Points that might be mentioned in an answer RJA

- clarify the safety requirements of individual subsystems; each should have a documented safety case that must be maintained through the reengineering process
- limit interactions by specifying interfaces carefully and tying them in to the component safety cases
- develop documentation + testing procedures for the QoS that the common platform must deliver
- ensure that common-platform failures are worked in to the individual safety cases, using whatever methodology the contractor uses (FMEA, fault tree analysis, ...)
- deal with compatibility issues, e.g. if two contractors use differing methodologies. You may have to impose product-wide or even industry-wide standards
- component-level testing should be broadened to include faulty + perhaps malicious inputs from other components
- system-level testing will need to be added
- while the above might be managed as a top-down project, waterfall style, one of the outputs of the project must be a system for evaluation and assurance of upgrades done later using an evolutionary methodology
- in the late, evolutionary, phase, feedback will be important. Systems for dealing with customer alerts / accident reports will be necessary
- might consider mechanisms for field upgrade if bug discovered (recall if severe, else during servicing)