have the capability to segregate spent Alt IX material from spent clino.

Segregation is a whole-plant concern, and this requirement will be flowed down to every system that handles both materials. Design reviews will be placed against these systems through assignment of V&V.

R-1961: MTP shall be capable of deploying the MRP technology for spent media sampling and retrieval.

BoD requirements flowing from this requirement will be informed by the MTP integration philosophy.
Since MRP will delivered after MTP, no commisioning tests are possible in the MTP timeframe.
However, lower-level V&V will cover those aspects of the design of MTP that accommodate MRP.

R-1853: MTP shall enable POCO removal of the inventory of residual material following bulk retrieval operations by the selected MRP retrieval technology.

The MRP integration assessment will information the flow of BoD requirements from this.

R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

Needs to be taken into account in the space allocation assessment. Important to test sampling at both inactive and active commissioning, because when active, the ventilation system is running.

V-1067: Operational tests to demonstrate the ability to manage large volumes of liquor associated with removal of spent bed residue.
OT: Operational Test

V-1045: Carry out flow modelling with analogy to existing plant.
DA: Design Assessment
CD

V-1066: Tank calibration tests: establish capacity, level alarm, switching points, etc. (This is done in situ, because of the tank installation retraints that affect rigidity and distortions.)
OIC: On-site Inactive Commissioning
IC

V-1064: Carry out assessment of tank sizing and configurations.
DA: Design Assessment
CD

V-1068: Demonstrate ability of ventilation route to achieve passive cooling.
OIC: On-site Inactive Commissioning
IC

V-1065: Demonstrate the ability to maintain an adequate degree of segration of spent media throughout MTP.
OIC: On-site Inactive Commissioning
IC

V-1073: Carry out assessment to establish the MRP integration philosophy.
DA: Design Assessment
CD

V-1094: Demonstrate ability to deploy equipment to remove residual material.
OIC: On-site Inactive Commissioning
IC

V-1087: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
IC

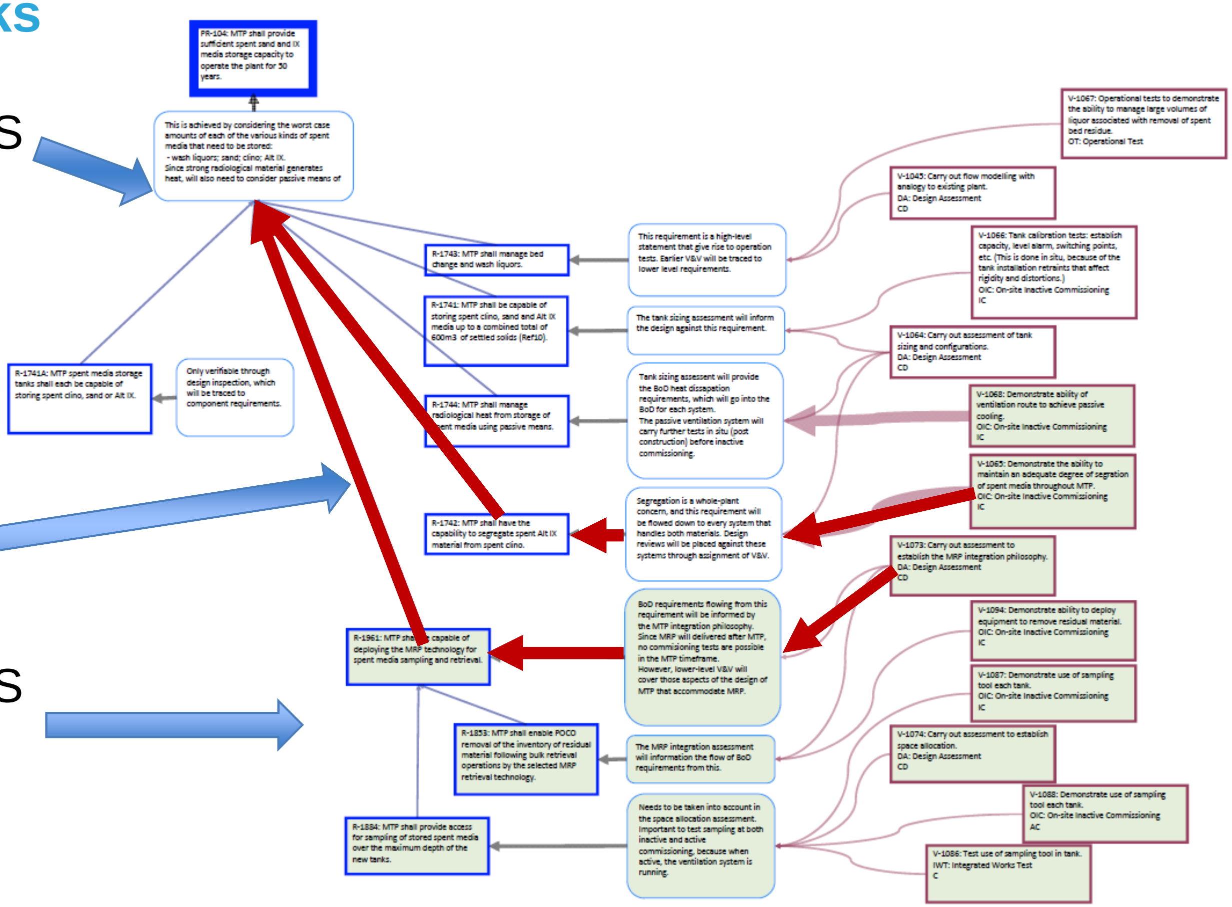
V-1074: Carry out assessment to establish space allocation.
DA: Design Assessment
CD

V-1088: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
AC

V-1086: Test use of sampling tool in tank.
IWT: Integrated Works Test
C

Cross-tool suspect links

- data managed in DOORS
- cross-platform links
- data managed in DOORS NG and RQM



PR-104: MTP shall provide sufficient spent sand and IX media storage capacity to operate the plant for 50 years.

This is achieved by considering the worst case amounts of each of the various kinds of spent media that need to be stored:
- wash liquors; sand; clino; Alt IX.
Since strong radiological material generates heat, will also need to consider passive means of

R-1741A: MTP spent media storage tanks shall each be capable of storing spent clino, sand or Alt IX.

Only verifiable through design inspection, which will be traced to component requirements.

R-1743: MTP shall manage bed change and wash liquors.

R-1741: MTP shall be capable of storing spent clino, sand and Alt IX media up to a combined total of 600m3 of settled solids (Ref10).

R-1744: MTP shall manage radiological heat from storage of spent media using passive means.

R-1742: MTP shall have the capability to segregate spent Alt IX material from spent clino.

R-1961: MTP shall be capable of deploying the MRP technology for spent media sampling and retrieval.

R-1853: MTP shall enable POCO removal of the inventory of residual material following bulk retrieval operations by the selected MRP retrieval technology.

R-1884: MTP shall provide access for sampling of stored spent media over the maximum depth of the new tanks.

This requirement is a high-level statement that give rise to operation tests. Earlier V&V will be traced to lower level requirements.

The tank sizing assessment will inform the design against this requirement.

Tank sizing assessent will provide the BoD heat dissapation requirements, which will go into the BoD for each system.
The passive ventilation system will carry further tests in situ (post construction) before inactive commissioning.

Segregation is a whole-plant concern, and this requirement will be flowed down to every system that handles both materials. Design reviews will be placed against these systems through assignment of V&V.

BoD requirements flowing from this requirement will be informed by the MTP integration philosophy.
Since MRP will delivered after MTP, no commisioning tests are possible in the MTP timeframe.
However, lower-level V&V will cover those aspects of the design of MTP that accommodate MRP.

The MRP integration assessment will information the flow of BoD requirements from this.

Needs to be taken into account in the space allocation assessment. Important to test sampling at both inactive and active commissioning, because when active, the ventilation system is running.

V-1067: Operational tests to demonstrate the ability to manage large volumes of liquor associated with removal of spent bed residue.
OT: Operational Test

V-1045: Carry out flow modelling with analogy to existing plant.
DA: Design Assessment
CD

V-1066: Tank calibration tests: establish capacity, level alarm, switching points, etc. (This is done in situ, because of the tank installation retraints that affect rigidity and distortions.)
OIC: On-site Inactive Commissioning
IC

V-1064: Carry out assessment of tank sizing and configurations.
DA: Design Assessment
CD

V-1068: Demonstrate ability of ventilation route to achieve passive cooling.
OIC: On-site Inactive Commissioning
IC

V-1065: Demonstrate the ability to maintain an adequate degree of segration of spent media throughout MTP.
OIC: On-site Inactive Commissioning
IC

V-1073: Carry out assessment to establish the MRP integration philosophy.
DA: Design Assessment
CD

V-1094: Demonstrate ability to deploy equipment to remove residual material.
OIC: On-site Inactive Commissioning
IC

V-1087: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
IC

V-1074: Carry out assessment to establish space allocation.
DA: Design Assessment
CD

V-1088: Demonstrate use of sampling tool each tank.
OIC: On-site Inactive Commissioning
AC

V-1086: Test use of sampling tool in tank.
IWT: Integrated Works Test
C

Summary

- Complex systems engineering scenarios can be supported by a combination of DOORS, DOORS NG and RQM
- Different layers of information may be best managed in different tools
  - DOORS for established systems engineering processes
  - DOORS NG where benefits come from wider toolset (e.g. agile software)
- Cross-platform linking allows for end-to-end traceability
- Suspect links will work across the tools
- Other forms of impact analysis may be a little fragmented

Thank You.