WHEN TRUST MATTERS

Modular Assurance of Complex Systems Using Contract-Based Design Principles

Paper: 

Building trust in complex systems

Dag McGeorge - Senior Principal Researcher
Digital Assurance research program - DNV

29 October 2024

Complex systems

Desirable and undesirable behaviours **emerge** from interactions within the system and with its environment

The reason for developing and using a complex system is the **value** that can be created by using it

Using a complex system **responsibly** means that the use is constrained in such a way that any harm occurring is acceptable considering the benefits (value)

Piper Alpha

On 6th July 1988, explosions and fire on the Piper Alpha oil platform caused 167 casualties

A conclusion in the public inquiry report was that:

"The presentation of the formal safety assessment should take the form of a Safety Case, which would be updated at regular intervals and on the occurrence of a major change of circumstances"

Cullen, 1990


Piper Alpha Memorial

Complex systems (2)

If the harm only impacts the user,
the user can make a value judgment and decide to use it or not

Because complex systems usually can harm others,
the value judgement cannot be left just to the user

Any such value judgement must be based on facts

- Claims supported by evidence

What is assurance?

Assurance is a way of **establishing justified confidence** in something so that it can be relied upon to **safeguard the interests** of various stakeholders

Assurance:

"*Grounds for justified confidence that a claim has been or will be achieved*"

(ISO 15026-1)

Claims express system properties that someone cares about

High-level claims can be about :

- system reliability
- system safety
- fairness
- …

Lower-level claims could be about:

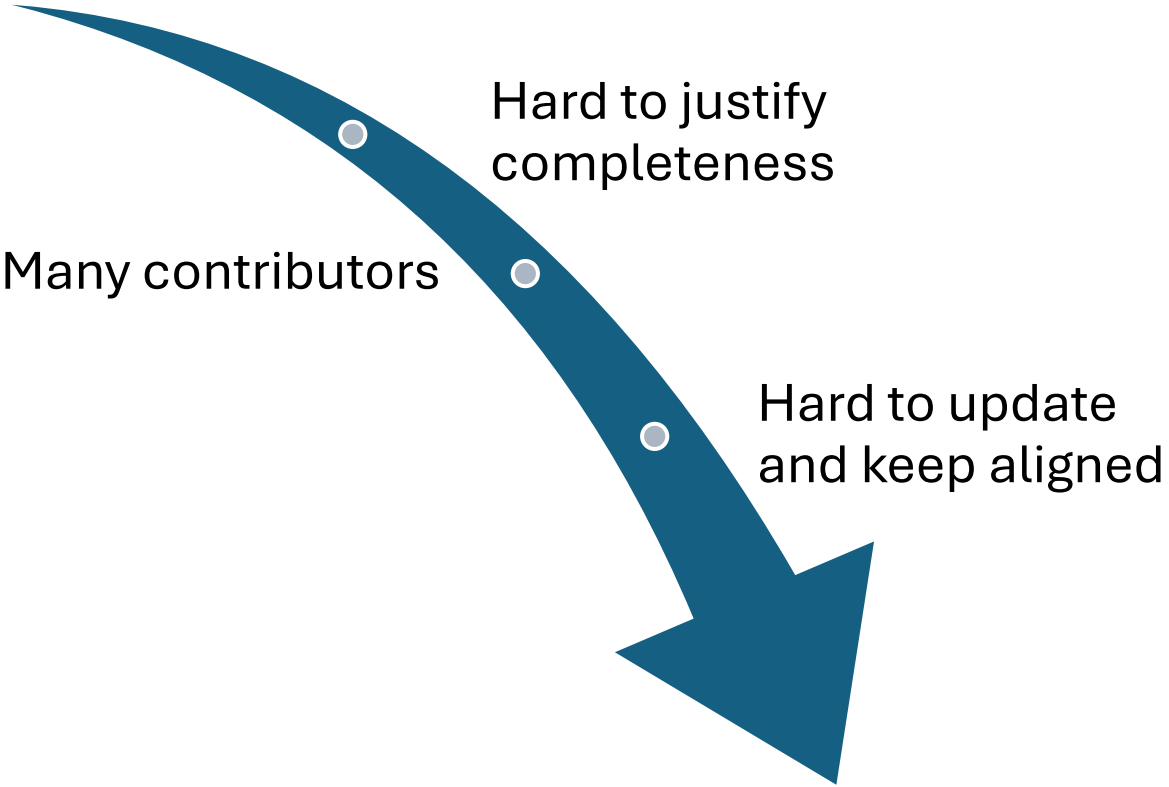
- deviation from planned path
- AI accuracy
- sensor resolution
- …

DNV


P1
Infusion hazards have been identified
Air in line hazard description
Sn1
Air in Line hazard (H1) has been mitigated
Evt1
Hazard log
Evt6
Sy stem Description docu
J1.1
Hazard controls has a been identified during adequate Hazard Analysis
J
Sb1.1
Argument by refraining to hazard controls
A
Safety analysis of the hazard is complete
Gl1.1
Prevents controls for preventing hazard are effective
Gl1.2
Corrects e controls are effective
J1.1.1
The needed maintai procedures are listed in the "Clinician manual" if performed by a trained clinician, they are effective
Sb1.1.1
Argument by demonstrating different areas of related
Al1.1.1
Infusion procedures are performed by properly trained personnel
Sb1.2.1
Argument by refraining to corrects e controls
J1.2.1
Corrects e controls have been identified during adequate Hazard Analysis
Downstream Monitor design documentation
Gl1.3
Air in line detection by downstream sensor is effective
P1.1.1
Clinician manual and training ensures complete infusion set
P1.1.2
Clinician manual and training ensures priming line line before use
P1.1.3
Clinician manual and training ensures needed delivery path
Gl1.4
Pump halts when air in line is detected
P1.2.1
Air in line alert recorded in sy stem log
Gl1.5
Alarm sounded and displayed when air in line detected
J1.3.1
Detects e controls decomposition
Sb1.3.1
Argument by refraining to the related safety requirement and its
Evt1.1.1
Clinician manual.pdf
Evt1.1.2
Sy stem Description docu
Evt1.1.3
Clinician manual.pdf
Evt1.1.3
Clinician manual.pdf
Evt1.2.1
Sy stem log docu
Sb1.3.2.1
Argument by refraining to the related safety requirement and its implementation
J1.3.2.1
If the corresponding safety requirement has been defined and tested, implemented the alarm sound
P1.3.1
Requirement specified Downstream sensor detects air in line
P1.3.2
Test demonstrate the requirement is satisfied
J1.3.1.1
If the corresponding safety requirement has been defined and tested, implemented the pump will stop
Sb1.3.1.1
Argument by refraining to the related safety requirement and its
Al1.3.1.1
Testing process is complete
P1.3.2.1
Safety requirement for preventive alarm is defined
P1.3.2.3
Safety requirement SC1.2 step 2 verified in the test process
Evt1.3.1.1
Safety Requirements.pdf
Evt1.3.1.2
Software Test Report.pdf
Testing env ironment and tools
Evt1.3.2.2
Downstream Monitor Test Report.pdf
Evt1.3.2.3
Pre report downstream monitor failure
Evt4
Definition of safety requirement to source alarm
Evt1.2.4
Safety Requirements docu
Evt5
Software Test Report
Evt1.1.1
Clinician manual.pdf
DNV

Some challenges

Industrial problems → large arguments with complex structure



C_e

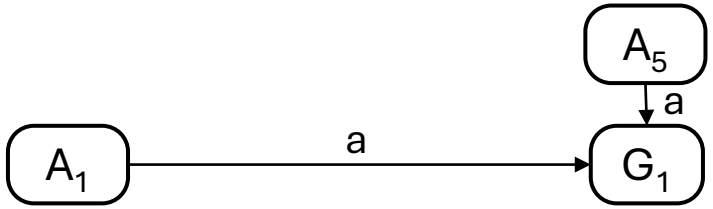
C_{sys}

$$K = (\{A_i\} , G)$$

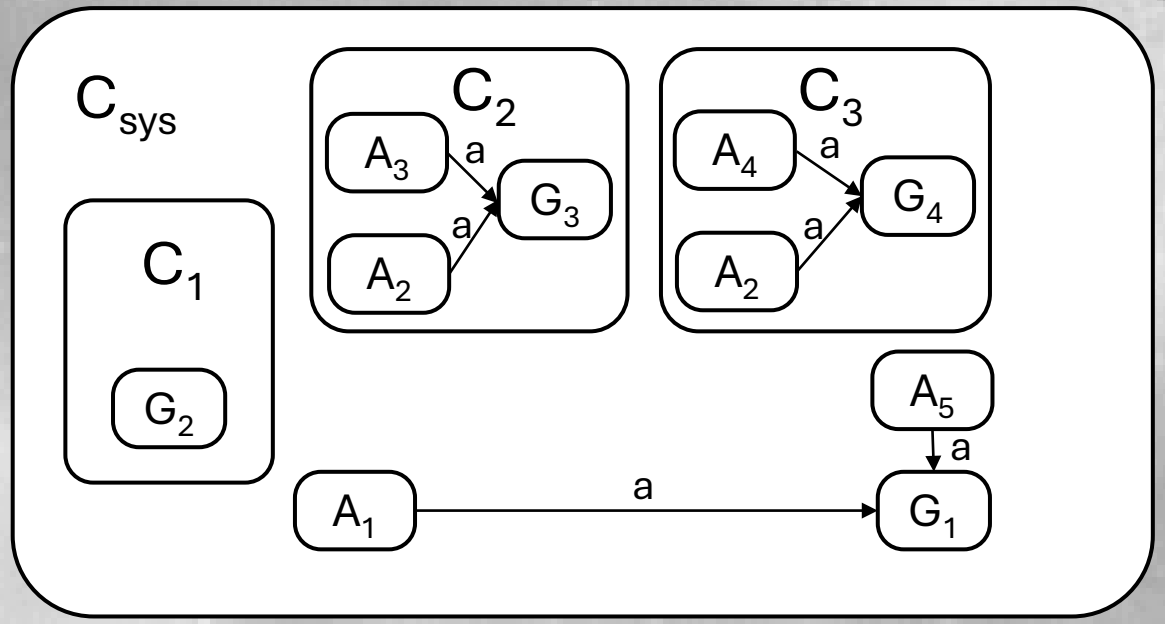
C_e

C_{sys}

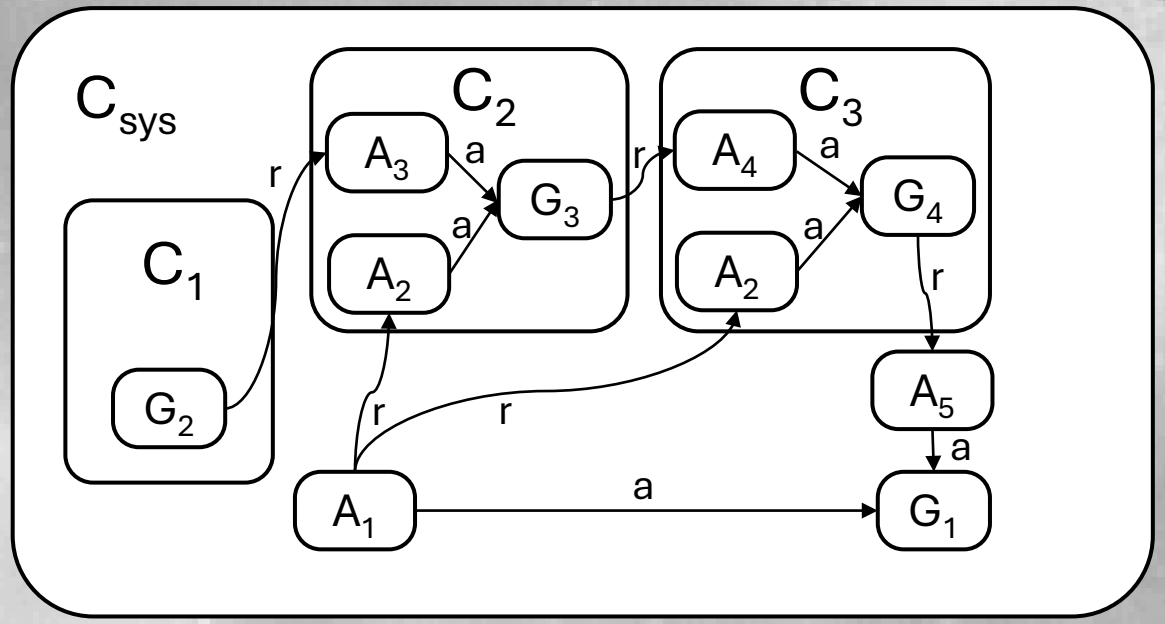
$K = (\{A_1, A_5\}, G_1)$



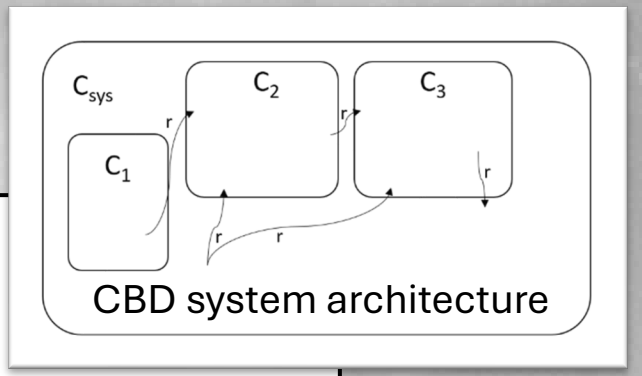
C_e



C_e



Assurance module architecture

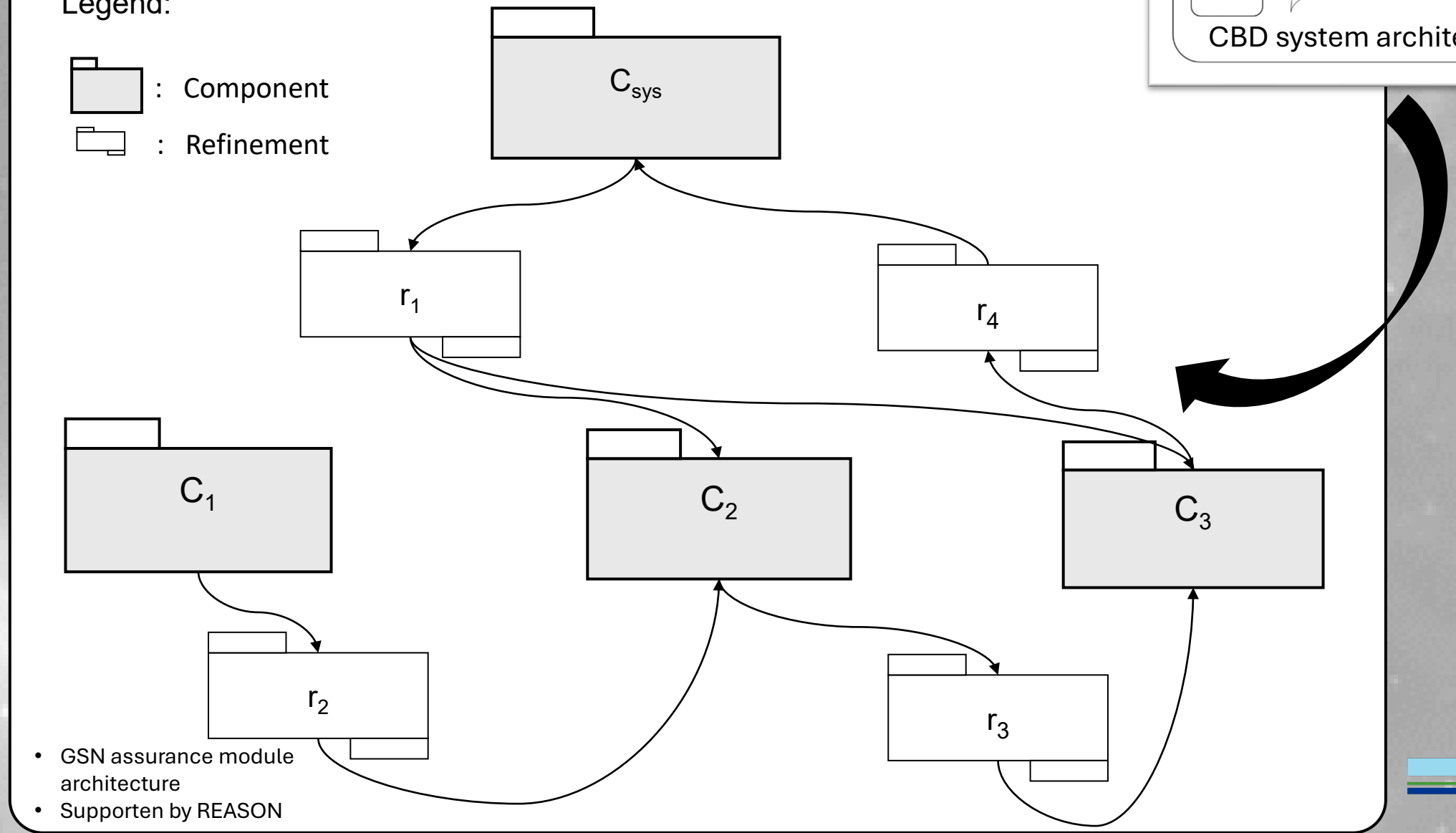


CBD system architecture

Legend:

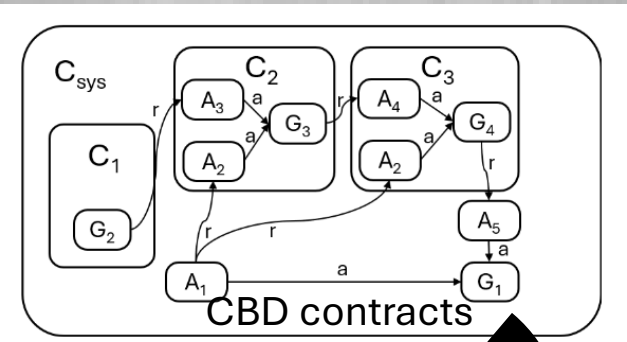
: Component

: Refinement



- GSN assurance module architecture
- Supporten by REASON

Assurance module architecture



Legend:

: Component

: Refinement

C_{sys}
$(\{A_1,A_5\}, G_1)$

$r_1=A_1 \sqsubseteq A_2$

$r_4=G_4 \sqsubseteq A_5$

C_1
$(\emptyset, G2)$

C_2
$(\{A_2,A_3\}, G_3)$

C_3
$(\{A_2,A_4\}, G_4)$

$r_2=G_2 \sqsubseteq A_3$

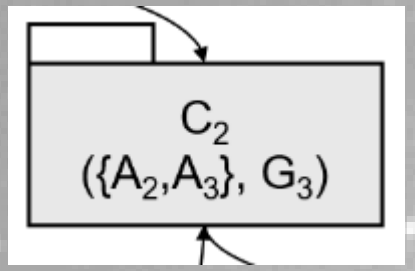
$r_3=G_3 \sqsubseteq A_4$

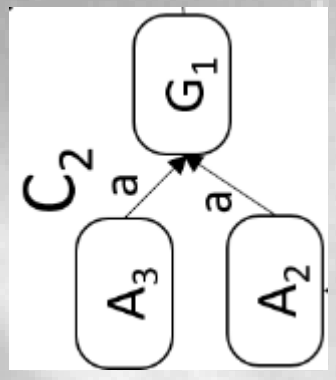
- GSN assurance module architecture
- Supporten by REASON

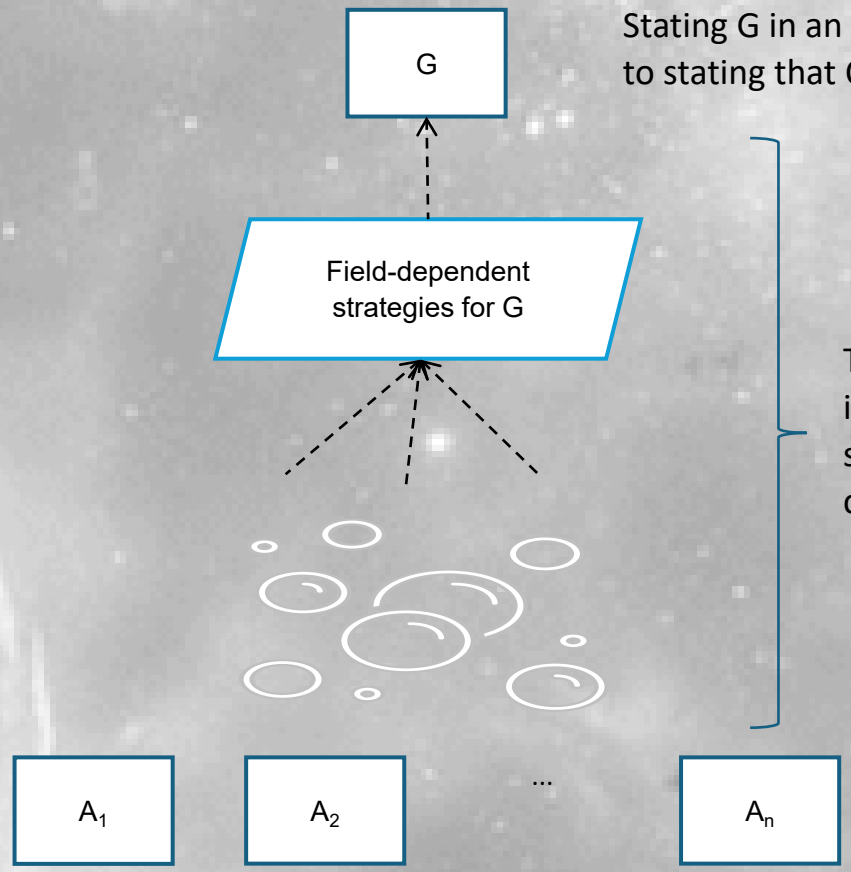
DNV

Component modules (a-relations)

Contract for component C:
$K_c=(\{A_i\}, G)$





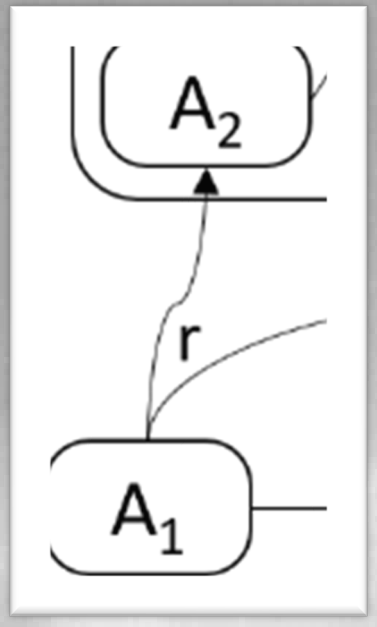


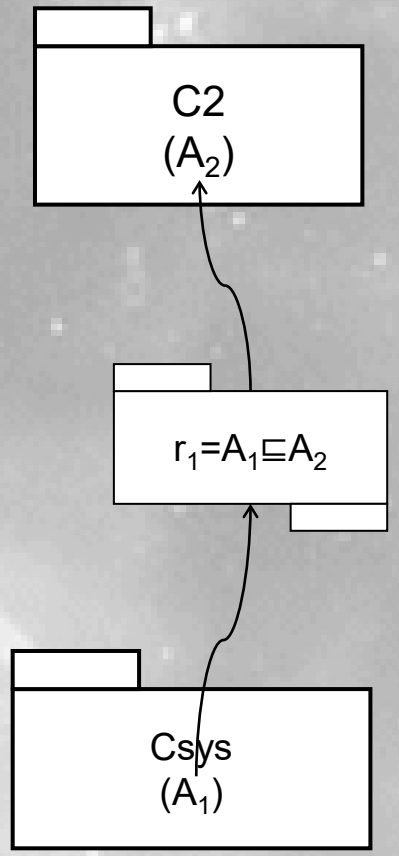
Stating G in an argument about C is equivalent to stating that C satisfies contract K_c

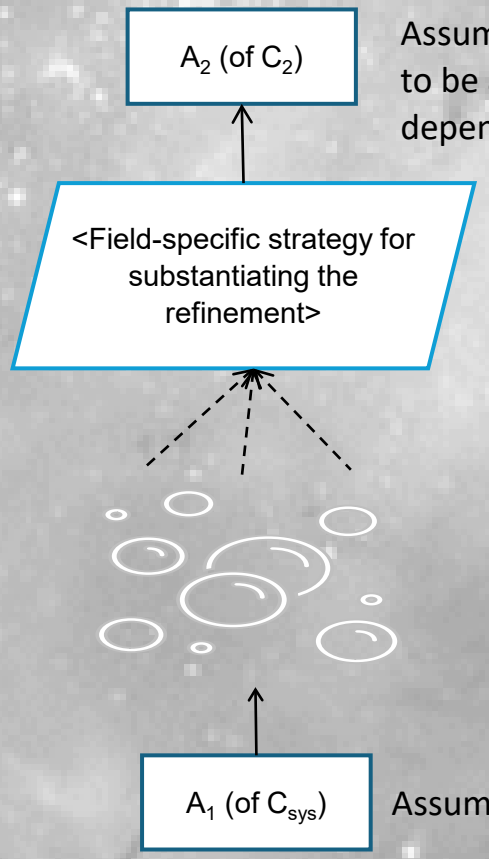
The argumentation that substantiates G from A_i is field-dependent and can involve many strategies and layers of reasoning and component-specific evidence.

Assumptions from the allocated contract K_c.

Refinments (r-relations)





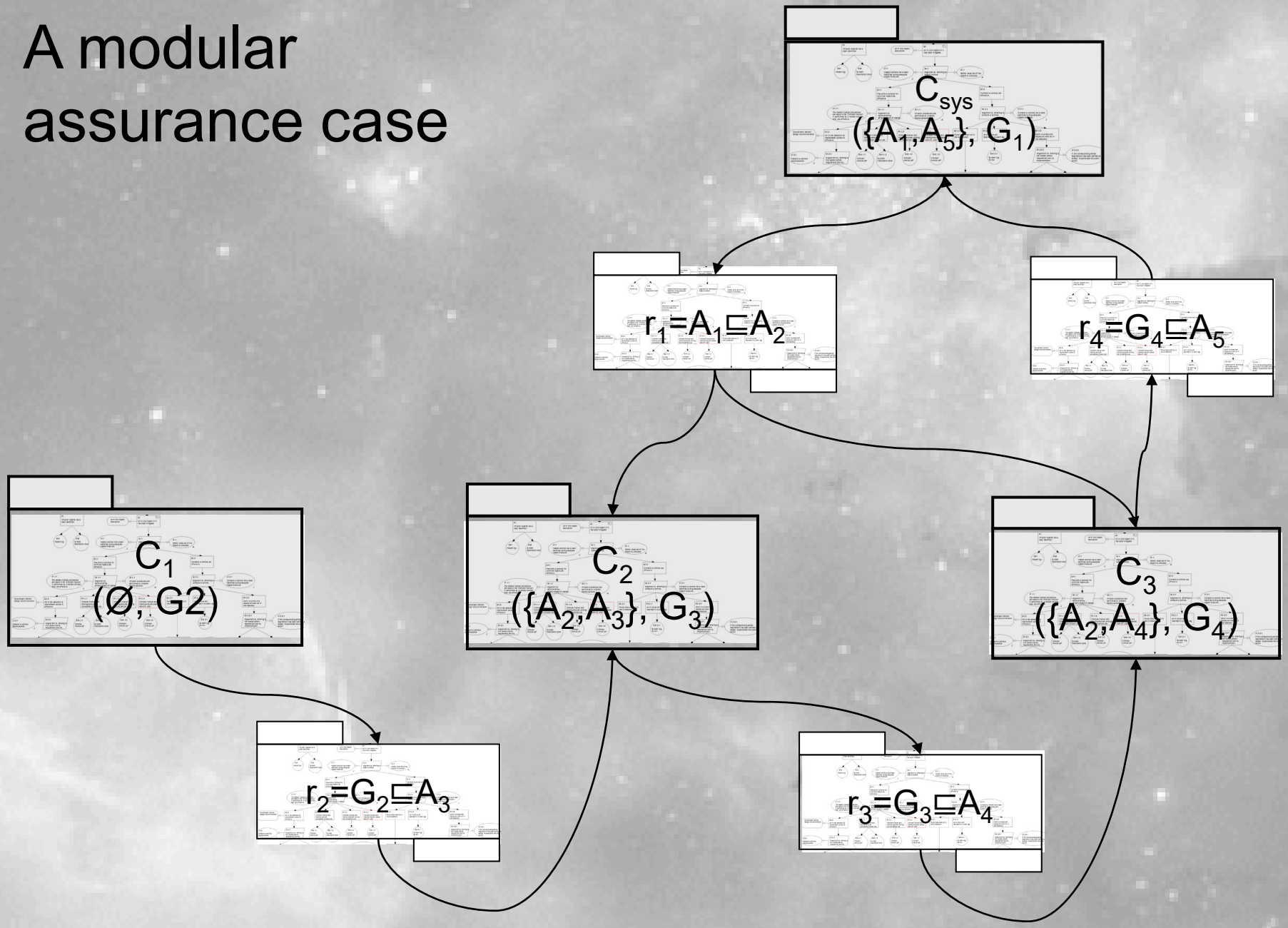


Assumption of the dependent component, shown to be a refinement of an assumption of the dependent component.

The argumentation is field specific and could be trivial or involve layers of reasoning and evidence.

Assumption of the independent module C_{sys}

A modular assurance case



System

Refinements for vertical integration

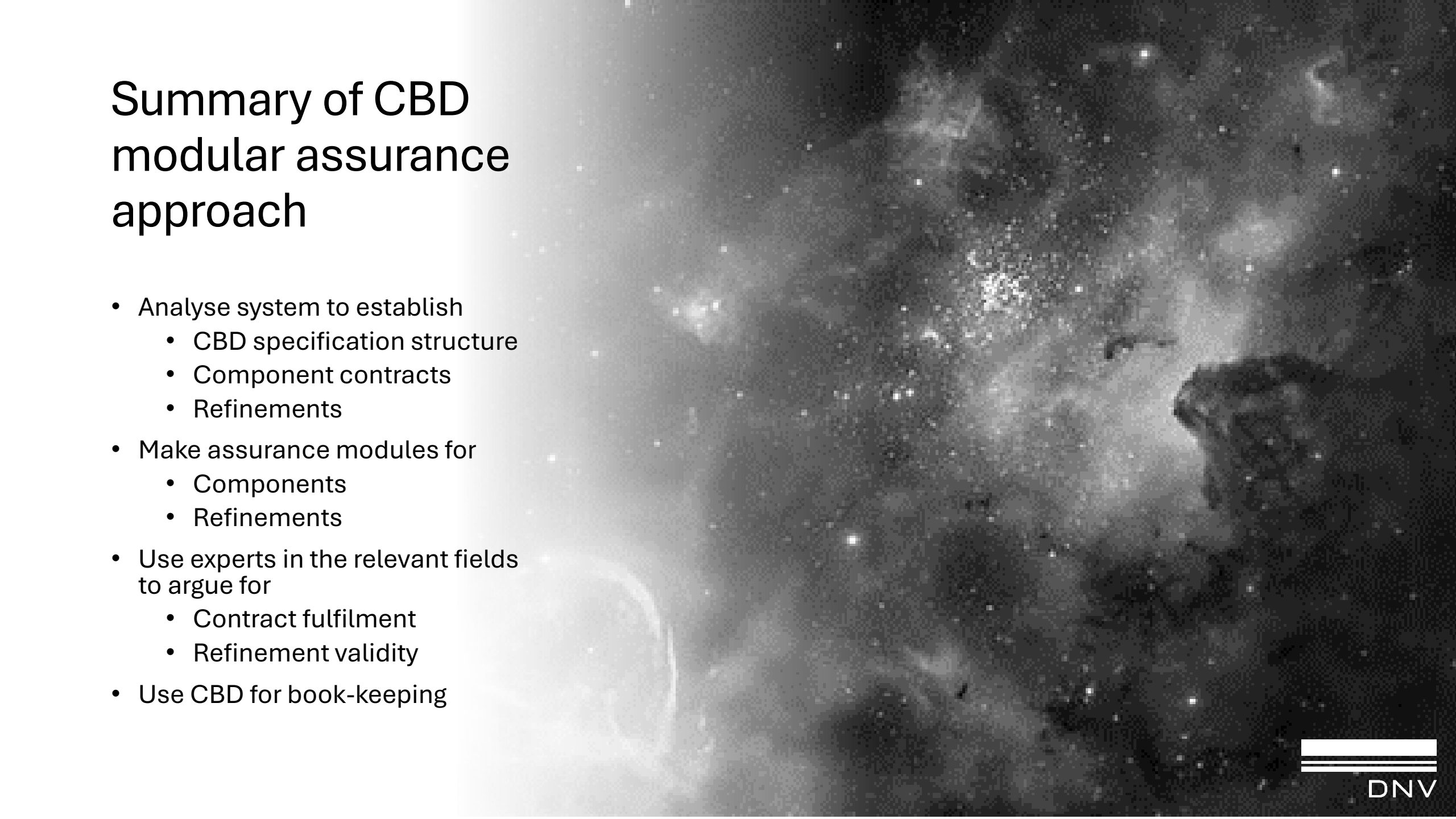
Sub-systems

Refinements for horizontal integration

DNV

Summary of CBD modular assurance approach

- Analyse system to establish
  - CBD specification structure
  - Component contracts
  - Refinements
- Make assurance modules for
  - Components
  - Refinements
- Use experts in the relevant fields to argue for
  - Contract fulfilment
  - Refinement validity
- Use CBD for book-keeping



Thank you for your attention!

dag.mcgeorge@dnv.com

www.dnv.com