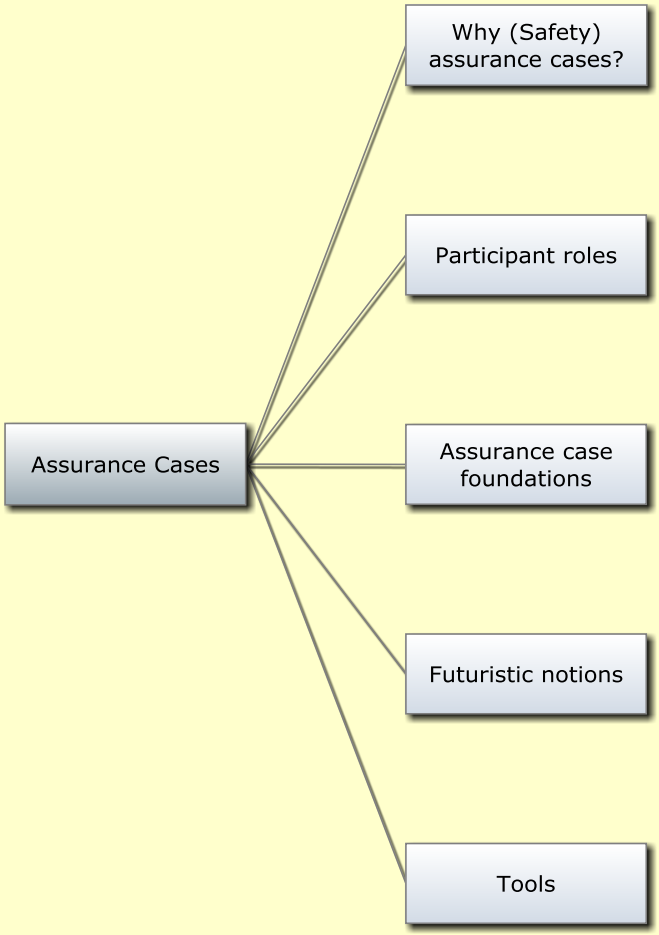
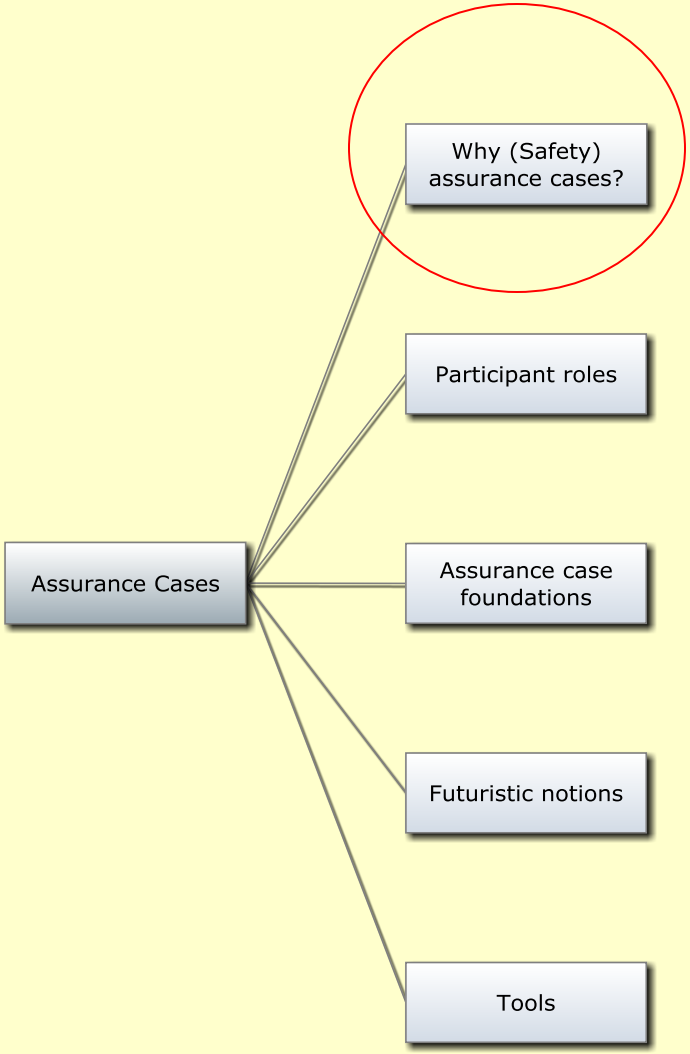
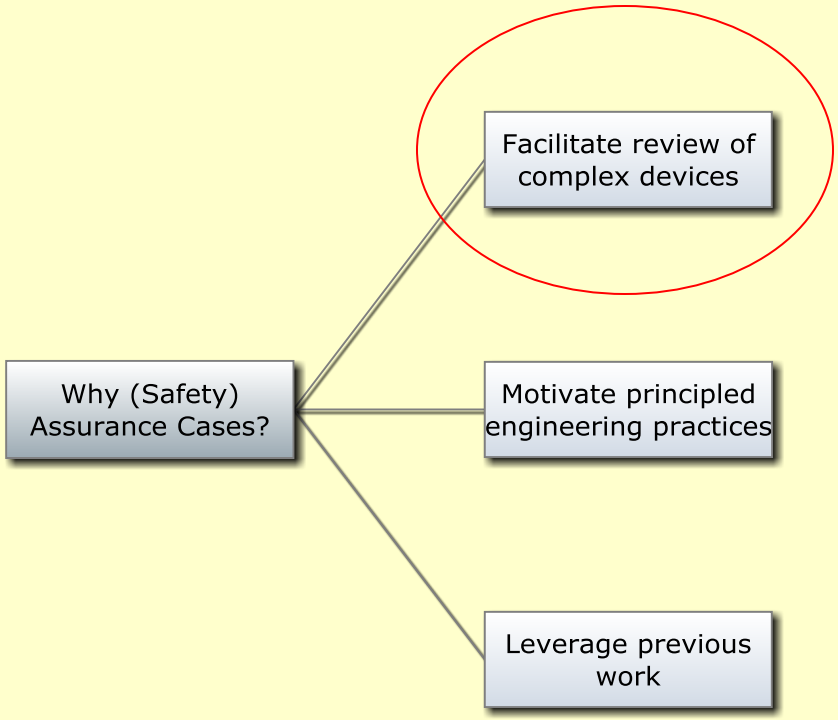
Thoughts on
Assurance Cases

Paul L. Jones
FDA/CDRH/OSEL

Material Organization

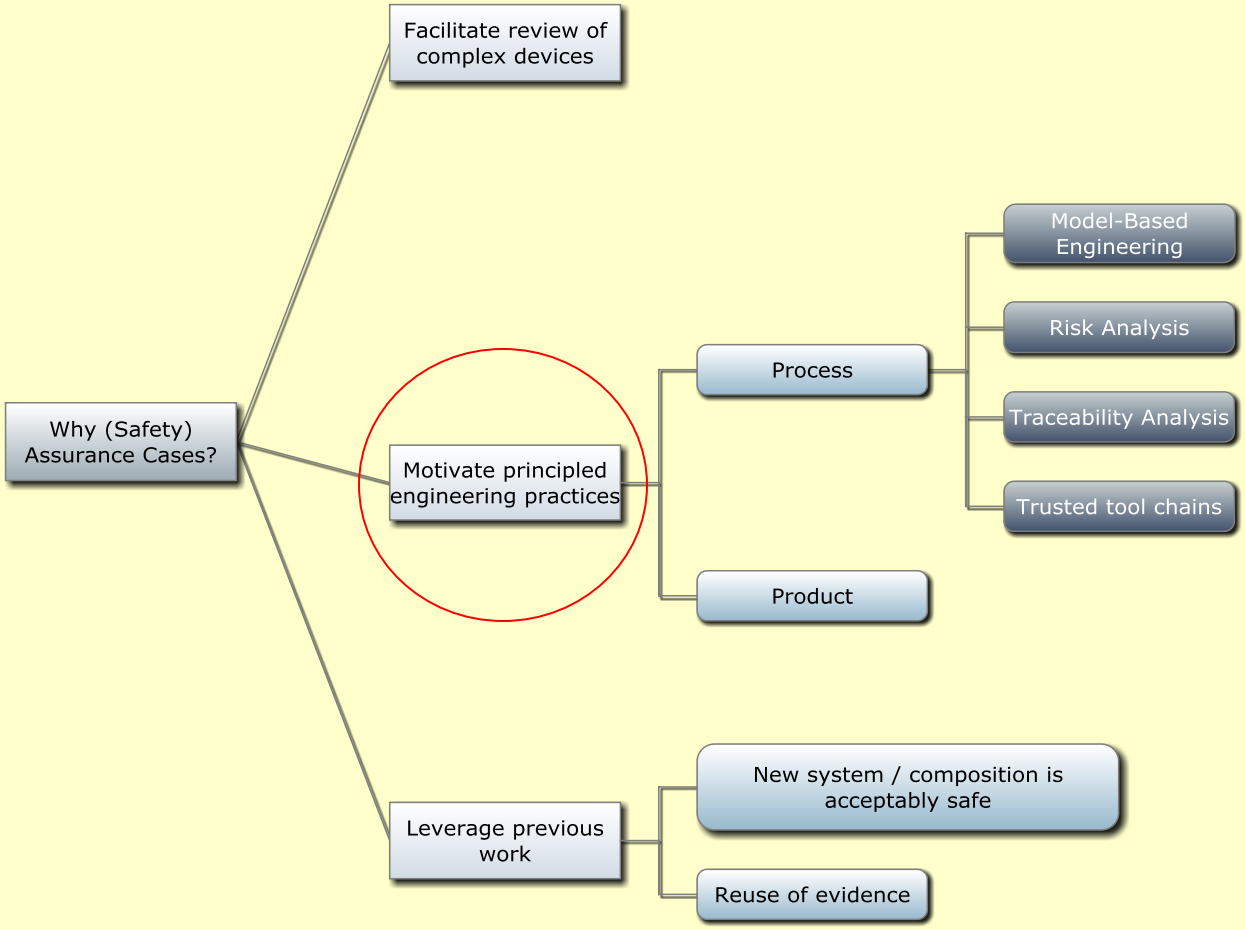


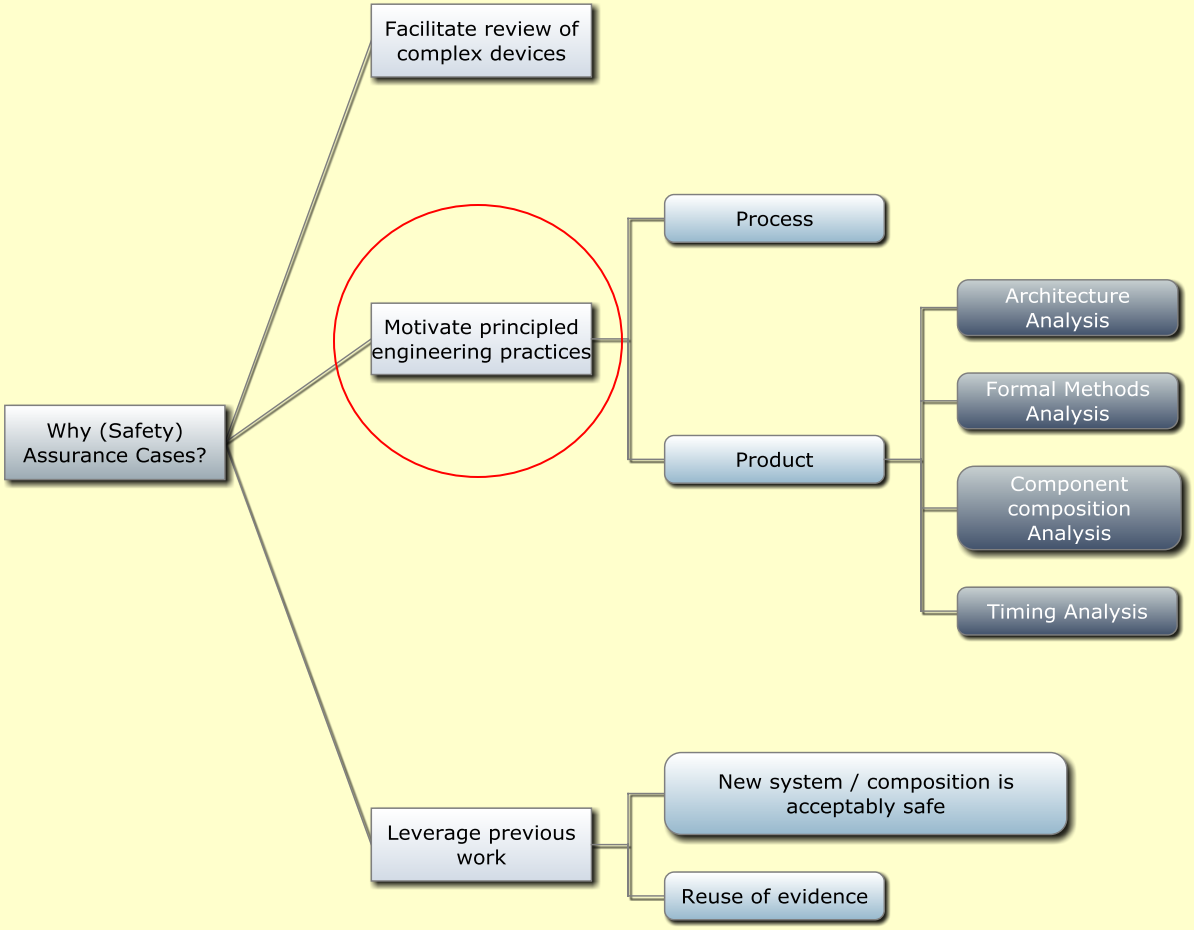

Why (Safety) assurance cases?
Participant roles
Assurance Cases
Assurance case foundations
Futuristic notions
Tools

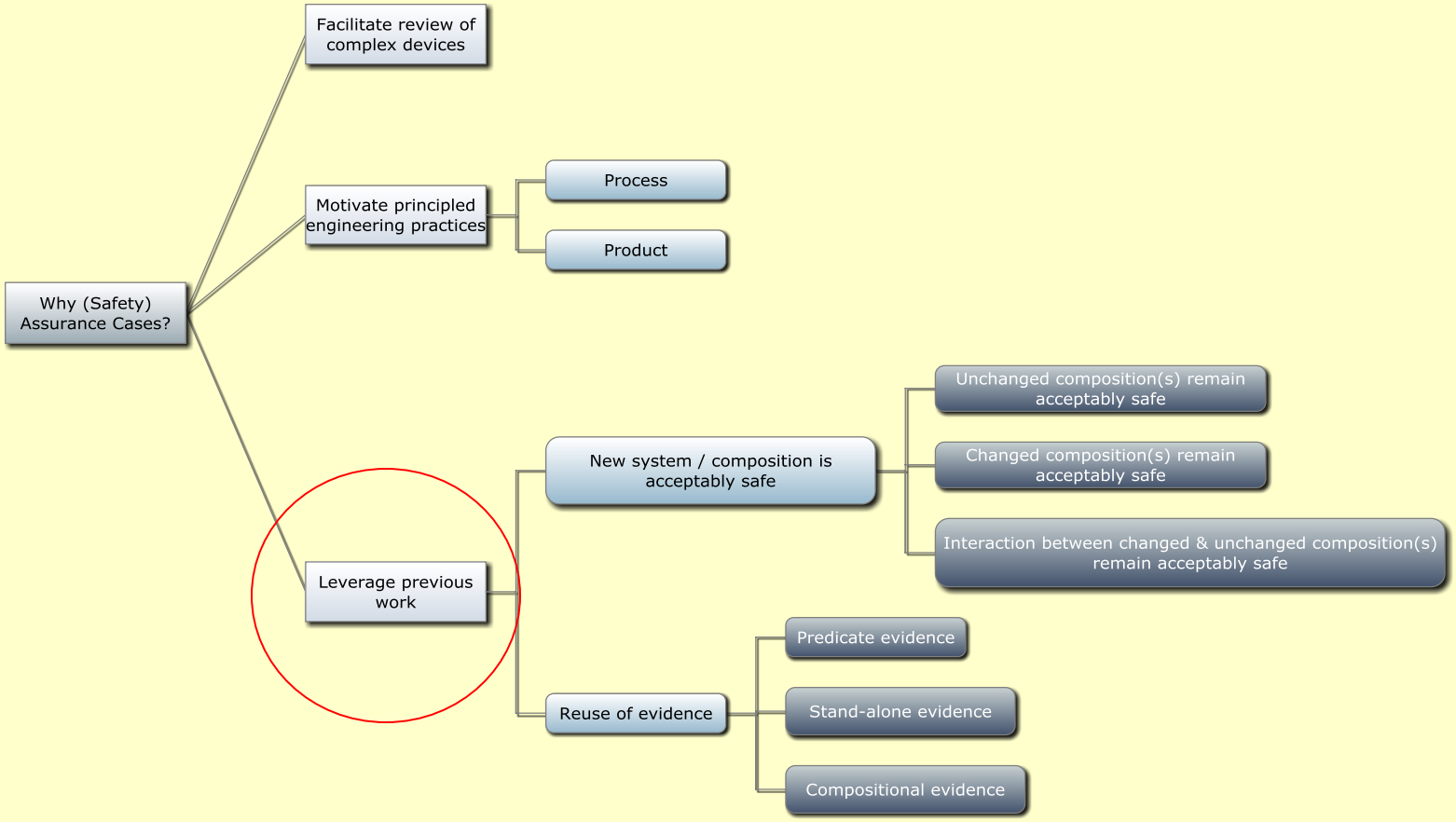

Why (Safety) Assurance Cases?
Facilitate review of complex devices
Motivate principled engineering practices
Leverage previous work

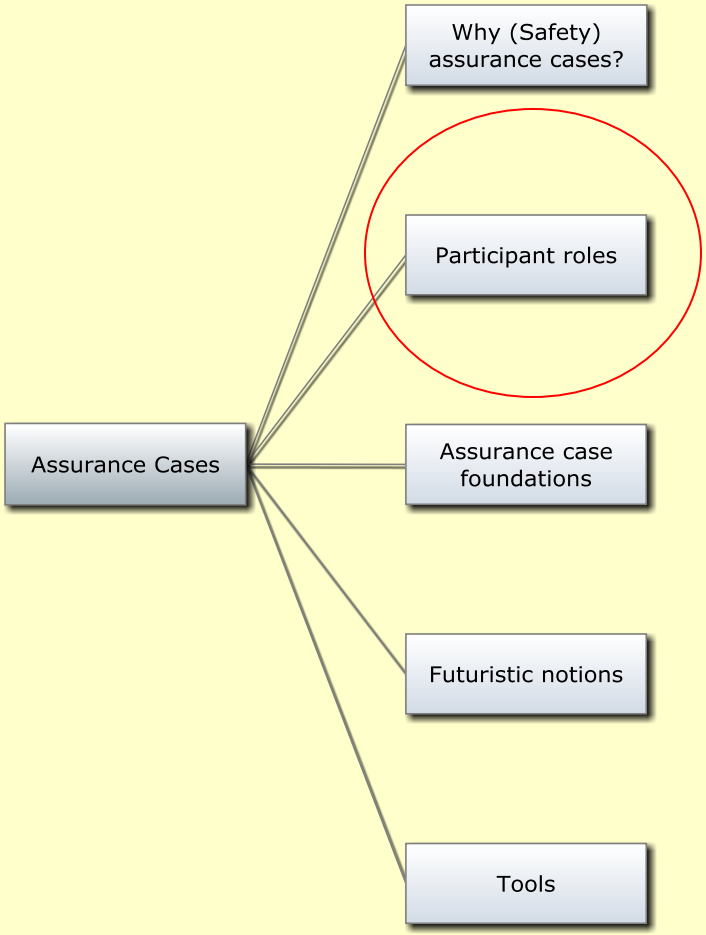
A day in the life of a regulator …

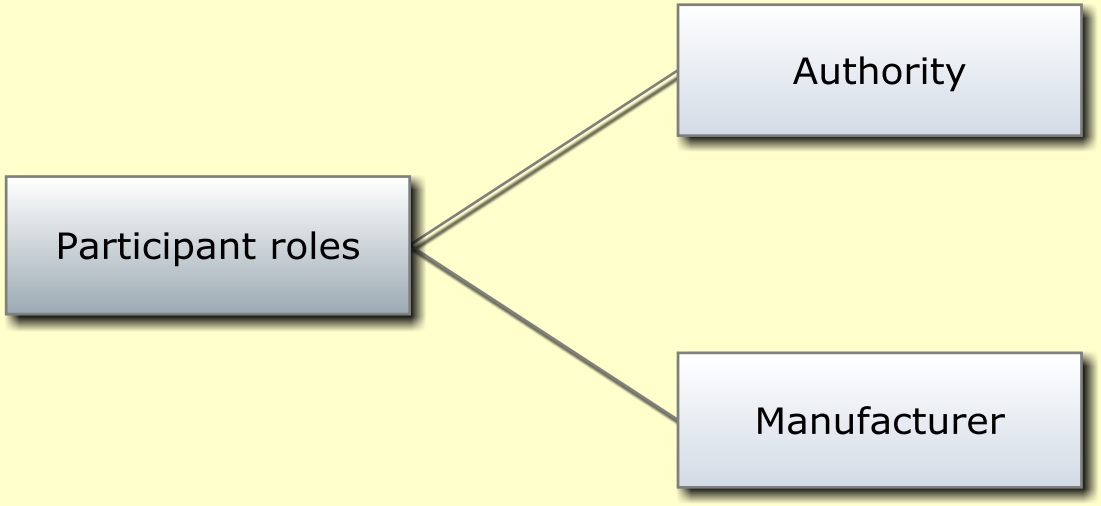
A day in the life of a regulator …

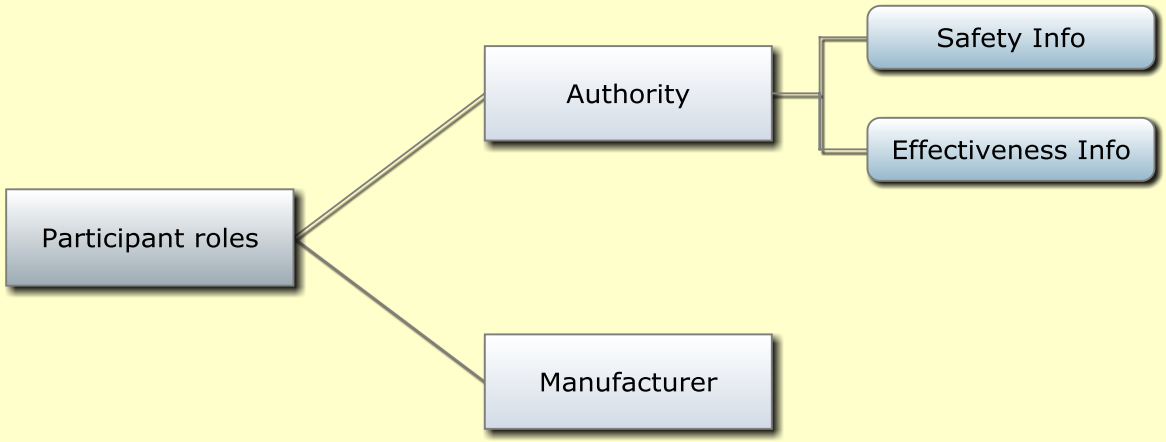

Why (Safety) Assurance Cases?
Facilitate review of complex devices
Motivate principled engineering practices
Process
Model-Based Engineering
Risk Analysis
Traceability Analysis
Trusted tool chains
Product
Leverage previous work
New system / composition is acceptably safe
Reuse of evidence

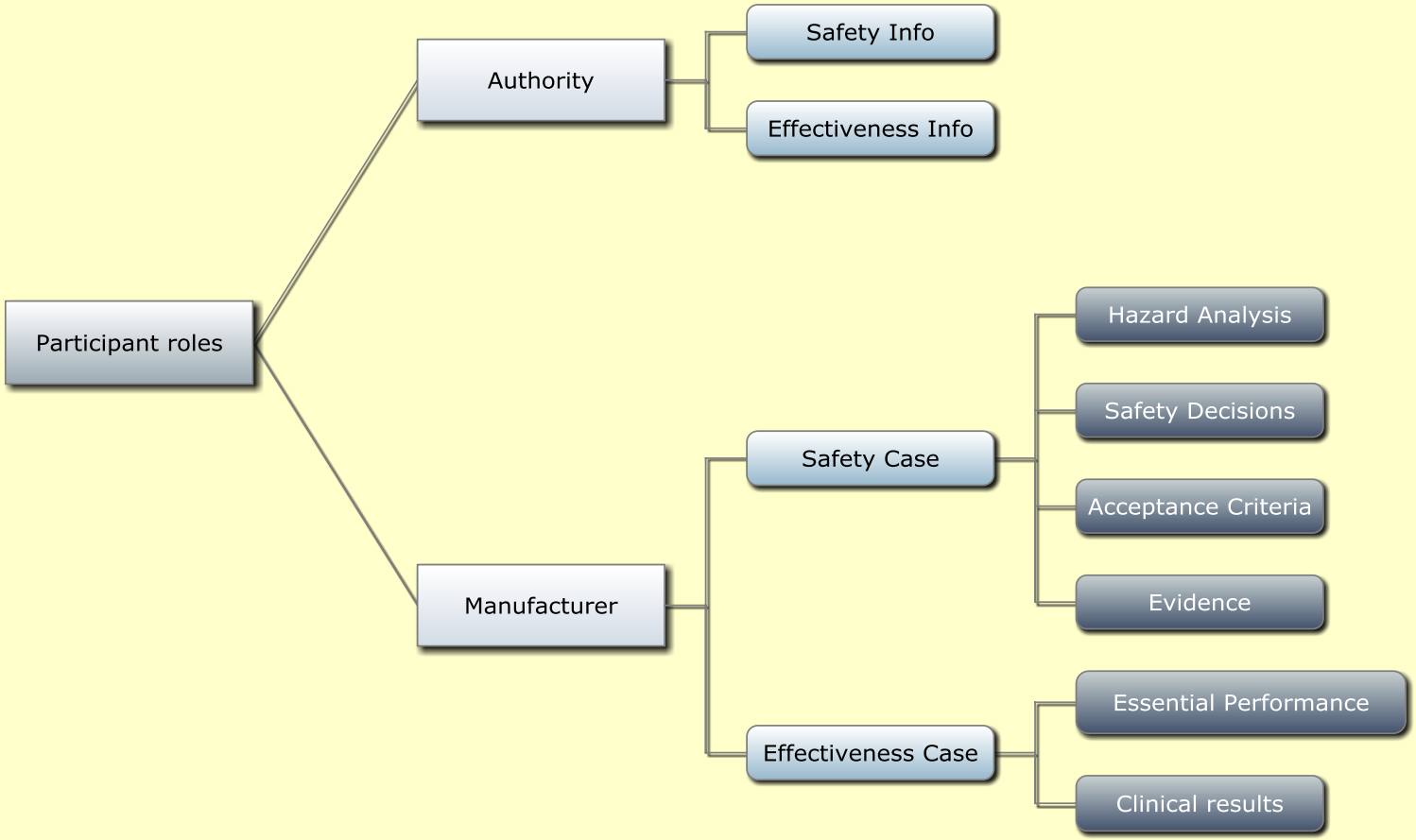

Why (Safety) Assurance Cases?
Facilitate review of complex devices
Motivate principled engineering practices
Process
Product
Architecture Analysis
Formal Methods Analysis
Component composition Analysis
Timing Analysis
Leverage previous work
New system / composition is acceptably safe
Reuse of evidence

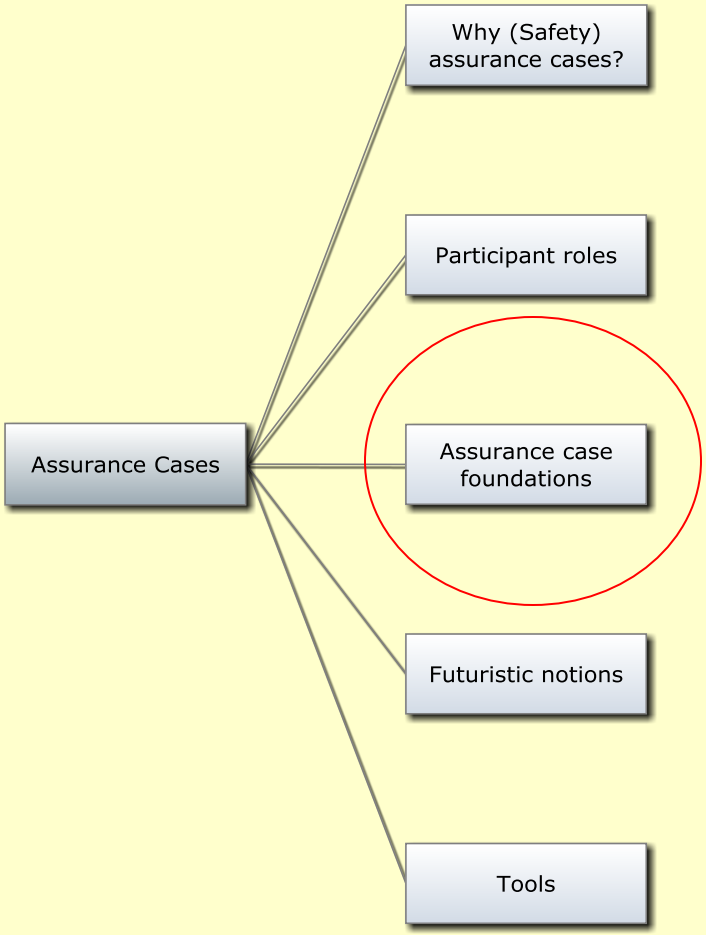

Why (Safety) Assurance Cases?
Facilitate review of complex devices
Motivate principled engineering practices
Process
Product
Leverage previous work
New system / composition is acceptably safe
Unchanged composition(s) remain acceptably safe
Changed composition(s) remain acceptably safe
Interaction between changed & unchanged composition(s) remain acceptably safe
Reuse of evidence
Predicate evidence
Stand-alone evidence
Compositional evidence


Why (Safety) assurance cases?
Participant roles
Assurance Cases
Assurance case foundations
Futuristic notions
Tools

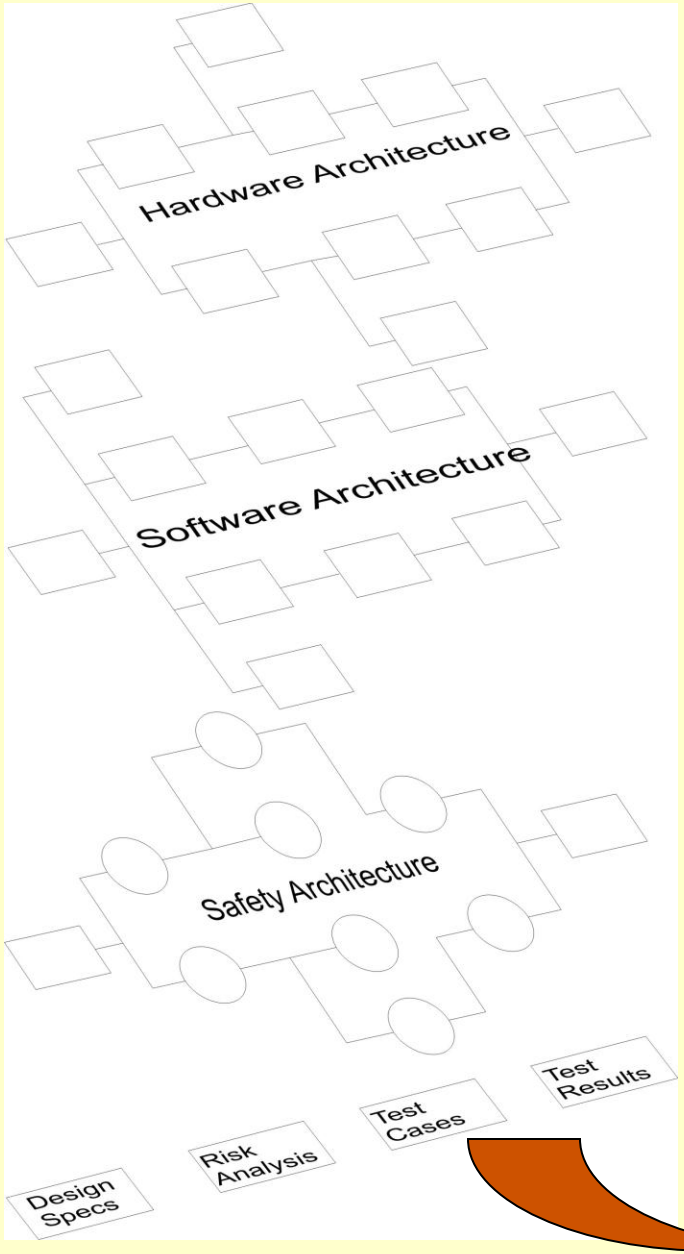

Participant roles
Authority
Manufacturer


Participant roles
Authority
Safety Info
Effectiveness Info
Manufacturer

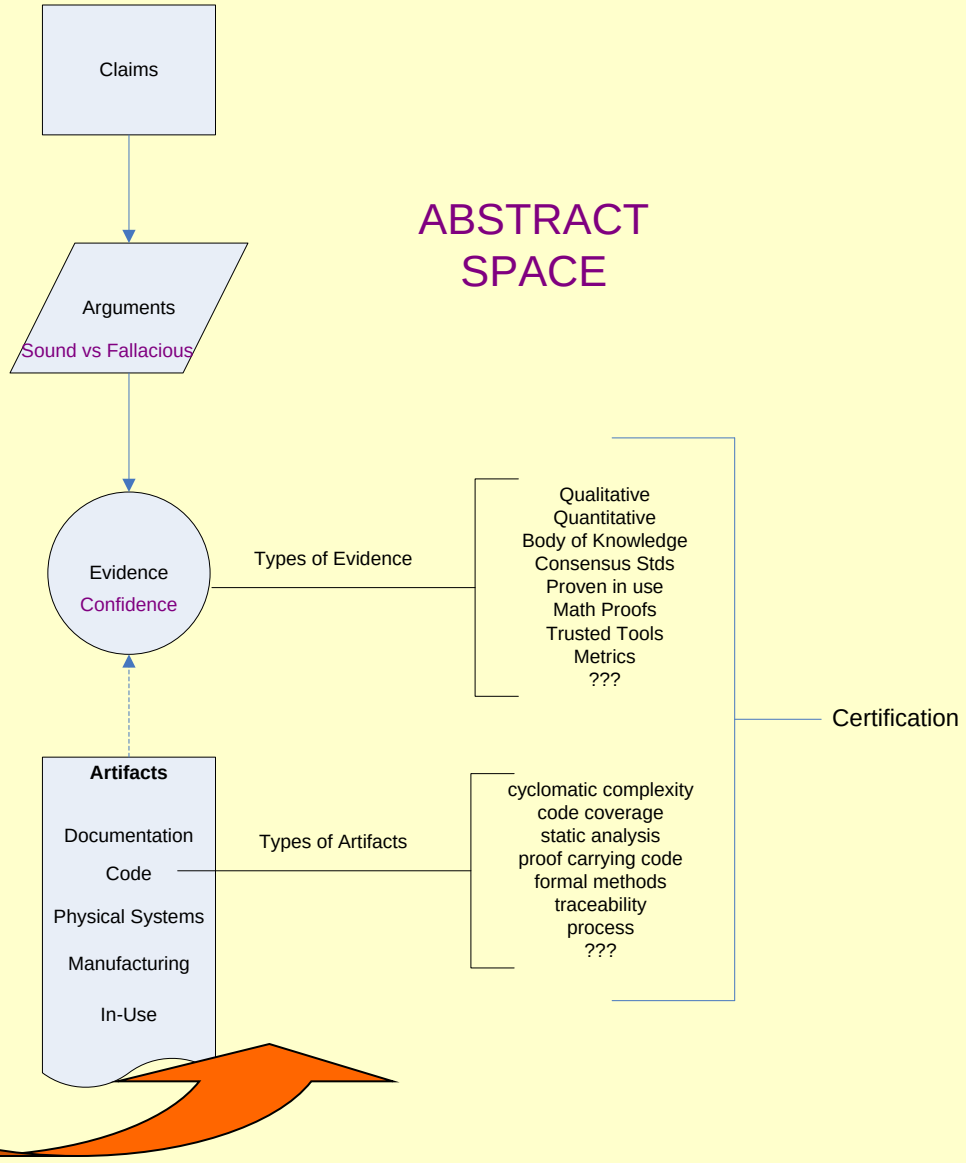

Participant roles
Authority
Safety Info
Effectiveness Info
Manufacturer
Safety Case
Hazard Analysis
Safety Decisions
Acceptance Criteria
Evidence
Effectiveness Case
Essential Performance
Clinical results


Why (Safety) assurance cases?
Participant roles
Assurance Cases
Assurance case foundations
Futuristic notions
Tools

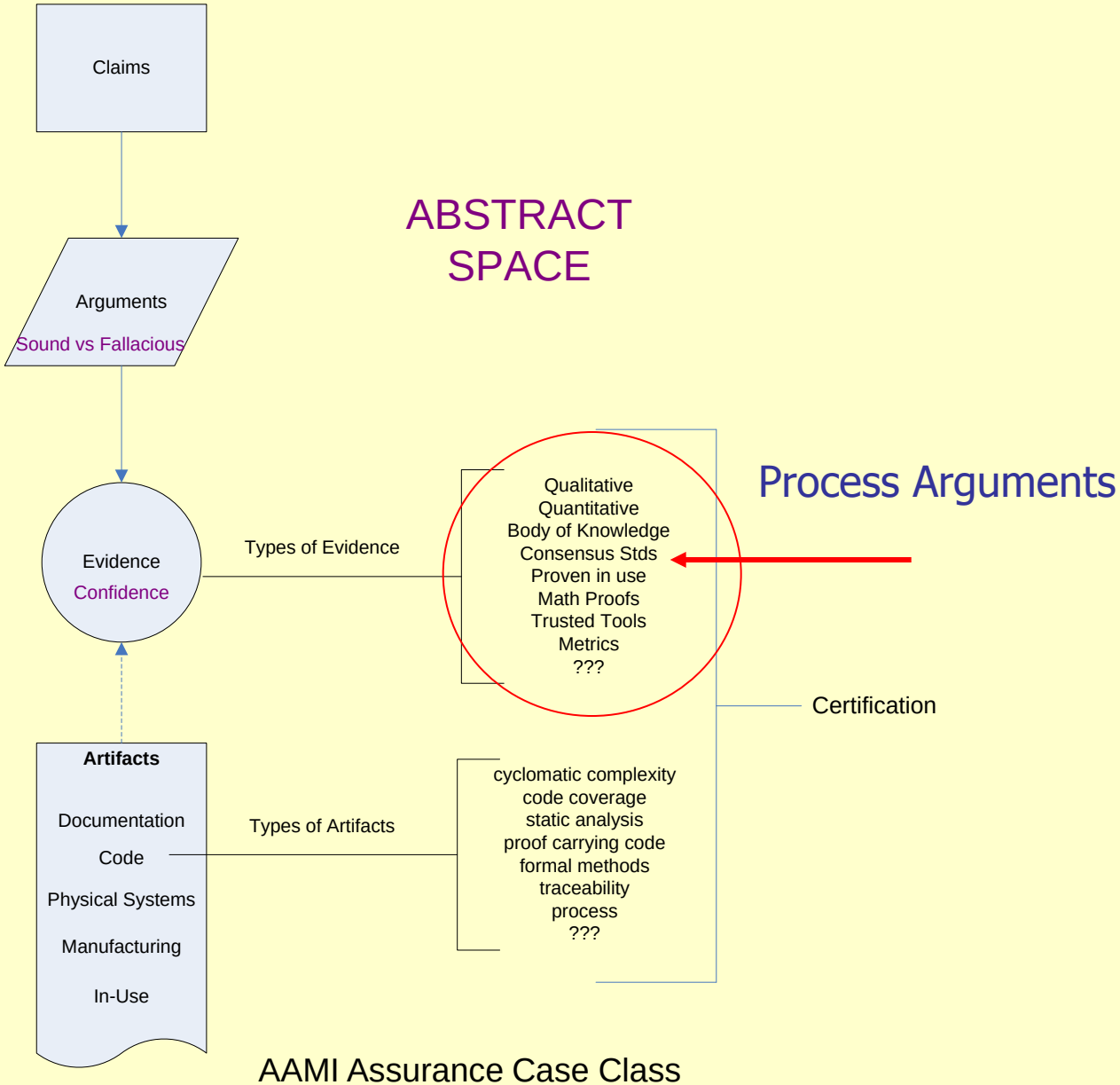
System Abstraction



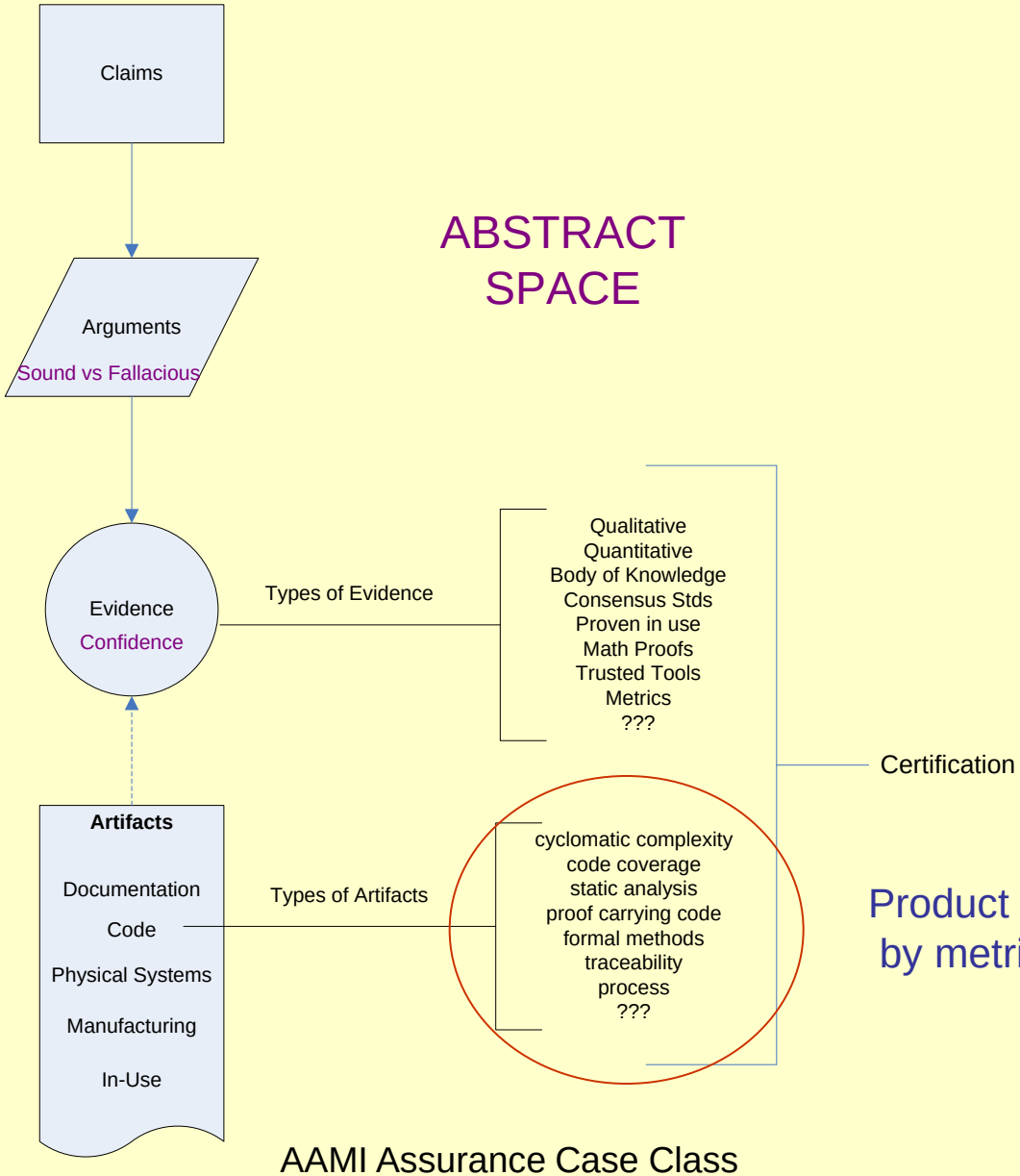
Assurance Case Framework

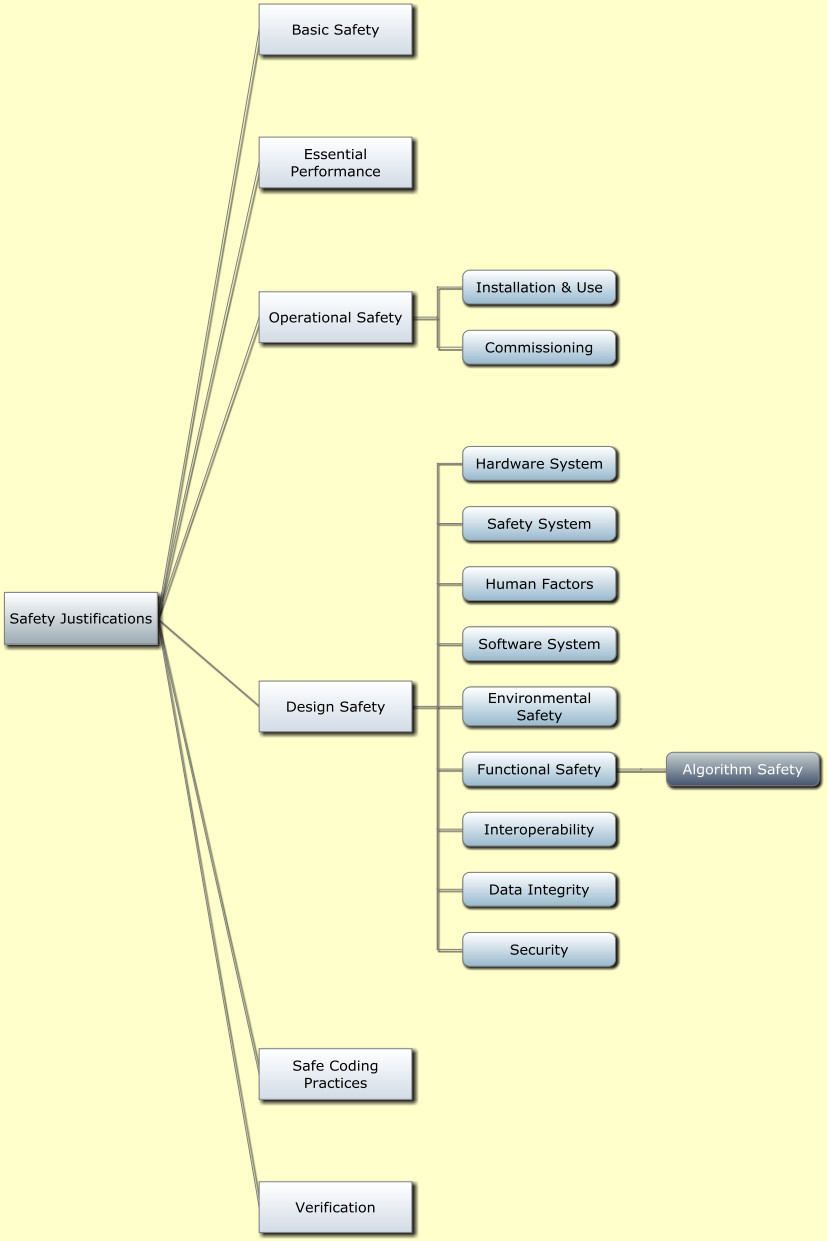


Assurance Case Framework

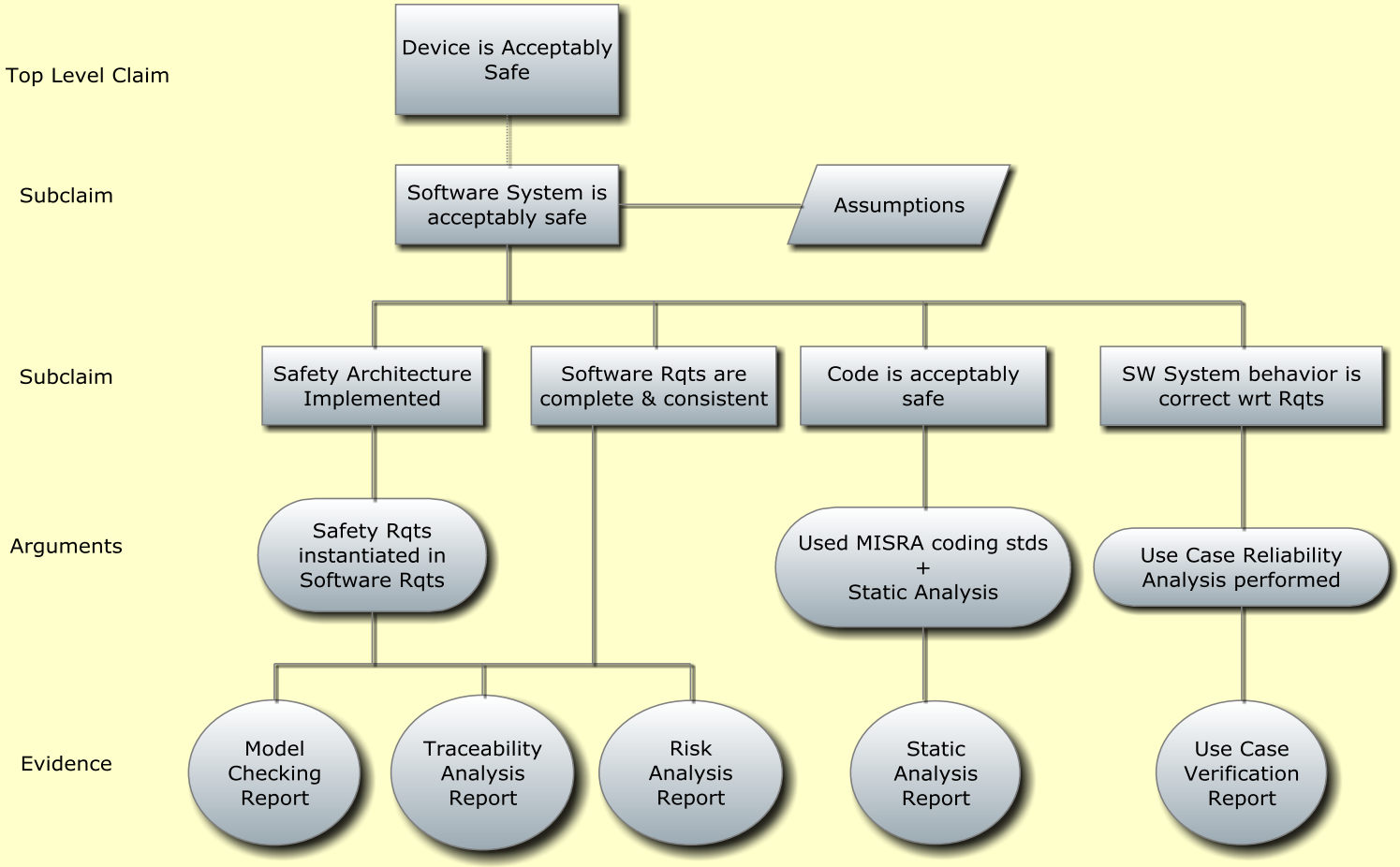


Assurance Case Framework




Basic Safety
Essential Performance
Operational Safety
Installation & Use
Commissioning
Safety Justifications
Hardware System
Safety System
Human Factors
Software System
Design Safety
Environmental Safety
Functional Safety
Algorithm Safety
Interoperability
Data Integrity
Security
Safe Coding Practices
Verification

Possible Software System Safety Case Fragment
- ILLUSTRATIVE -



Regulatory Physics

$Confidence = Q_{specs} \times Q_{accep} \times Q_{evid} \times Q_{traceability} \times J$, where¶

- Q_{specs} is the quality of regulatory specifications, measuring the overall comprehensiveness and correctness of these specifications. ¶
- $Q_{accep} = \prod_{\text{for all acceptance criteria}} Q_i$, where Q_i the quality of acceptance criterion i, measuring the reasonableness and/or acceptance level of i. ¶
- Q_{evid} is the quality of all evidences submitted by the manufacturer, measuring the trustworthiness, integrity, and acceptance levels of all such evidences.¶
- $Q_{traceability}$ is the quality of traceability information submitted by the manufacturer, measuring the Correctness, Consistency, and Completeness (C^3) of the traceability, and ¶
- J is a judgment that regulators make on how well the acceptance criteria are met by the device based on all the evidences.¶

If all of the above quality values and J fall into the range of [0, 1], then the confidence level is also somewhere in the range of [0, 1].¶