SAFETY RELATIONSHIPS

The Furious Engineer

Informs safe

According to safe

DESIGN

BUILD

Achieves safe

Informs safe

Realized during

HAZARDS

Mitigates

Mitigates

Informs need to

Design for safe

Maintains safe

Need to recover from

Informs safe

In accordance with

Realized during

Realized during

Mitigates

Mitigates

MAINTAIN

OPERATE

Maintains safe

ACCIDENTS

Requires

ARCHITECTURE VIEW

The Furious Engineer

Gn_yy
The {operational scenarios} are completely and correctly identified by <the customer>

G0
The design of the <XX> is demonstrably safe to operate

Gn_xx
Away goal from the Build Leg

G2
<XX Design's> contribution to {Hazard} is acceptably managed

G1
The ways in which <XX> may contribute to {Hazard} are completely and correctly identified

Gn_yy
The {Hazards} to which the <XX> design may contribute are completely and correctly identified by {the customer}

G2.1
<XX design's> contribution(s) to {Hazard} is acceptably managed

G1.1
<XX design> is modelled at each level of design abstraction

G1.2
<The XX design> has been analysed to identify the ways in which it may contribute to {Hazard}

G2.2
<XX design's> contribution(s) to {Hazard} is acceptably managed

G1.2.1
{Safety Analysis n} identifies the contribution of the {XX design} to the {Hazard}

G2.2.1
<XX design's> contribution(s) to {Hazard} is acceptably managed at {tier n}

G3
Potential hazardous failures at {tier n} are acceptably managed

G4
Safety Requirements from {tier n-1} have been adequately allocated, decomposed, apportioned, and interpreted at {tier n}

S2.2.1
Argument over safety requirements identified for {tier n}

G5
{Safety Requirement n} is addressed through the realisation of the design at {tier n}

G3.1
The {tier n} design process does not introduce hazardous errors

G3.2
Safety Requirements at {tier n} address the potential hazardous behaviours identified at {tier n}

G6
{Safety Requirement} demonstrably satisfied through evidence provided at {tier n}

G7
{Safety Requirement} addressed through the realisation of the design at {tier n}

G3.1.1
The {tier n} design process does not introduce hazardous errors

G3.1.2
The {tier n} design does not contain hazardous errors

Gn
Design process conformant...(away goal to conformance leg?)

Gn
Design lifecycle conformant...(away goal to lifecycle module in conformance leg?)

G3.1.1.2
Independent reviews confirm the efficacy of the design process

G3.1.2.1.1
Safety analyses carried out on {tier n design}

G8
<XX design> is modelled at each level of design abstraction

ARGUMENT VIEW

Identifies the need to
Maintains safety functions identified in
Deliver Safe Platform
Contributes
Contributes to
Contributes to
Contributes to
Design XX
Built to
Depends on to facilitate safe design
Informs
Build
Contributes to
Operate
Requires
Enables
Maintain
Disposal
D
Necessitates
Informs the need to
Contributes to
Assure the Safe Design of XX
Assure the Safe Build of XX
Delivers
Delivers
Design Safety Case
Build Safety Case
Comprises
Risk Leg
Asserts confidence in
Confidence Leg
Asserts confidence in
Conformance Leg
Contributes to PAM
Premise
XX design is safe to operate
In the context of
Helps to mitigate
Which may manifest during
Through careful management of
Hazardous Failure Modes
Including
Hazards which XX contributes to
Including
Design errors
Identifies
Identify contributions
Achieved through
Sufficient to address
Safety analyses
Identified from
Safety requirements
Instantiated into
Demonstrably satisfies
In the context of
Design
Modelled at each
Level of Design Abstraction

KEY

The Furious Engineer

Goal

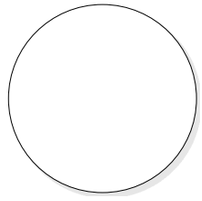
Justification

Context

Assumption

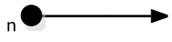
In the context of

Solved by

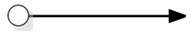


Solution (Evidence)

Strategy

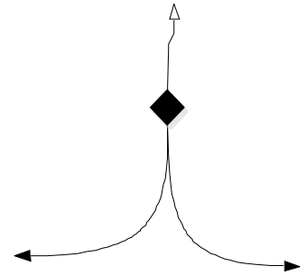


A solid ball is the symbol for many (zero or more). The label next to the ball indicates the cardinality of the relationship.

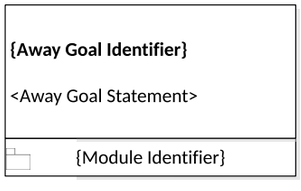


A hollow ball indicated 'optional' (zero or one)

A line without mutliplicity symbols indicates a one to one relationship



Optionality relationship



An away goal reference repeats a claim presented in another argument module

Undeveloped and uninstantiated Entity

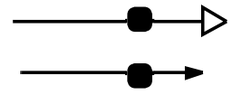
Uninstantiated Entity

Undeveloped Entity

<nn>
Text to be replaced by a specific instance on instantiation of the pattern

{nn}
An attribute to be replaced with the correct identifier on instantiation

Composite relationship - supported by AND in the context of



Assurance Claim Point

Goal G0

OUT OF SCOPE:
1. **Control Damage Hazards (CDH)**
2. **Post Accident Mitigation (PAM)**
3. **Disposal**

The definition of 'safe' is not normally required at this level (as the pattern argues what constitutes 'safe') - but there is a unique relationship with the customer here in this regard

C0
What constitues 'safe' is defined by {the customer}

ACP G0

C0b
{Operating Context} for <XX>

G0
The design of the <XX> is demonstrably safe to operate

Gn_xx
Away goal from the Build Leg

Gn_yy
The {operational scenarios} are completely and correctly identified by <the customer>

ACP S0

C0b
{Hazards} are defined by <xx> in <yy>

ACP C0b

S0
Argument by Appeal to each hazard to which the <XX design> contributes

G1
The ways in which <XX> may contribute to {Hazard} are completely and correctly identified

C2.1
Definition of {acceptably managed}

G2
<XX Design's> contribution to {Hazard} is acceptably managed

The Furious Engineer

Goal G1

G1
The ways in which <XX> may contribute to {Hazard} are completely and correctly identified

C0b
{Hazards} are defined by <xx> in <yy>

Gn_yy
The {Hazards} to which the <XX> design may contribute are completely and correctly identified by {the customer}

ACP S0

S0
Argument by Appeal to a model of the <XX design>

S0b
Argument by Appeal to a compelling safety analysis of the design

G1.1
<XX design> is modelled at each level of design abstraction

ACP G1.1

G1.2
<The XX design> has been analyzed to identify the ways in which it may contribute to {Hazard}

C1.1
<XX Design> as baselined by <xx> in <yy>

S1.1
Argument over the <XX System Model> at each tier of design

S2.2
Argument over the {Safety Analyses} at each tier of design

C2.2.1
{tier n} design

Number of tiers of system design abstraction

Number of hazards to which the XX design contributes

Sn 1.1 XX <Model at {tier n}>

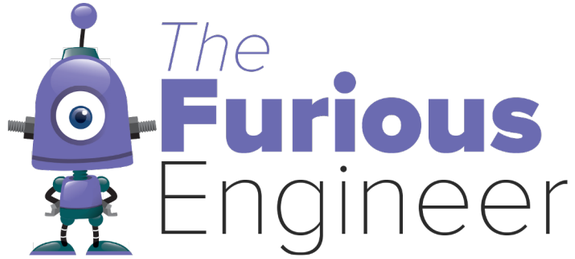
ACP Sn1.1

G1.2.1
{Safety Analysis n} identifies the contribution of the {XX design} to the {Hazard}

Number of {tiers} of the XX design

Sn 1.2.1
<Safety Analysis of each {tier}>

ACP Sn1.2.1



ACP Sn1.1

G_ACPSn1.1
Deficiencies in the completeness of the {tier n} model are acceptable

G_ACPSn1.1e
'Trustworthiness' of any modelling tool used..?

SACPSn1.1
Argument over identified deficiencies in the {tier n} model

CACPSn1.1b
{analysis purposes} definition

G_ACPSn1.1b
The level of granularity in the {tier n} model is acceptable for analysis purposes

G_ACPSn1.1c
Residual assurance deficits relating to the {configuration control} of the {tier n} model are acceptable

G_ACPSn1.1d
Residual assurance deficits relating to {unforeseen modifications} of the {tier n} model are acceptable

CACPSn1.1d
{unforeseen modifications} of the {tier n} model definition

CACPSn1.1c
{configuration control} definition

The Furious Engineer

Goal G2

C2
Description of <XX>

ACP C2

G2
<XX Design's> contribution to {Hazard} is acceptably managed

ACP C0b

C0b
{Hazards} are defined by <xx> in <yy>

C2.1
Definition of {acceptably managed}

S2
Argument by Appeal to each {hazard} to which the <XX design> contributes

n

Number of hazards to which the xx design may contribute

G2.1
<XX design's> contribution(s) to {Hazard} is acceptably managed

C2.2
<XX design> contribution may in some cases be defined as an explicit safety requirement

G1
The ways in which <XX> may contribute to {Hazard} are completely and correctly identified

S2.1
Argument over each identified <XX design> contribution to {Hazard}

ACP C2.1

C2.1
Description of the ways in which <XX> may contribute to {Hazard}

n

Number of xx design contributions to {Hazard}

G2.2
<XX design's> contribution(s) to {Hazard} is acceptably managed

Goal

G2.2

G2.2
<XX design's> contribution(s) to {Hazard} is acceptably managed

S2.2
Argument over <XX's> contribution to {Hazard} at each tier of design

G2.2.1
<XX design's> contribution(s) to {Hazard} is acceptably managed at {tier n}

C2.2.1
{tier n} design

ACP C2.2.1

ACP S2.2.1

G3
Potential hazardous failures at {tier n} are acceptably managed

G4
Safety Requirements from {tier n-1} have been adequately allocated, decomposed, apportioned, and interpreted at {tier n}

S2.2.1
Argument over safety requirements identified for {tier n}

ACP C2.2.1b

C2.2.1b
Safety requirements identified for {tier n}

Number of Safety Requirements at {tier n}

G2.2.1.1
{Safety Requirement n} is addressed through the realization of the design at {tier n}

C5
The term "Safety Requirements" includes "Safety Integrity Requirements"

n++

At least 1 of 2

G6
{Safety Requirement} demonstrably satisfied through evidence provided at {tier n}

G7
{Safety Requirement} addressed through the realization of the design at {tier n +1}

The Furious Engineer

Goal G3.1.1

This claim is applicable wherever an argument is being presented over the tiers of the system development lifecycle. {tier n} refers to the current tier being considered in the argument. This goal claims that the potential hazardous failures at the current tier are acceptably managed

The design process at any tier may be flawed. This goal claims that potentially hazardous design errors have not been introduced at the current tier. This is supported by arguing about the design process adopted at the current tier, and about the design artefact itself

The Furious Engineer

C3
"Potentially hazardous failures" includes both those contributing to known hazards AND "emergence"

G3
Potential hazardous failures at {tier n} are acceptably managed

C3.1
{acceptably managed} definition

C2.2.1
{tier n} design

C3.1
Potentially hazardous design errors at {tier n} design are {design errors}

G3.1
The {tier n} design process does not introduce hazardous errors

G3.2
Safety Requirements at {tier n} address the potential hazardous behaviours identified at {tier n}

At least 1 of 2

G3.1.1
The {tier n} design process does not introduce hazardous errors

G3.1.2
The {tier n} design does not contain hazardous errors

G3.2.1
Hazardous Failure Modes are correctly identified at {tier n}

C3.1
{tier n} Hazardous Failure Modes

G3.2.2
Safety Requirements sufficient to address Hazardous Failure Modes are defined

Goal G3.1.1

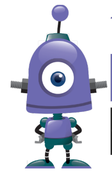
CSn n
{Challenges}

G3.1.1
The {tier n} design process does not introduce hazardous errors

C3.1.2
{hazardous errors} definition

ACP S3.1.1

S3.1.1
Argument over the efficacy of the <XX> design process



The Furious Engineer

C3.1.1.4
Definition of {periodic}

C3.1.1.4b
Definition of {safety analyses}

C3.1.1.4c
Definition of {design review}

G3.1.1.4
The design process facilitates periodic reviews to allow staged {safety analyses} and {design reviews}

ACP G3.1.1.4

Sn3.1.1.4
{Safety Management Plan}

ACP Sn3.1.1.4

Sn3.1.1.4b
{Engineering Management Plan

ACP Sn3.1.1.4b

Gn
Design process conformant...(away goal to conformance leg?)

...need to be modelled from EMP or equivalent

Gn
Design lifecycle conformant...(away goal to lifecycle module in conformance leg?)

(Table B of Part 2, Clause 6/7 /8 of Pt1/2/3

G3.1.1.1
Dialectic arguments...use positive challenges in the appropriate confidence leg (Linking ACPs)

G3.1.1.2
Independent reviews confirm the efficacy of the design process

This COULD simply be appealed to the 61508-1 (clause 6) away goal - but 61508 isn't particularly strong in this regard

G3.1.1.3
A robust Configuration Management framework has been applied during the design process

C3.1.1.3
Definition of {Configuration Management}

C3.1.1.3b
Definition of {robust}

Sn3.1.1.3
{Configuration Management Plan}

ACP Sn3.1.1.3

Sn3.1.1.3b
{Configuration Management Evidence}

ACP Sn3.1.1.3b

S3.1.1.2
Argument over the internal independent reviews of the <XX> design process

C2.1
Definition of {internal independent review}

S3.1.1.2b
Argument over the external independent reviews of the <XX> design process

C2.1
Definition of {external independent review}

G3.1.1.2.1
Internal independent reviews confirm the efficacy of the design process

At least MooN

ACP Sn n

Sn n
<Independent review Report>

Sn n
<Independent review Report>

Sn n
<Independent review Report>

ACP Sn nb

G3.1.1.2.2
External independent reviews confirm the efficacy of the design process

At least MooN

ACP Sn n

Sn n
<Independent review Report>

Sn n
<Independent review Report>

Sn n
<Independent review Report>

ACP Sn nb

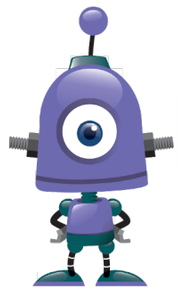
Goal G3.1.2

G3.1.2
The {tier n} design does not contain hazardous errors

C3.1.2
{hazardous errors} definition

S3.1.2
Argument over an analysis of the design for errors

S3.1.2b
Argument over the validity of requirements,



The Furious Engineer

G3.1.2.1
Safety analyses carried out on {tier n design} confirm that the {tier n} design contains no hazardous errors

G3.1.2.2
{Safety requirements} instantiated at {tier n} do not introduce hazardous errors

G3.1.2.1.1
Safety analyses carried out on {tier n design}

G8
<XX design> is modelled at each level of design abstraction

At least MooN

ACP Sn n

Sn n <Technique/ Measure>

Sn n <Technique/ Measure>

Sn n <Technique/ Measure>

ACP Sn nb

Number of tiers of system design abstraction

G3.1.2.2.1
{Safety Requirements} at {tier n} are validated

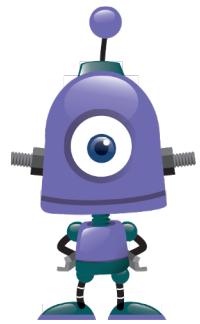
C3.1.2.2.1
{Validation} is defined as {definition}

ACP Sn n

Sn n <Technique/ Measure>

ACP Sn nb

Goal G3.2.1



The Furious Engineer

C2.2.1
{tier n} design

ACP C2.2.1

G3.2.1
Hazardous Failure Modes are correctly identified at {tier n}

S3.2.1
Argument over a diverse and varied range of safety analysis techniques

J3.2.1
A diverse and varied range of techniques and methods increases confidence in the claim

J

G3.2.1.1
<Safety Engineering Techniques> applied to the {tier n} correctly identify the {Hazardous Failure Modes}

Multiplicity required - at least MooN

ACPs required for appropriateness of T/M, SQEP nature of analyst, and varied/diverse characteristics of the different T/M

Sn n
<Technique/ Measure>

ACP Sn nb

Sn n
<Technique/ Measure>

ACP Sn nb

Sn n
<Technique/ Measure>

ACP Sn nb

Goal G3.2.2

The Furious Engineer

C3.2.2
Definition of {sufficient}

C3.2.2
Definition of {address}

G3.2.2
{Safety Requirements} sufficient to address {Hazardous Failure Modes} are defined

C3.1
{tier n} Hazardous Failure Modes

S3.2.2
Argument over safety requirements identified for {Hazardous Failure Modes}

Number of {Hazardous Failure Modes}

G3.2.2.1
{Hazardous Failure Mode} is sufficiently addressed through {safety requirements}

Sn3.2.2.1
<Safety Requirements Specification>

Sn n
<Technique/ Measure>

ACP Sn3.2.2.1

ACP Sn n

Goal G4

The act of allocation, decomposition, apportionment and interpretation can reasonably be seen as a single, unified act (owing to the nature of requirements engineering)

G4
Safety Requirements from {tier n-1} have been adequately allocated, decomposed, apportioned, and interpreted at {tier n}

ACP C4

C4
Safety Requirements from {tier n-1}

C4b
Definition of {adequately}

G3.2.2
{Safety Requirements} sufficient to address {Hazardous Failure Modes} are defined

S4
Argument over the {tier n} design and the Safety Requirements specified at {tier n}

C4.1b
Safety Requirements identified for {tier n}

ACP C4.1b

G4.1
Safety Requirements at {tier n} adequately capture the Safety Requirements from {tier n-1} for the {tier n} design

C2.2.1
{tier n} design

G4.2
Design decisions taken at {tier n) are appropriate to ensure that the Safety Requirements from (tier n-1} are maintained in the context of the potential hazardous failures identified at {tier n}

ACP C4.2

C4.2
Potential hazardous failures at {tier n} identified in Goal G3

S4.1
Argument over each Safety Requirement fon {tier n-1}

Number of Safety Requirements from {tier n-1}

G4.1.1
{Safety Requirement n-1} is adequately captured by one or more {Safety Requirement} at {tier n}

S4.2
Argument over design decisions taken at {tier n}

C4.2
Design decisions taken at {tier n}

Number of relevant design decisions

C4.2.1
Safety Requirements relevant to {design decisions} are Safety Requirements

G4.2.1
{Design decision} ensures Safety Requirements from {tier n-1} are maintained in the context of the identified potential hazardous failures

Goal G4.1.1

G4.1.1
{Safety Requirement n-1} is adequately captured by one or more {Safety Requirement} at {tier n}

C4.1.1b
{adequately} defiinition

S4.1.1
Argument over the 4+1 Principles for the careful management of safety requirements

C4.1.1
{The 4 + 1 Principles}

A4.1.1
Safety Requirements are {Prevent}, {Protect}, {Mitigate}, and {Recover}

A

The Furious Engineer

Number of Safety Requirements decomposed from {tier n - 1}

G4.1.1.1
{Safety Requirements} decomposed at {tier n} adequately address the identified {hazards}

G2.2.1
<XX design's> contribution(s) to {Hazard} is acceptably managed at {tier n}

G4.1.1.2
{Safety Requirements} decomposed at {tier n} maintain the intent of the {safety requirement} at {tier n-1}

G4.1.1.3
{Safety Requirements} are satisfied

C4.1.1c
{satisfied} definition

Sn4.1.1.3
<System Design Description>

ACP Sn4.1.1.3

G4.1.1.4
{Safety Requirements} instantiated at {tier n} mitigate {hazardous behaviour}

C4.1.1c
{mitigate} definition

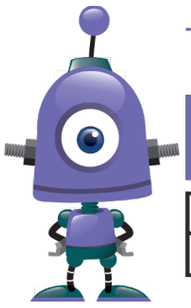
S4.1.1.4
Argument over the safety analyses to identify {emergence}

Sn n
<Technique/ Measure>

ACP Sn n

G4.1.1.5
{Safety Requirements} at {tier n} aggregate to meet the intent of {safety requirement} at {tier n-1}

This Goal 'replaces' the `+1 Principle' in this case



The Furious Engineer

Goal G4.2.1

C4.2.1
Safety Requirements relevant to {design decisions} are Safety Requirements

G4.2.1
{Design decision} ensures Safety Requirements from {tier n-1} are maintained in the context of the identified potential {hazardous failures}

C4.2.1c
{design decision} definition

C4.2.1b
{hazardous failures}

ACP G4.2.1

S4.1.1
Argument by appeal to the analyses leading to {design decisions} at {tier n}

G4.2.1.1
{Safety Analyses} undertaken for {tier n} result in {design decisions} which mitigate {hazardous failures}

C2.2.1
{tier n} design

Sn4.1.1.3
<System Design Description>

ACP Sn4.1.1.3

Sn n
<Technique/ Measure>

ACP Sn

Goal G6

The Furious Engineer

G6
{Safety Requirement} demonstrably satisfied through evidence provided at {tier n}

C2.2.1
{tier n} design

C6c
{demonstrably satisfied} definition

S6
Argument over {traceability} of the {safety requirement} into design

C6b
{traceability} definition

Forward AND backward traceability

Number of Safety Requirements

G6.1
{Safety Requirement} demonstrably satisfied by the instantiation of the design at {tier n}

Sn4.1.1.3
<System Design Description>

ACP Sn4.1.1.3

Goal G8

The Furious Engineer

G8
<XX design> is modelled at each level of design abstraction

C8
{design abstraction} is a {tier} of design

Levels of design abstraction

S8
Argument over the {modelling process)

CS8
{modelling process} definition

S8b
Argument over the {inputs to} the {modelling process)

G8.2
<Modelling process> was implemented by {SQEP} personnel

C8.2
{SQEP} definition

ACP G8.2

Sn8.2
<Competence Profile>

Sn8.2b
<Competence Record>

ACP Sn8.2

ACP Sn8.2b

C8.1
{robust} definition

C8.1b
{defensible} definition

G8.1
<Modelling process> is robust and defensible

ACP G8.1

Sn8.1
<Model Process>

Sn3.1.1.4b
<Engineering Management Plan>

ACP Sn8.1

ACP Sn3.1.1.4b

G8.3
All {required inputs} to the {modelling process} were provided

C8.3
The definitive list of all {required inputs}

ACP G8.3

Sn8.3
<Interface Specification>

Sn8.3b
<Functional Requirements Specification>

Sn8.3c
<Safety Requirements Specification>

Sn8.3d
<Use Cases and Scenarios>

ACP Sn8.3

ACP Sn8.3b

ACP Sn8.3c

ACP Sn8.3d