File 20100910.1539: Weekly activity report 0153:

```
weekly activity report 153 (loughry)
Joe Loughry
Sent: 10 September 2010 15:39
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. 20100909.1203 (GMT+1) sequence no. 0153, week 8+12 TT

This has been an extremely busy week; Lockheed work took up more time
than could really afford to give it, but I made progress on several
fronts.  I am still blocked in some directions, but moving forward on
the main task.  I am feeling pressurised by deadlines and the upcoming
confirmation of status viva, but I also feel confident that my thesis
will work, if I can only convince more people that the idea is sound.

I met with Dr Martin on Friday.  After describing the inconsistent
politics visible throughout the RM 5.0 CT&E negotiations and despairing
of whether I will ever completely understand them, I reported on the
previous two weeks' telecon activity and progress during the time I
was in France.  In the telecon session I missed, the participants were
reportedly generally downbeat, in agreement that the October 1 date could
not possibly be met, to the dismay of the PMO.  The following week's
telecon, however, was much more hopeful, with participants seemingly
confident of bettering the 1st October date by a few days towards the
end of the month of September.  Perhaps the difference was that the NSA
pen test team were not on the second call.  The more I am attuned to
look for it, the more I can see instances where people from different
agencies do not talk to one another.  It is frustrating, like watching
a scene through darkness and smoke.

On the other hand, I am making great progress with the numerical model.
I am working on a vector representation of accreditor work unit offer
packages, to be used in operations with a matrix representation of the
global state.  Basic operations are working but the accreditor--accreditor
interaction piece is resisting solution.  I have nothing I can demonstrate
at the moment, because the only way to look inside the state of the
system is to inspect floating point numbers.  I want to instrument the
model to produce graphs, so that a person can see the result of applying
a perturbation to the system, measure how long it takes to settle down
into a new equilibrium, and observe the level of the new equilibrium.
The values are multidimensional, so I am unsure exactly how I am going to
show those in a line graph.  But I am working on it, and I expect to have
it in a form I can write about in another week or so.  The deadline for
the ACSAC conference is in about a week, and I want to submit a revised
paper there, or to IM 2011 at about the same time.

Which led into the primary topic I wanted to talk to Dr Martin about in
this week's meeting: confirmation of status.  I need to confirm during
Michaelmas term.  I have the following pieces of work I can talk about,
with items marked with * being immediately relevant to the confirmation
sub-task:

 - Literature survey *
 - Two case studies: $R^\prime$ (historical) and $R^{\prime\prime}$ (in
progress) *
 - Interviews with US and UK certifiers and accreditors
 - Model of inter-DAA communication *
```

- Tool development
- Validation
- Confirmation report *

We discussed how to proceed. The top-level goal is to persuade a pair of assessors that I have a complete plan for finishing the research and writing up in the space of another year, at most. Dr Martin described three schools of thought about how to approach confirmation. Some people, he said, are in a position to submit a mostly finished thesis. This can be a problem for assessors, because of the limited opportunity to improve what is already done or to alter the direction of work already done. The second way is to show a partially completed thesis, some chapters replaced by a page saying 'Chapter six goes here' with a list of things the chapter will be about. Perhaps the best way to approach confirmation is with a concise, five-page report describing where things are and where they are going, together with a plan describing how to get there, the whole thing backed up by a few published papers that will form substantial portions of chapters. The latter is the method I intend to use.

What I have is a story of a lot of things I have tried, a lot of blind alleys I went down, a lot of things that did not work and a few things that did. I am following the philosophy described in an article by DeMarco (IEEE Software, 2009), where he told of a project manager who instructed his team, 'I have a ship date in mind, but I'm not going to tell you what it is. Some day, I will come by and tell you it is time to deliver the software in a week. And you will be ready, because you have always been ready.' At every step along the way, I have tried to think of how I would defend this result, why I took certain decisions, what worked, what didn't, why I did x and not y. I am looking forward to this viva, because I think I could talk for hours about all the blind alleys I went down in search of one that wasn't. I finally have some pieces that fit together, and I am beginning to assemble the puzzle and see a picture emerge.

Dr Martin suggested a risk management approach to the five-page report, given that I am a little short of already-published results. I agreed; this gives me a framework on which to hang the contents. They are:

- A list of required components of the dissertation that are largely completed;
- List of remaining components (chapters) and their expected contents;
- A full list of tasks that need to be accomplished;
- Time and other resources needed by each task;
- Resource or scheduling conflicts anticipated;
- Potential risks and countermeasures assigned to each risk;
- Measurements I will use to track progress, expected results and allowed deviation bands;
- A list of fall-back positions with decision criteria for switching to each contingency plan;
- Check points to force progress back on track if it is discovered to be falling behind at any point.

Five pages is not a lot of room to work, but it is permissible to include a background narrative going into detail about all the approaches I tried that didn't work, if that additional material is relegated to an annexe.

Once I write the report, I expect it will take a while for assessors to be chosen, for them to read it, and for time to be scheduled later in the term for a viva. It is complicated somewhat by the fact that I have to travel. Dr Martin said that there is scope to update the report, a few days before the viva, with the latest information, especially if

it can be presented in a form with change bars.

We talked about the preliminary results I have now. I am stymied on the accreditor interviews approach. First it was Dr Ian Levy, now Dan Nichols---I speculated that perhaps the formal tone of my emails was putting them off somehow. I proposed switching to a more informal contact approach. Dr Martin cautioned the risk of burning relationships later if non-attributable information ends up published; I hadn't been thinking of that, myself worrying about the consistency and comparability of informal contact information, outside of the structured framework of a survey. We discussed the usability of data obtained from alternate methods, and ways of keeping it consistent with controls. I need to consult with Dr Jirotka.

I described the paper I presented in Europe as being less substantive than the following one will be. Dr Martin countered that what I presented last week was in fact substantive, just that it described my methodology rather than results. So I felt rather better about that after talking with my supervisor than I did before.

My plan for next two weeks is to finish the ACSAC paper and get it submitted, then write the five-page report and deliver it to Dr Martin by the 24th of September. Dr Martin laughed about my To-Do list at the end; here I have 14 tasks all listed under 'immediately'. Yes, it is getting longer. Some of those tasks are one-hour jobs---very easy ones---I just haven't got to them yet, because new tasks keep crowding onto the front of the list. I promised to get some of them done and knocked off the list soon.

I have a preliminary Table of Contents now with chapter headings that mirror the titles of papers I have either published, or are about to be submitted. I will discuss the TOC in next week's report.

There was no CT&E hotwash telecon planned this week; the participants are trying to figure out what to do next. All of the reports are finalised; they are waiting for the results of the 21st September 2010 pre-CDTAB meeting after which the next steps will be clearer. Instead of a meeting, I spent time reviewing the final versions of the NSA I173 CT&E report, I733 penetration testing report, DNI CAT report, regression testing report, ST&E report, POA&M Validation Report, and the final draft POA&M. In the ST&E report, there was one Cat I finding, unrelated to the CDS; two Cat II findings that are open; eight Cat II findings closed; and two Cat III findings that remain open, both representing site accreditation issues (800-53 controls) not directly related to the CDS. In the POA&M Validation Report issued by DIA, the Test Director recommended that RM 5.0 receive an 'ATO with POA&M.

I spoke with a person who has attended a pre-CDTAB meeting in the past. He described the general flow of the proceedings and at a high level the character of the participants. The overlap of CDTAB membership with the set of participants I have so far met is small; in general the more high-powered participants in the RM 5.0 CT&E effort will attend the pre-CDTAB meeting in a relatively low-status capacity. I need to find out who are the members of the CDTAB and DSAWG; I used to know the membership of the CDTAB when the Chairman was Paul Livingston, but he has retired now. It is possible that the people who were Livingston's techies at the time are now senior members of the board. The membership roster is likely to be FOUO controlled information; if I can get a list, it will have to be relegated to a non-published appendix.

With attendance at the the pre-CDTAB meeting on the 21st unlikely

to occur, this puts even more pressure on getting to talk to working accreditors in the US government to get a handle on their work practices and the needs of their task. I emailed Mr Paul Ozura this week for advice. He is presently working IV&V but used to be an accreditor; it was he who suggested Dan Nichols as a first point of contact. Rob Drake and Frank Sinkular are to be my next targets, and I need to figure out what went wrong with the last contact before risking a similar outcome with them. Mr Ozura is a busy person, but he has yielded volumes of information in the past when I have managed to get him at the right time. I have not received a reply yet but I will report results when I have them. While waiting, I have been reading books on the history and development of risk management (Bernstein, 1996) and its connection to the discovery of probability theory, which I need in my approach to quantify the market value of a risk mitigation work package. To further my own understanding of option trading, I read MacKay's 1856 book about the tulip craze in Holland in the seventeenth century, the French monetary collapse of 1720, and the South Seas bubble, all of which were directly caused by trading in options. Tobias (1970) provided some insight into the short-term stochastic behaviour of market prices as they are visible to individual investors. I needed this to tune the random number generator at the centre of the simulation to get it to produce accurate results. I am still playing with the formula I use to compute the 'velocity' of a risk vector. It just does not seem right for risk to be a dimensionless quantity, like a probability, because like a probability, risk is never an isolated number---a probability is the chance of occurrence of a particular event, just as a risk is the probability of a certain event together with the cost of that event, and the cost of mitigating the risk, and the cost of not mitigating it. Ivan Flchais' definition of risk is the closest to what I have found useful in this regard.

My ATAS application was successful; I received a certificate that I can use to submit a Tier 4 visa application. I want to get that in the post tomorrow, because my passport will be out of commission for a while during the time it takes for the Consulate to process it. The date when I can come back for confirmation of status is partly dependent on when I can get my passport returned.

I am participating in the Comlab DPhil Student Conference this year as a member of the committee and a reviewer. The organisers asked me to submit an abstract myself as well, so I said I would do that too. I will make the abstract connected in some way to the long-delayed Crosstalk article, to try to make some progress in that direction.

Finally, a friend today recommended that I should contact Dr David Pennock, Principal Research Scientist with Yahoo! Research. Dr Pennock's speciality is prediction markets, in particular one called Intrade. He was an early proponent of prediction markets for forecasting demand in the magnetic storage industry. I am looking at some of his papers and presentations now. I will contact him tomorrow.

My current task list (in priority order, most urgent first):

1. The deadlines for ACSAC submission and Comlab DPhil Student Conference are in one week; fix the numerical model; get a simple option mechanism based on the 1636 pattern working; implement 'acid test' in MATLAB.
2. First draft of confirmation report due to Dr Martin 24th September.
3. Waiting for a reply from Paul Ozura; still trying to get responses from US accreditors; shift contacts to informal mode. Deadline for this task (for travel) is early October.

```
4. Crosstalk article: immediately after writing confirmation report,
write the interpretation of the first case study in terms of
accreditor behaviour incentives.  Extend mnemonic anonymisation codes
and document them.  Write a preliminary overview of second case study
based on final reports from NSA I173 and I733, DNI CAT, ST&E, and the
POA&M Validation Report.
5. Get the other two planned surveys done for background on the case
studies.
6. Update first case study chart with audience suggestions from VALID
2010 conference.
7. Make fault-tree diagrams for $R^\prime$, $R^{\prime\prime}$ and
$S^\star$.
8. Draw up an organisation chart for $R$, $R^\prime$, $S^\star$,
$R^{\prime\prime}$, $N$, $L$ and $G$.

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

End of WAR 0153.

References