APPENDIX 2-2

Safety

Example Justification using Goal Structured Notation

1. Safety Regulatory Objectives

- Definition/explanation of strategic safety objectives linked to equivalence and transparency
- Introduction of the Goal Structure Notation (GSN) focussing on Goal 1 in this report
- Precedence for Objective Safety Regulation (e.g. ESARRs, CAA CAP 670 SW01, UK Defence Standard 00-56 Issue 3) TOP-DOWN approach
- Capturing the overall safety picture both operational safety and airworthiness
- Interaction between Strategic Safety Objectives and existing regulation

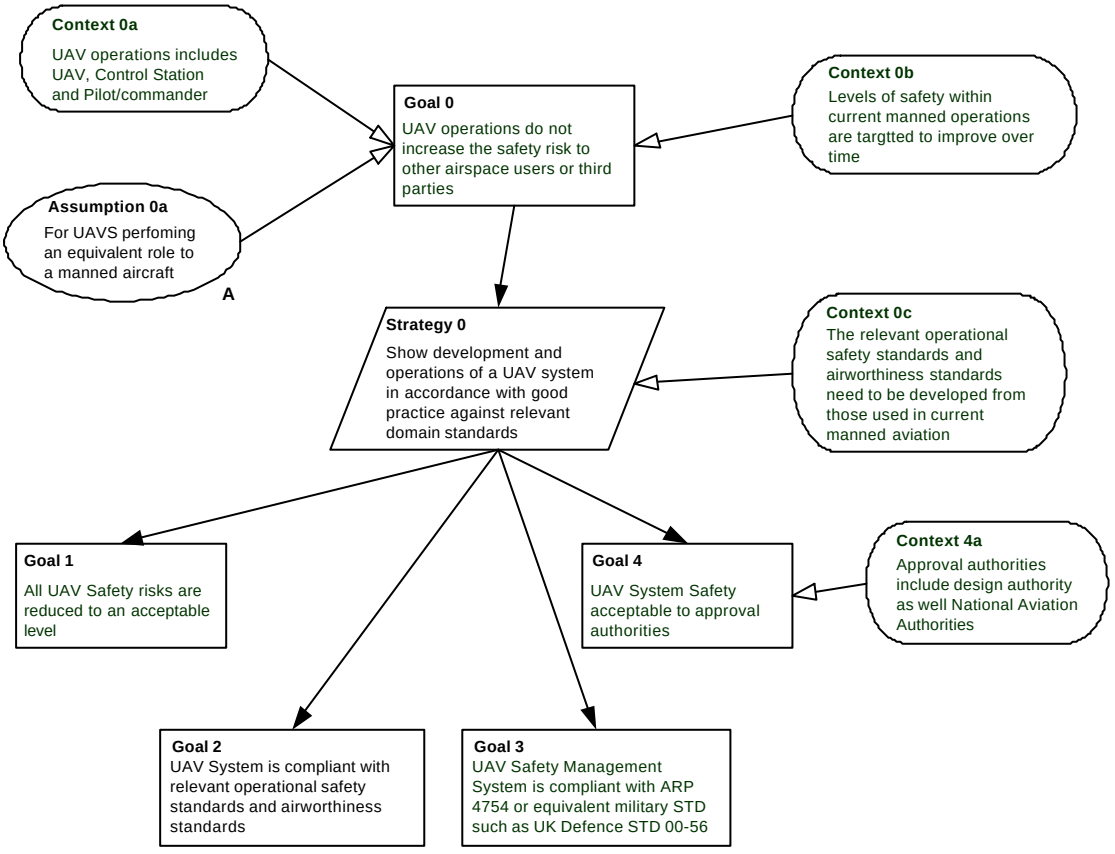

Figure 1 – Top Level Statement (Goal) and Strategy for its determination

Explanaition of

GSN Element	Explanaition
Goal 0	Top level objective taken from principle objective to ensure that UAVS operation in civil airspace does not increase the risk to other airspace users or third parties.
Context 0a	UAVS is a complete system of systems including the Air Vehicle(s), Control Stations, pilot/commander, maintainer, operator and the

	interface with the overarching Air Navigation System.
Context 0b	The target levels of safety set for Civil Airspace are not static, with increase in air traffic demanding more stringent safety targets to ensure that risks decrease in the future
Assumption 0a	In current regulatory framework there is not one certification standard for all aircraft rather each certification is tailored based on the categorisations of the aircraft. As such UAVS certification is likely to based on a similar premise, with different levels of certification depending on factors such as intended airspace, weight, kinetic energy, mission (e.g. military or civil), etc.
Strategy 0	To show that UAVS will not increase risk to users and third parties we need a coherent, rational and workable regulatory framework in which to assess and certify.
Context 0c	The current regulatory framework does not cater for all types of UAVS and their intended applications so needs to be evolved if UAVS are to realise a wider role in aviation.
Goal 1	Primary safety risks from UAV operations are described further in the next section.
Goal 2	As the regulatory framework evolves UAVS must still be shown to comply with all relevant regulations. Reference to existing airworthiness and ATC JARS/FARs
Goal 3	Safety Management Systems for organisations and companies involved in UAVS design, development, manufacture and operation. E.g. Design Approved, licensed, etc. Reference to certification of organisations
Goal 4	UAVS Approval procedures should be the same as for manned aircraft certification processes. Reference?

2. Safety Risk considerations

- Need to agree an acceptable level of safety risk
- Relevant risk factors: population density, kinetic energy, airspace, lethal area (related to kinetic energy), complexity.
- Not possible to provide absolute assurance but need to ensure that we have done all that is reasonable practicable to identify all of the risks to safety posed by the introduction of UAVS.
- Risk initiators include: random and systematic factors, e.g. lack of consideration of airworthiness issues, poor design or build, lack of understanding of operational context (overall risk spectrum, procedures, training, etc)
- Potential Risk issues specific to UAVS: flight termination (need and mechanisms for), continued safe flight following loss of data link, UAVp situational awareness, operations in VFR (e.g. sense and avoid),
    - *a mission will be carried out from the location of the control station , as much the demand for a long range data-link comes up. Thinking about a so called "Global Mission", the need of a satellite system is a must to be discussed.*

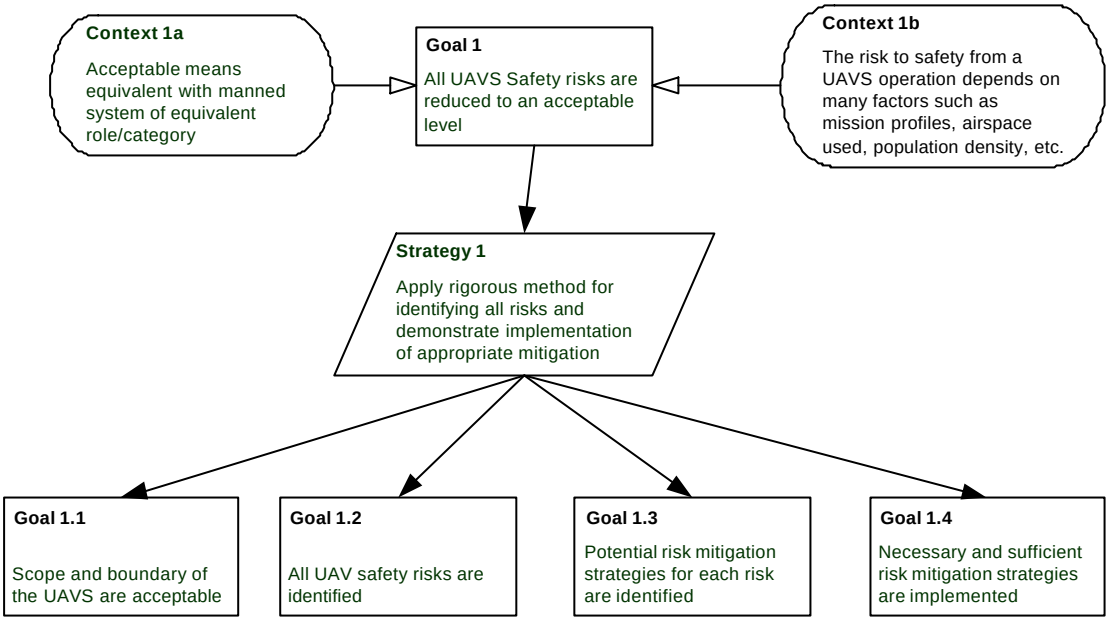

Figure 2 – 1st Level - Goal 1 "Acceptable Risk" and its determination strategy explored

3. Scope of UAVS operations

- Need to understand the intended operational role or set of missions for the UAVS as well as any limitations imposed by the capability of the UAVS and whether or not the role can be implemented through exceptions to certification.
- Knowing the mission will lead to the 4 following questions:
  - What will be the main task of the system ?
  - How long does a mission take ?
  - Where do we want to operate it ?
  - Who is going to operate it?
- Example categorisations

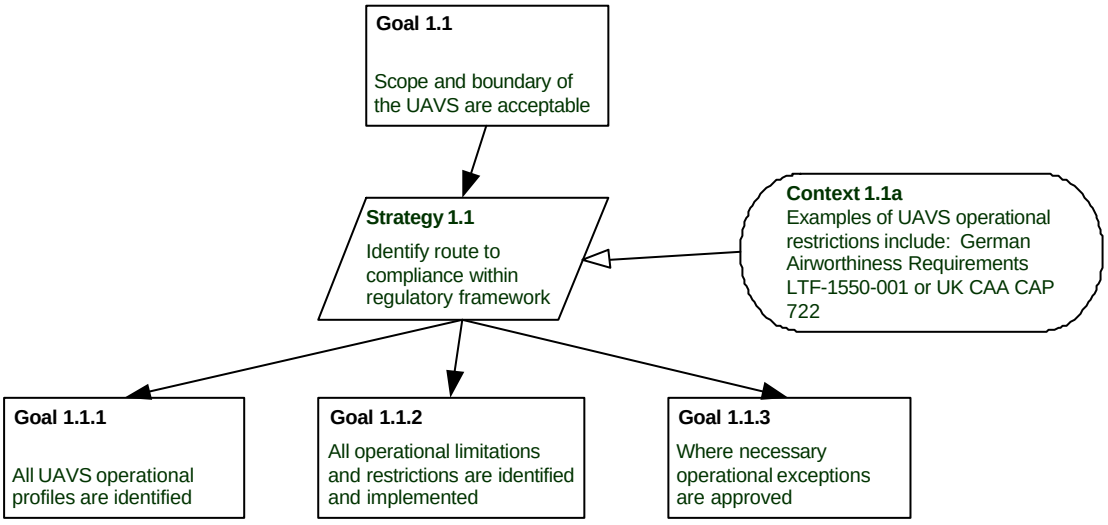

Figure 3 – 2nd Level - Goal 1.1 "UAV System Scope" and its determination strategy explored

4. Identification of UAVS Safety Risks

- Overarching approach to safety assessment for UAVS

- Introduction to risk id techniques (from ATM safety paper – AJS)
- Link to GSN

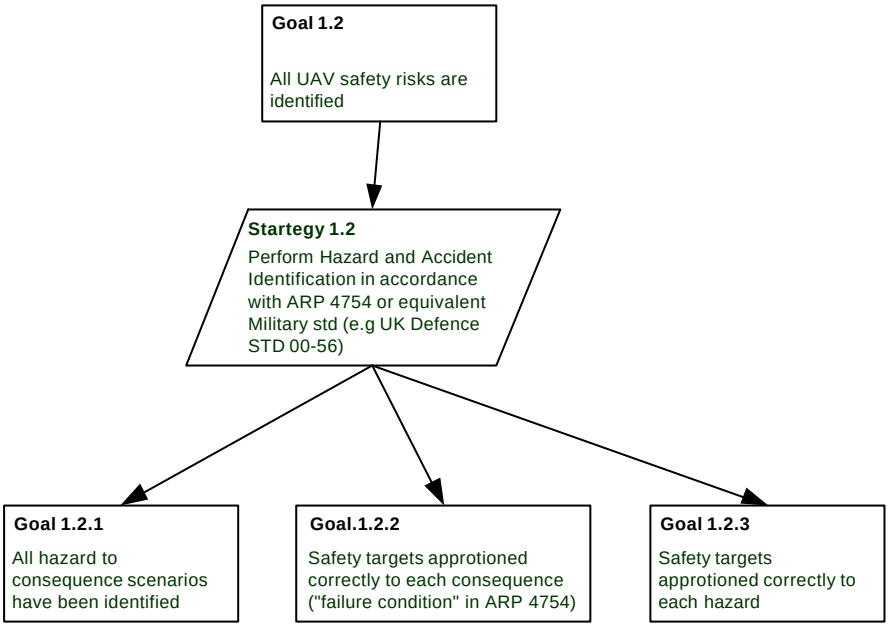

Figure 4 – Level 2 - Goal 1.2 "Risk Identification" and its determination strategy explored

- Significant aviation accident scenarios (references are SRC doc 2 Review and Analysis of Historical Data)
    - mid-air collision
    - air vehicles hits the ground
    - air vehicles hits objects on the ground
    - accidents related to landing aids
    - Also need to consider: detachment of air vehicle components, operation of hazardous UAV components (e.g. rotor blades, radars, specific payloads, etc.)
- Potential UAVS related causes of accidents (under work)
    - Unrecoverable loss of Air Vehicle control
    - Extraneous changes in air vehicle attitude
    - Air vehicle piloted off cleared level
    - Incorrect display of air vehicle position (in 4-D)
    - Spurious air vehicle positional drift
    - Air vehicle accelerated fatiguing events
    - Uncontained release of high energy debris (e.g. jet engine disintegration)
    - Extraneous deployment of flight termination devices
    - Insufficient thrust for flight
    - Critical failure of component mounting/ interface
    - Air vehicle recovery when not cleared to do so
    - Air Vehicle launch when not cleared to do so
    - Reduction in Air Vehicle Lateral Control during recovery
    - AV launched when AV not fit for flight
    - Occupational Health Hazards
    - Unlawful Intervention
- Potential UAV causes can be caused by Air Vehicles or Control Station
    - Loss of or errors in flight control
    - Loss of power
    - Loss of or errors in communication (ATC, datalink, transponder)
    - Loss of or errors in navigation (positional awareness, position reporting)
    - Loss of propulsion (Engine failure, fuel leak, excessive fuel use)

- Failure of UAV launch or recovery mechanisms

- Fault Tree – one example

5. Risk Mitigation Identification and Implementation

- Risk mitigations specific to UAVS
  - Emergency procedures, flight termination, etc.
  - Data link loss
  - Remote piloting
- Operational risk mitigations already built into current Air Navigation System – need to be transparent, need conformance with other air users in order to share airspace safely.
- Design Risk Mitigation –
  - Compliance with Airworthiness JARs
  - Lot of advice in ARP 4754, but may need updating to cover UAVS specifically.
- Principles – Safety Case built on certification and operational procedures
- Manufacturing, operation and maintenance will have to be organized in accordance with commercial regulations (i.e. JAR 21, JAR 145 and JAR OPS)
- Link to GSN

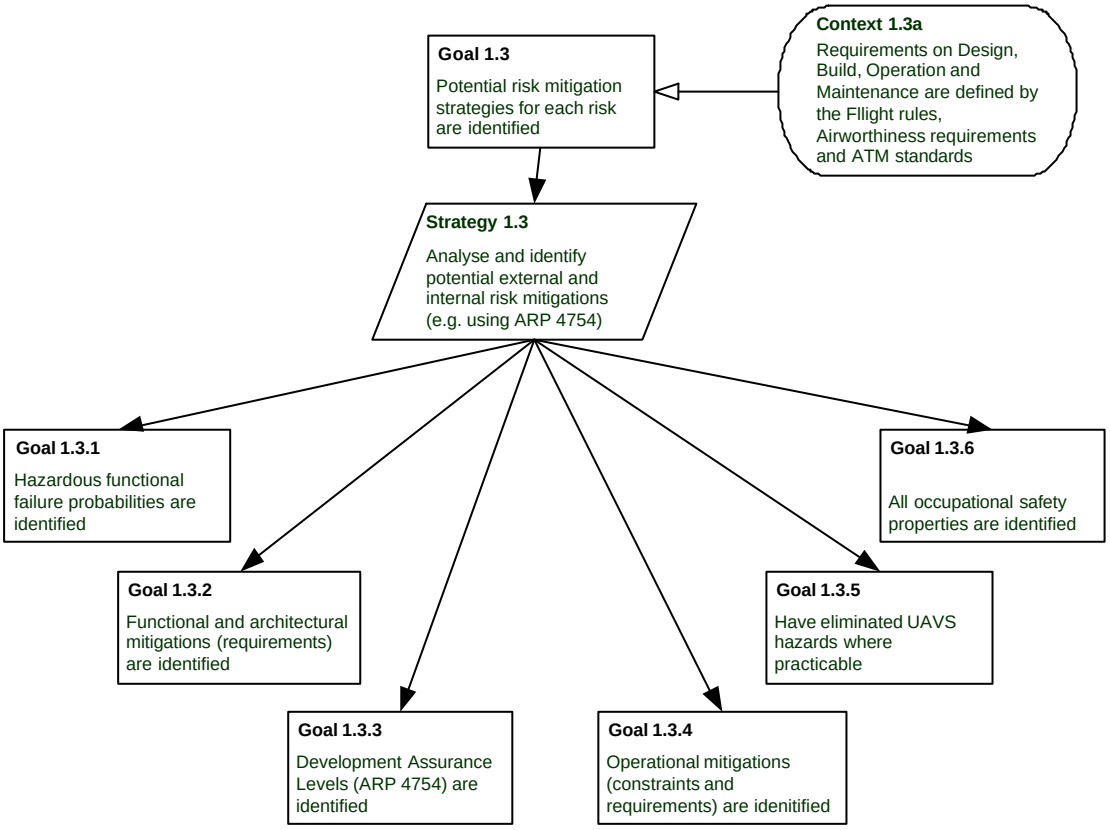

Figure 5 – Level 2 - Goal 1.3 "Risk Mitigation" and its determination strategy explored