Abstract

An Operational Information System (OIS) supports a real-time view of an organization's information critical to its logistical business operations. A central component of an OIS is an engine that integrates data events captured from distributed, remote sources in order to derive meaningful real-time views of current operations. This Event Derivation Engine (EDE) continuously updates these views and also publishes them to a potentially large number of remote subscribers. This paper describes a sample OIS and EDE in the context of an airline's operations. It then defines the performance and availability requirements to be met by this system, specifically focusing on the EDE component. One particular requirement for the EDE is that subscribers to its output events should not experience downtime due to EDE failures and crashes or increased processing loads. This paper describes a practical technique for masking failures and for hiding the costs of recovery from EDE subscribers. This technique utilizes redundant EDEs that coordinate view replicas with a relaxed synchronous fault tolerance protocol. Combination of pre- and post-buffering replicas is used to attain an optimal solution, which prevents system-wide failure in the face of deterministic faults, such as 'ill-formed' messages. By minimizing the amounts of synchronization used across replicas, the resulting 'zero downtime' EDE can be scaled to support the large number of subscribers it must service.