Development Plan Impacts

At this point in the LSST DMS design process it is impossible to fully specify the fault tolerance strategies to be used by all components, particularly when the algorithms to be implemented are not yet fully understood. It is possible, however, to specify how fault tolerance will be incorporated into the design, development, and testing process so that cost and schedule impacts may be estimated.

The fault tolerance software frameworks, as described above, will be developed by the middleware team. Their areas of applicability, detection strategies, and recovery strategies will be clearly documented. Tests of the common failure classes and their handling by the frameworks will be included in not only framework-specific test suites but also integration test suites.

As a system is designed, a fault tolerance design pattern will be chosen for each of its components so that the overall system can meet its availability requirements. In particular, an appropriate software framework will be chosen. As part of the analysis to determine the proper pattern, system-unique fault types will be identified. If the framework-provided treatments are inadequate, extensions may be added to the framework or custom mitigations may be developed, provided that the benefits are worth the lifecycle costs.

Examples of these choices might include:

- Infrastructure systems such as routing, DNS, and authentication are expected to use the redundancy strategy, with hot/hot or hot/standby configurations.
- The data ingest system and the image storage and retrieval system will also use redundancy to protect against data loss. Checksumming and acknowledgments that data has been written correctly to stable storage will be used as fault detection strategies.
- The image processing pipeline in the nightly alert processing will likely use a strategy that delivers partial results on time and uses spare capacity to deliver the remaining results later. This strategy will be implemented as a configuration of the pipeline framework.

System developers will need to document their choice of fault tolerance design pattern and any variations from its software framework. They will show that the availability requirements will be met. Preventive maintenance procedures will also need to be documented.

System-unique failure modes will be incorporated into system test plans.

The end result will be a common set of fault tolerance concepts and practices, implemented in shared software and hardware requirements, that is applied in a documented and tested fashion to each of the DMS systems.