The Regulation of Change in Air Navigation Services

Some current issues

John Penny
System Safety Specialist
CAA (SRG)

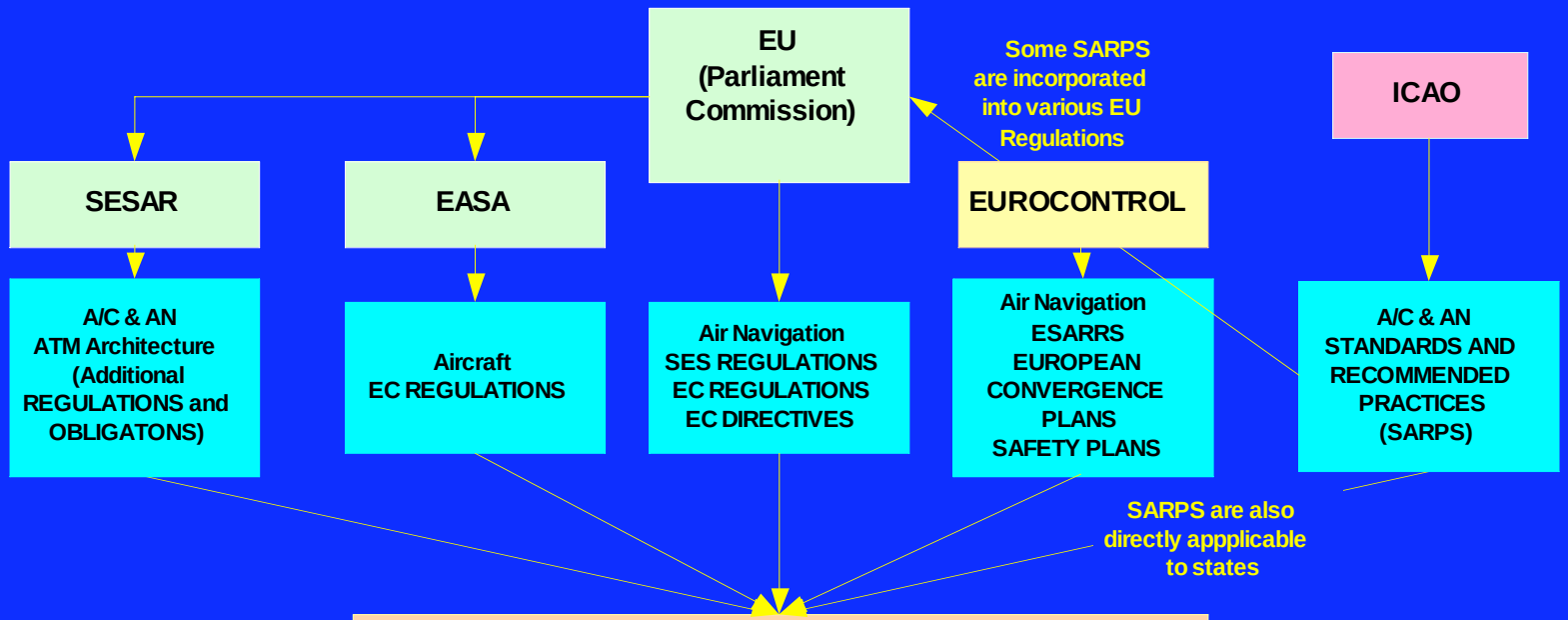
Safety Regulation Group

CIVIL AVIATION AUTHORITY

Single European Sky

- Overview - organisations
- Oversight of change
  - Risk Assessment & Mitigation
- Goal Based Regulation
- Safety & Interoperability

Organisations



STATES AND ATM INDUSTRY
SUBJECTED TO VARIOUS REGULATIONS AND OBLIGATIONS

SAFETY :
SES REGULATIONS
EC REGULATIONS
EC DIRECTIVES
EASA REGULATIONS
ICAO SARPS
ESARRS
EUROCONTROL/EUROPEAN SAFETY PLAN
EUROCONTROL/EUROPEAN CONVERGENCE PLAN

INTEROPERABILITY /CAPACITY/QUALITY/SECURITY/ECONOMIC:
SES REGULATIONS
EC DIRECTIVES
EUROCONTROL /EUROPEAN CONVERGENCE PLAN

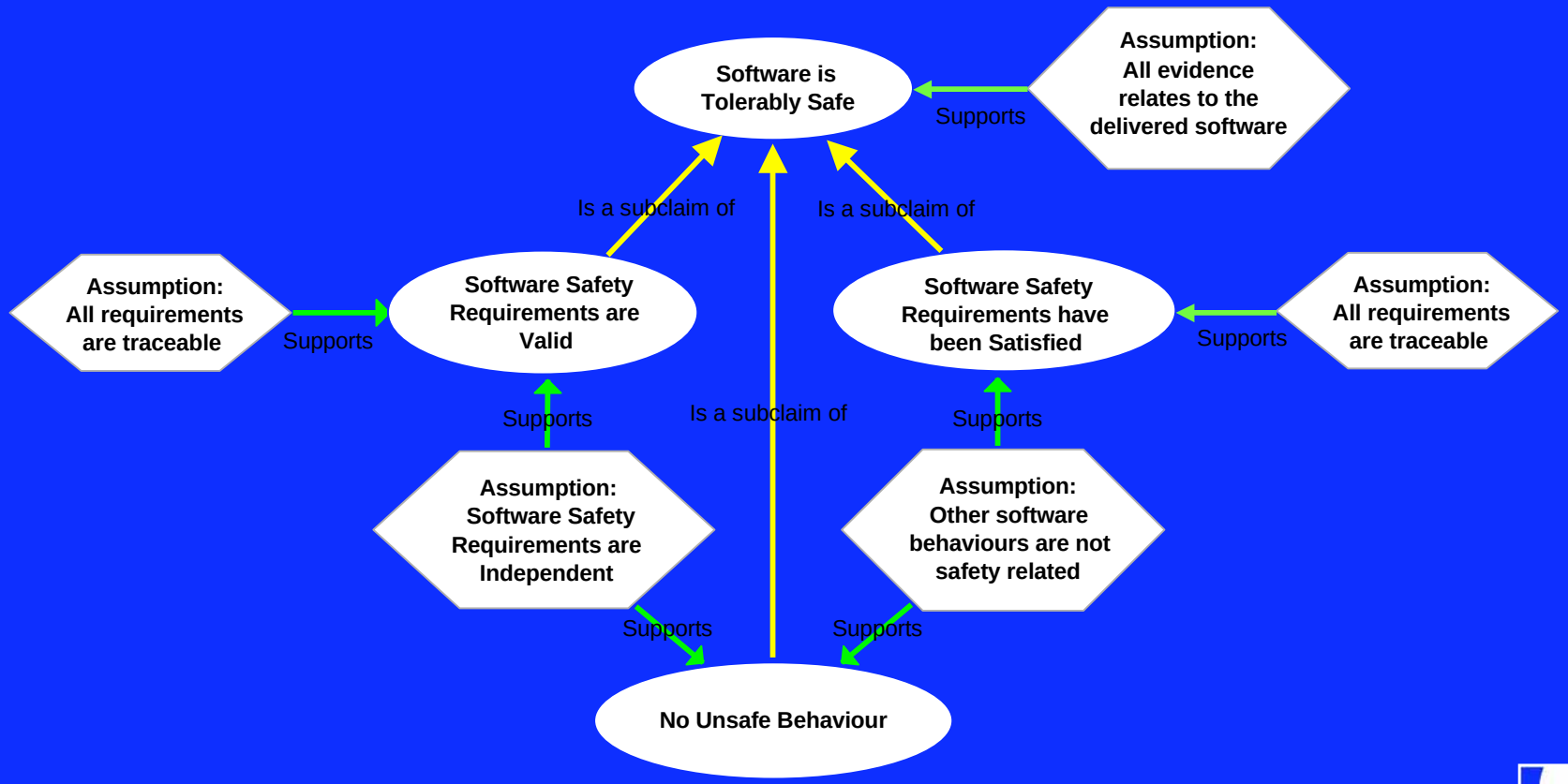
Oversight of change

- Change Principle
  - Don't do it until you know its safe
- Risk Assessment & Mitigation
  - All parts of the system (People, procedures, Equipment) and the environment of operations
  - Quantitative risk/Cumulative risk
  - Argument
- Choices
  - Proportionate regulation *(Hampton et al)*
  - It is not a case of "to oversee or not to oversee" but "how much to oversee and when to oversee".
- Oversight criteria
  - Supplier competence/performance,
    Safety risk of change,
    Novelty/Size/Complexity of change
  - Objective measure of regulatory risk informs the depth and rigour of the oversight

SES - Goal Based Regulation

- Notion of a single Target Level of Safety (TLS) for Air Navigation Services – 1.55.* 10^{-8} accidents with Air Navigation causes per a/c flight hour (ESARR 4)
- Service provider argues that safety risk is acceptable via a safety case
  Single goal – 'TLS will be met'
- Properties of the argument are prescribed
  - Safety objectives/Safety Requirements
  - Satisfaction of safety requirements
  - Traceability to service level functions
- No prescription on form of the argument
  - Freedom to innovate system structure/component detail/component source
  - Freedom to innovate arguments
- Constraints on scope and applicability
- ALARP ?

Experience of GBR – SW01
Complete SW Safety Model



Safety Regulation Group

CIVIL AVIATION AUTHORITY

Experience of GBR – SW01

- SRG has been working with Air Navigation Service Providers to provide appropriate guidance:
  - COTS guidance - available
  - Legacy guidance – end of year
- Research is being performed on some underlying issues:
  - Apportionment of safety requirements
  - Use of architecture & verifiability of components
  - Verification of safety requirements using statistical test
  - Objectivity/confidence in combining arguments and evidence
  - Modular safety cases
- Overall, although the cultural change has proved challenging, the techniques developed show promise. The 'genie is out of the bottle' and there can be no going back.
- EC are currently transposing ESARR 6 (SW01) into EU regulations.

Experience of GBR – SW01

- Product vs process: Predominance of process standards mitigates against argumentation.
  - Prescribed techniques do not necessarily lead to satisfaction of safety requirements – SIL x $\neq 10^{-y}$
  - Saliency and strength of evidence not dealt with
  - Little experience of Argumentation
- Evidence: Both product and process evidence is needed
  - Uncertainty about provenance of evidence undermines confidence
  - Process arguments should be linked to items of product evidence not assumed to give blanket coverage
- Argument chains / diverse reasoning:
  - Product and process arguments are diverse. When combined, what is the confidence that the overall argument has satisfied the claim?
  - Diversity exists independently in product and process evidence as well: proof, test, analysis. None are perfect.
    What is the confidence in the overall argument?
  - Stopping conditions – when have we assembled sufficient evidence

Experience of GBR – SW01

- Safety and the supply chain
  - Long chain of suppliers
  - Contracts aimed at mitigating business risk do not assist development for safety or safety assessment
    - Encourages a ‘silo’ mentality
    - Customers are unaware of the architecture of subsystems/components
    - A component delivered to satisfy a set of safety requirements ignores the behaviour present in the component but unspecified by the customer
    - Suppliers often use COTS or legacy components without having to declare them to the customer
    - Suppliers are often unaware of the constraints the environment can provide
- Improvements in component trustworthiness will assist but more open architectural development/analysis is still needed

Safety & Interoperability

- SES interoperability is based on standard components and standard policies/practices
- Benefits of standard components
  - Efficiency of inter-working across systems
  - Economies of scale
  - Evidence of the integrity of implementation improves over time
- However ‘component safety’ is a non-sequitur
  - A component is neither safe nor unsafe
  - Components can be used safely or unsafely
- The property of concern for a component is its ‘Trustworthiness’ i.e. does its specification correctly declare ***all*** its behaviour

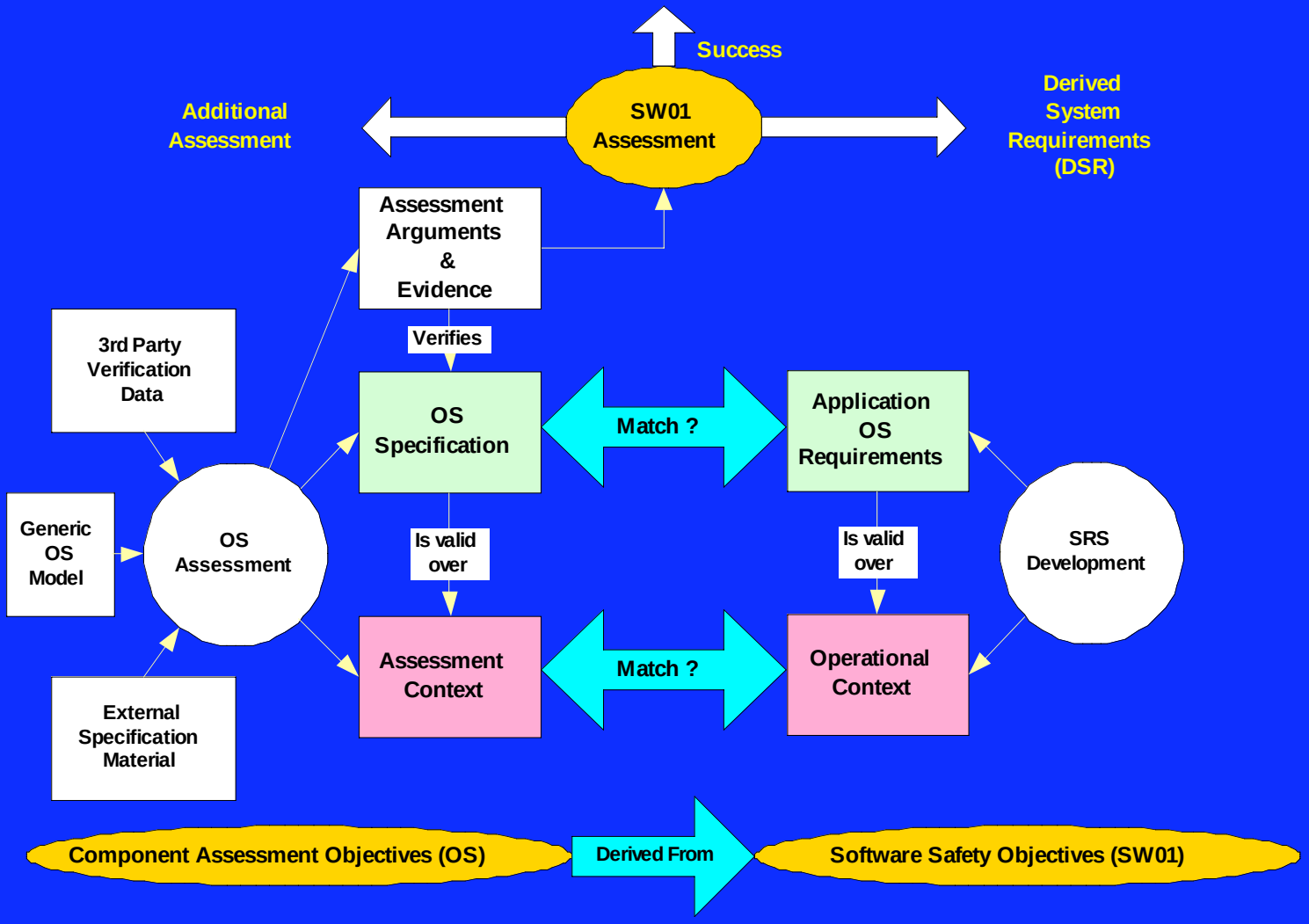
Interoperability - Systems

- Systems and procedures for airspace management.
- Systems and procedures for air traffic flow management.
  - TACT, TLPD, IFPS, ADEXP, OLDI
- Systems and procedures for air traffic services.
  - RDP, NAS, VCS,
- Communications systems and procedures.
  - Radios, CPDLC, Voice Comms, Data Comms
- Navigation systems and procedures.
  - NDB, VOR, DME
- Surveillance systems and procedures.
  - PMR, SSR, ASMGCS, MultiLat, ADSB, CPDLC, NODE
- Systems and procedures for aeronautical information services.
  - ATFN
- Systems and procedures for the use of meteorological information.
  - MARS

Practical Trustworthiness?

- Safety assessment relies on knowing the complete behaviour of the component
- The complete behaviour of a moderately complex component is essentially limitless
- Components always do more than it says ‘on the tin’
- Weaken – add a constraint:
  Safety assessment relies on knowing the complete behaviour of the component in its environment of operation.
- Providing the component specification correctly describes all its behaviour in a completely defined environment and that environment exactly matches the environment of use then the component behaviour is completely known
- The fidelity of the context specification is as important as the fidelity of the behavioural specification
- Architecture is key:
  A well designed system provides the opportunity to constrain component context and allow trustworthy behaviour to be demonstrated within practically verifiable limits

Example: Assessing COTS against SW01



Mismatches

	SW01 Assessment	Action (SRS Development)
OS Specification vs SRS Requirements	Complete match	None (Very Unlikely)
	More behaviour	Assess impact (CBA): None/DSRs/Look for another OS
	Less behaviour	
Assessment Context vs Operational Context	Covers	None
	Partially covers	Assess impact (CBA)-Change: Application context (DSRs) OS context (Additional assessment)
	Does not cover	Look for another OS
Confidence in behaviour vs Confidence required of behaviour	Higher	None
	Equal	None
	Lower	Assess impact (CBA): DSRs/Additional Assessment

Conclusions

- What would a regulator like to see?
  - That Safety Cases are primarily of use to the ANSP
  - A balanced view of the role of product and process arguments
  - Realistic safety requirements and realistic reliability claims for components
  - Inclusion of the whole supply chain in the architectural design and analysis of a system
  - Holistic systems engineering (human factors engineers?)
  - Argumentation (a bit of philosophy!) to feature in engineering education
- Above all – Think Safety!

Additional Slides

Expansion of Oversight slide

Safety Regulation Group

CIVIL AVIATION AUTHORITY

Change Principles

- The safety of the change should be predicted.
  (Do not make a change if you don't know how safe it will be.)
- … before there is a chance of actual harm being caused
  (Do not introduce any part of the change before there are arguments and evidence that it will be safe i.e. produce a safety case before any physical change is made.)
- Any change should leave the service at least as safe as it was before
- Harm may be caused during: Installation, commissioning, operation (including planned changes), maintenance and de-commissioning.
  (If an operational change is required that is not covered in a safety case then it is considered as a new change – start again!)
  (Evidence for operation can be gathered during installation and commissioning e.g. the operational safety case does not need to be complete until just before operation begins.)

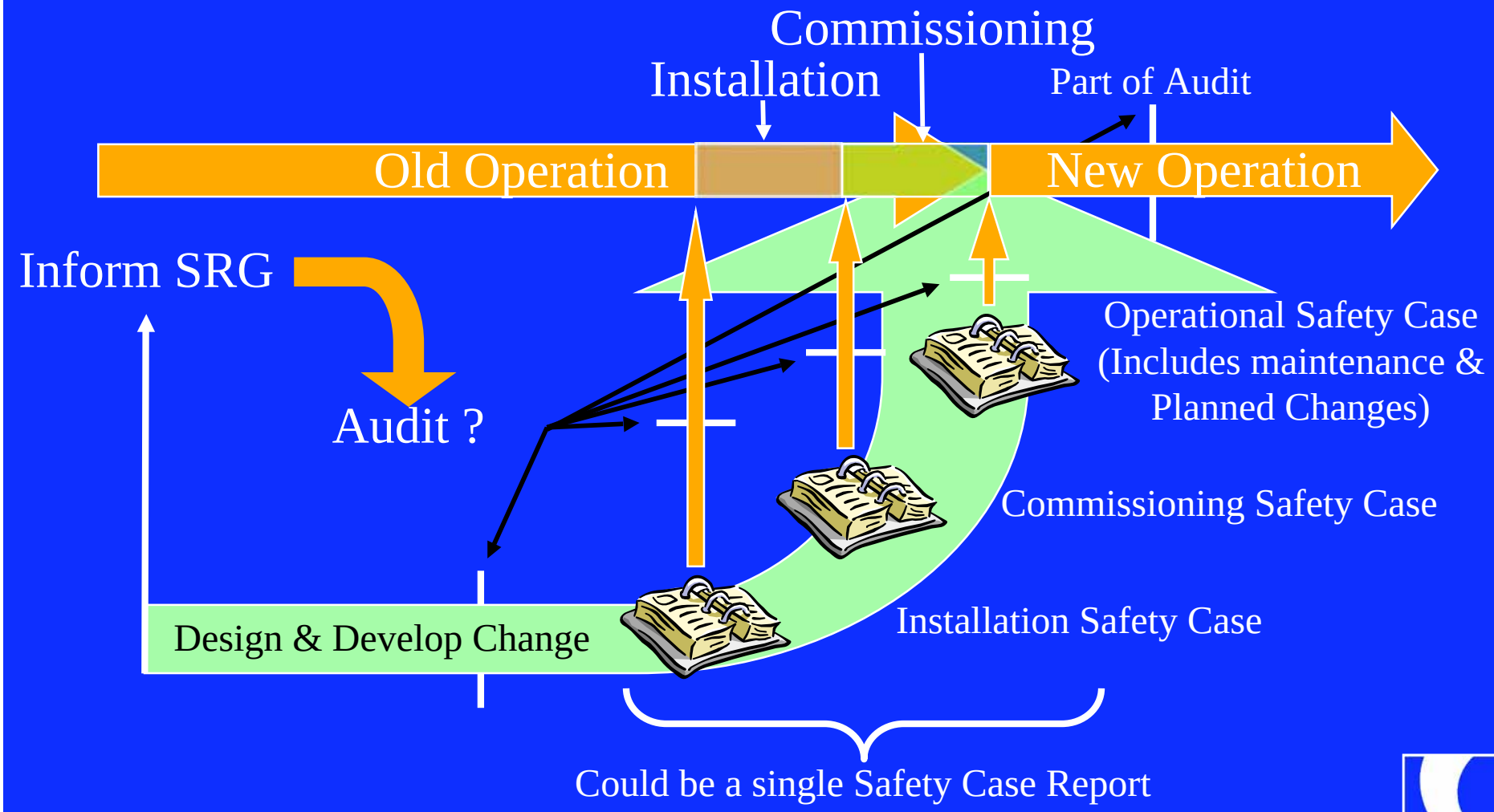
Note: These principles equally apply to establishing a service

i.e. going from no service to a service is a change

Risk Assessment and Mitigation

- All parts of the system (people, procedures and equipment (hardware and Software)) are to be subjected to ***quantitative risk*** assessment *(where practical)* and mitigation.
- The environment and the organisation must also be considered for their impact on safety risk.
- Services and products used by the ATSP but not managed by him are also subject to Risk Assessment and Mitigation (RAM).
- Risk Assessment and Mitigation must consider all phases of operation from installation through to de-commissioning, including maintenance and operational changes.
- The risk assessment is to deal with ***cumulative risk*** i.e. the ***total risk*** of all the services offered must be ***tolerable***.
- The ATSP is required to ***argue*** the safety of ***each*** change. *(The Safety Case)*

Fitting Oversight to the Change lifecycle



Safety Regulation Group

CIVIL AVIATION AUTHORITY

Oversight Choices

- It must be the case that:
  - Some changes are reasonably simple and require little oversight. Any oversight could be part of periodic audit
  - Some changes are so 'risky' that the NSA should be involved from very early in the project and consequently will need to signify approval prior to operation.
- UK Government guidance is to move towards 'proportionate regulation': *(Hampton et al)*
  - risk assessment should be the foundation of all regulators' enforcement programmes;
  - there should be no inspections without a reason, and data requirements for less risky businesses should be lower than for riskier businesses;
- It is not a case of "to oversee or not to oversee" but "how much to oversee and when to oversee".
- How do we choose what and when to oversee?

Oversight Criteria

- Generally the criteria are drawn from the following categories:
  - Supplier competence
  - Supplier performance
  - Safety risk of change
  - Novelty of change
  - Size of change
  - Complexity of change
- An objective combination of these is referred to as a measure of Regulatory Risk and is used to inform the depth and rigour of the oversight.
- SRG is currently reviewing its measure of Regulatory Risk in the light of the SES changes