LIGO MIT
MIT Room NW22-295
185 Albany Street
Cambridge, MA 02139

TEL: 617.253.4824
FAX: 617.253.7014

January 14, 2009

To: R. Adhikari
From: R. Bork, T. Fricke, M. Landry, J. O'Reilly, S. Waldman, M. Zucker
Re: Review of HAM ISI watchdog implementation
Ref: LIGO-E0900006-x0

We met 1/13/09 to review the software safety implemented by AdL SEI group on the HAM ISI installed and in HAM6 at LLO. The code has also been concurrently implemented on the LHO HAM6 ISI.

J. Kissel, B. Abbott and B. Lantz presented and answered questions on information collected at
http://lhocds.ligo-wa.caltech.edu:8000/advligo/HAM_Watchdog_Review

Key design documents include LIGO-T09000011, *The HAM ISI Watchdog* by J. Kissel, and LIGO-T0810027, *Advanced LIGO Watchdog Concept* by R. Bork and R. Adhikari.

In summary we concur that after two modifications detailed below, and after successful completion of the proposed testing already in progress, the implementation should afford sufficient protection to SEI and payloads to permit safe unattended operation.

We make several additional requests for technical clarification, and suggest or recommend some design improvements. Resolutions are not expected to interfere with deployment.

It should be clarified that SEI protection will not be complete (to AdL standards) until a basic hardware layer is added, as outlined in T0810027. This will enforce a hardwired "keepalive" pulse, to protect against frozen processes or communications, and will enforce physical disconnection of DAC outputs from actuators on fault detection.

This hardware modification will be retrofit to field systems as soon as available. The software system reviewed here is operationally compatible with this future hardware interface layer, with minor or no changes.

A. REQUIRED MODIFICATIONS

1. **Implement forcing of default trigger thresholds** *(Lantz, Kissel)*
As now configured it's possible (for diagnostics, or by error) to set trigger threshold EPICS fields at unsafe values and leave them that way. Robust automation, which is itself difficult to circumvent or "adjust," is required to enforce the trigger defaults. For example, built-in "sunset" code could relax changes over some set interval, or the EPICS alarm handler could mask values and light off a corrective script. Since natural fault events typically produce confusing cascades of alarms, some of which cannot be cleared for a long time, reliance on alerting operators to take corrective action is *not* adequate.

2. **Ensure watchdog fault conditions are detected by the alarm handler** *(Lantz, Kissel)*
At a minimum the EPICS alarm handler should post operator alerts. To whatever extent it's consistent with recommendations discussed below, also consider having the alarm handler trigger a "down" script or other direct action.

B. RECOMMENDATIONS AND CLARIFICATIONS

3. **Justify complication caused by providing intermediate "damping only" fault states** *(Lantz)*
It's clear that reverting to optimized damping after an overload is likely to provide the gentlest landing for the payload, *in that subset of cases where it can be arranged*. However the payload has to be engineered to

withstand hard ISI shutdown anyway (e.g., when OMC SUS triggers the fault in the first place, when any trigger is not otherwise cleared within the timeout, etc.). "Soft" fault trips (those which leave damping capability intact) should account for a decreasing fraction of all faults, once isolation loops are commissioned to the required degree of robustness. It is unclear that reduced mechanical severity for some decreasing fraction of nuisance trips balances the burden of maintaining and vetting multi-state safety code, or the increased likelihood such code itself may fail.

4. **Verify stability of "damping only" loops under correlated sensor loss** *(Kissel)*
It is good that damping loops behave well when a sensor fails. Loss of correlated groups of sensors (e.g., associated by common power supply, AA chassis, ADC, cable, feedthrough) should also be checked out.

5. **Consider adding "dead channel" test** *(Lantz)*
As now configured the system only triggers on large absolute values. A dead or intermittent channel is only detected insofar as, and only after, it leads to loop instability. It also does not present any overt diagnostic symptom, nor any impediment to clearing the fault and restarting (presumably to repeat the cycle). With reasonable respect for CPU time, consider adding an RMS window test to trigger on unphysical sensor signals.

6. **Reconsider execution platform for auxiliary scripts** *(Kissel/Thorne/Barker)*
The three auxiliary shell scripts were not deemed critical to safe operation, but rather add operational convenience. Consider possible benefits (e.g., to maintainability, code revision coordination, network fault tolerance, etc.) of having these ISI-watchdog-specific scripts execute on the front ends, rather than the designated Ops script engine.

7. (related) **Develop a more robust way to insure that checker script is operating** *(Lantz)*

8. **Track watchdog variables in the conlog** *(Kissel/Thorne/Barker)*

9. **Detect and trigger on STS-2 saturations as well as ISI sensors** *(Kissel)*

10. **Describe prior fault incident(s) (e.g., 12 November 2008) and show how comparable faults are now precluded** *(Lantz)*

11. **Think of a better name than 'watchdog'** *(Adhikari)*