File 20101210.0709: Weekly activity report 0166:

```
weekly activity report 166 (loughry)
Joe Loughry
Sent: 10 December 2010 07:09
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20101209.1727 (GMT-7) sequence no. 0166, week 8+1 MT

I am struggling to get a simulation of the exact model I described in my
confirmation report running in time for the assessors to look at next
week; I do not want to have to re-draw the figures.  Using a pair of
integrals from $\ddot{x}$ to $\dot{x}$ and from $\dot{x}$ to $x$ on the
separated components of $\vec{v}$, I can get a reasonable-looking phase
space plot of the convergence behaviour with one force, but when I try
to run five forces in parallel, the simulation gets confused.  Part of
the problem is the limited toolbox in Simulink: there are step function
inputs available for use as a forcing function, and initial conditions
that I can set in the integrator, but neither of these is exactly suited
for the purpose I need, which is to model the behaviour after release
from a stressed initial position, not the action of a forcing function
on a system initially at rest.  Although setting an initial condition in
the integrator works well, it results in an artefact at the beginning
of the motion, throwing off the early trajectory although not the the
final result.  It is, however, the first few moments of the trajectory
that are most needed.  I now plan to use step functions, calculated
'backwards' from the fixed point at equilibrium (using a straight
line extrapolation until it is demonstrated that I need anything more
complicated) and set equivalent to the resultant force calculated at
each point from the initial conditions, to set everything in motion
simultaneously at the start.  This should yield an equivalent result.

If this doesn't work, I am going back to a discrete time simulation.
The root of the problem is that mass is implicit in the Simulink model.
Nowhere in the parameters of the simulation does a straightforward
value for $M$ appear.  It must instead be encoded as $1\over M$ in a
seemingly redundant gain block.  I can tolerate implicit values for
$M$ because inertia in this model is a synecdoche anyhow; what matters
is the path through risk space, although relative speed might become
important later.  A consistent assignment of concepts to values is
crucial; I claim that the path taken from a fixed point established
by the certification authority---the evaluated configuration at the
end of CT&E---to an equilibrium determined uniquely by the initial
conditions is related to observations in the case studies such that if
the path can be projected early in the ST&E process it has predictive
value for the final agreed-upon set of risks and risk mitigations
that will be acceptable to all accreditors and result in accreditation
without the necessity for inter-accreditor communication that violates
security policy.  The foregoing is too complicated a statement to defend,
however; it carries with it excessive implementation detail irrelevant
to the essential point.  Highlighting the problematic phrases, we have:
[the path taken] [from a fixed point established by the certification
authority---the evaluated configuration at the end of CT&E---]to
[an equilibrium] [determined uniquely by the initial conditions]
[is related to] [observations in the case studies] such that [if the
path can be projected early in the ST&E process] it has predictive
value for [the final agreed-upon set of risks and risk mitigations
that will be acceptable to all accreditors and result in accreditation]
```

[without the necessity for inter-accreditor communication that violates security policy]. Simplifying, we have: 'the evaluated configuration together with an accurate assessment of each accreditor's tolerance for risk is sufficient to predict the accreditation decision'. I claim that the preceding statement is validated by observation and supported by well-tested economic theory with which it is proved to be congruent. At present, this is the argument I intend to make to the assessors next week.

Looking ahead to work planned for January, I reviewed the section on attractors in Gleick (1987) and the discussion of exploitation vs exploration games in Halpern (2003). It is not clear that anyone has ever studied this particular physical system before---other than the obvious application to vibration analysis of spring suspensions, although those are usually symmetrical in arrangement, whereas this is arbitrary and asymmetric. There are similarities in behaviour to split and double pendulums, magnetic or spherical pendulums, and Chua's circuit---the last supporting an assertion I made earlier that the accreditor model could just as easily have been implemented in terms of R-C oscillators. It was far from obvious when I began, but looking back now it can be seen that this research progressed in a fairly classical manner. From observations of CT&E and ST&E activity on R-prime, R-double-prime, and R-zero, certain patterns were identified. The patterns included long time to certification, back-and-forth negotiation between developer and certification authority, inter-accreditor non-communication in CDS accreditations, and possibly other patterns. A hypothesis was formulated that the years-long negotiation might be short-circuited---still to the satisfaction of all concerned---if the final configuration could be predicted in a way that was sufficiently transparent to all stakeholders. The immediately apparent question is how to falsify the hypothesis. I can think of two ways it could be done: firstly, to show that a non-optimal or intermediate configuration satisfies all participants. I would call that a win nevertheless. Secondly, to successfully predict the final outcome, but not to the satisfaction of all participants. That one is more problematic, as it points to a shortcoming in the methodology, but it might be overcome by provision of more detail. The model chosen for the hypothesis is that of risks and risk mitigations considered as massive objects in a space---at present the plane, but possibly of larger dimension---which are continuously pulled in different directions according to forces exerted by accreditors who are constrained by security policy from communicating directly. It informs the design of an experiment to test the hypothesis and yield a measurable value that can be compared to a standard. I am in the process now of building the apparatus to run those experiments on.

The RM developer remarked again today that NSA I173 continues to send questions, several times a week, about portions of the system covered by TORAs for remote management and WinDDS components, and in combination, indicating that NSA are clearly still working through the certification. The developer continues to engineer and test the 5.01 patch. I heard rumours today that within the CDS user community, Radiant Mercury is now the generic term for CDS. People say they want a Radiant Mercury, and then they say what kind (TMAN or ISSE). Boyd Fletcher, now at NSA, is said to have praised RM highly at a recent UCDMO, NSA, DODIIS and AFRL meeting. The developer had representatives at that meeting, something that would not normally have occurred, but they were there to present on my other research project. These meetings will continue in future although the RM developer will not likely be invited. I met with a senior engineer on the project 9th December 2010 to discuss the RM roadmap; he showed me the presentation he gave at the Programme Management Review this week. I suggested that he add notations to the roadmap indicating

minor and major recertification trigger points. The developer commented to me that it is difficult to tell the difference between government regression testing and certification testing these days. What, for example, are NSA doing right now? Apparently they are still testing, inferring from the questions that NSA send to the developer every week. UCDMO do not tell the developer anything about what is happening with CDTAB and TORAs; the developer can only induce from the emailed questions that NSA keep asking. My correspondent listed a few recertification triggers: port to a different OS, obviously, but in general the roadmap is all about bundling of enhancements. As long as enhancements are all relatively minor, with not all of them impacting the security critical portions of the system, then an update can be regression tested by the government and accepted fairly readily. If enhancements are all over the map, that is more likely to trigger a recertification event. The RM roadmap is designed with the preceding consideration in mind. Another thing I heard today was that Dan Nichols, Technical Director of UCDMO, told the developer that UCDMO is hands-off now. UCDMO helped the RM developer with all that 5.0 testing work, but not any more. It is IAD, not UCDMO that are continuing the government regression testing at the behest of CDTAB.

Other work this week: I had to do emergency repairs to the OUSS web site when it ran over quota, and Lockheed meetings took up time as well this week, though I used on-site opportunities to talk to various people in the developer organisation as well. My list of tasks is unchanged from last week as the only thing I am thinking about is getting through this viva.

My current task list (in priority order, most urgent first; work on tasks in this order):

1. Low-level simulation is almost working, readying for a demo to the assessors in less than a week.

2. Prepare an overview talk for viva: history, motivating examples, thesis, preliminary results, rejected alternatives, detailed plan for finishing, and contingency planning. (This is partly done.) See number 4 for another aspect of the problem that I want to completely thought out ahead of time.

3. Crosstalk article is now going to wait until after I present to the assessors. In the outline, I have that R-prime was evaluated under CC v3.0, but I recalled recently that there was an earlier version of the system (call it R_0) for the E project that was supposed to be ‘evaluatable’ under CCv2.3. R-double-prime was certified under DIACAP as the first test case to replace DCID 6/3, but it looks now like DoD and IC will be put together under the tent by UCDMO soon, as soon as they obtain full control of DSAWG. That is expected to occur in the first week of January. It affects the whole structure of the Crosstalk article, so best work on the implementation of the model until an announcement is made.

4. Thinking about what the definition of ‘succeed’ and ‘fail’ are in the context of CC evaluation; ‘did not complete validation’, ‘abandoned before the end of validation’, ‘failed to receive certification’, ‘abandoned before the end of evaluation’ and ‘not submitted for evaluation’ are all different and significant events.

5. Running five (not four as previously misstated) simulations in parallel confused the engine. I think I know what the problem was, but I

have three days to fix it. To do: implement Prof. Polak's
equilibrium acid test from Yale and the double alarm clock option
model (not as easy to do without the timed elements available in
Simscape, but should be possible with discrete Simulink elements;
have to model it as a discontinuity).

6. Background reading: Pennock and Wellman (2004) on uncertainty markets,
Levitt and Dubner (2009) on asymmetric information, Bernstein (1996)
on risk assessment (on hold), Karp (2009) on research methods, and
Achdou & Pironneua on option pricing.

7. Ping the following people: Paul Ozura [BAH], Dennis Bowden [San Diego],
[Patti Spicer, Charles Nightingale, Hal Forsberg] at CSC. Waiting to
hear back from Dr Kladko on the CC lab visit; I let him know when I
would be on travel.

8. Small tasks (get these done before viva!): update first case study
chart with changes from last conference; draw fault-tree diagrams
for R-prime, R-double-prime and S-star; draw up organisation charts
for R, R-prime, S-star, R-double-prime, N, L and G; update
documentation of the current set of anonymisation codes.

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford

End of WAR 0166.

References