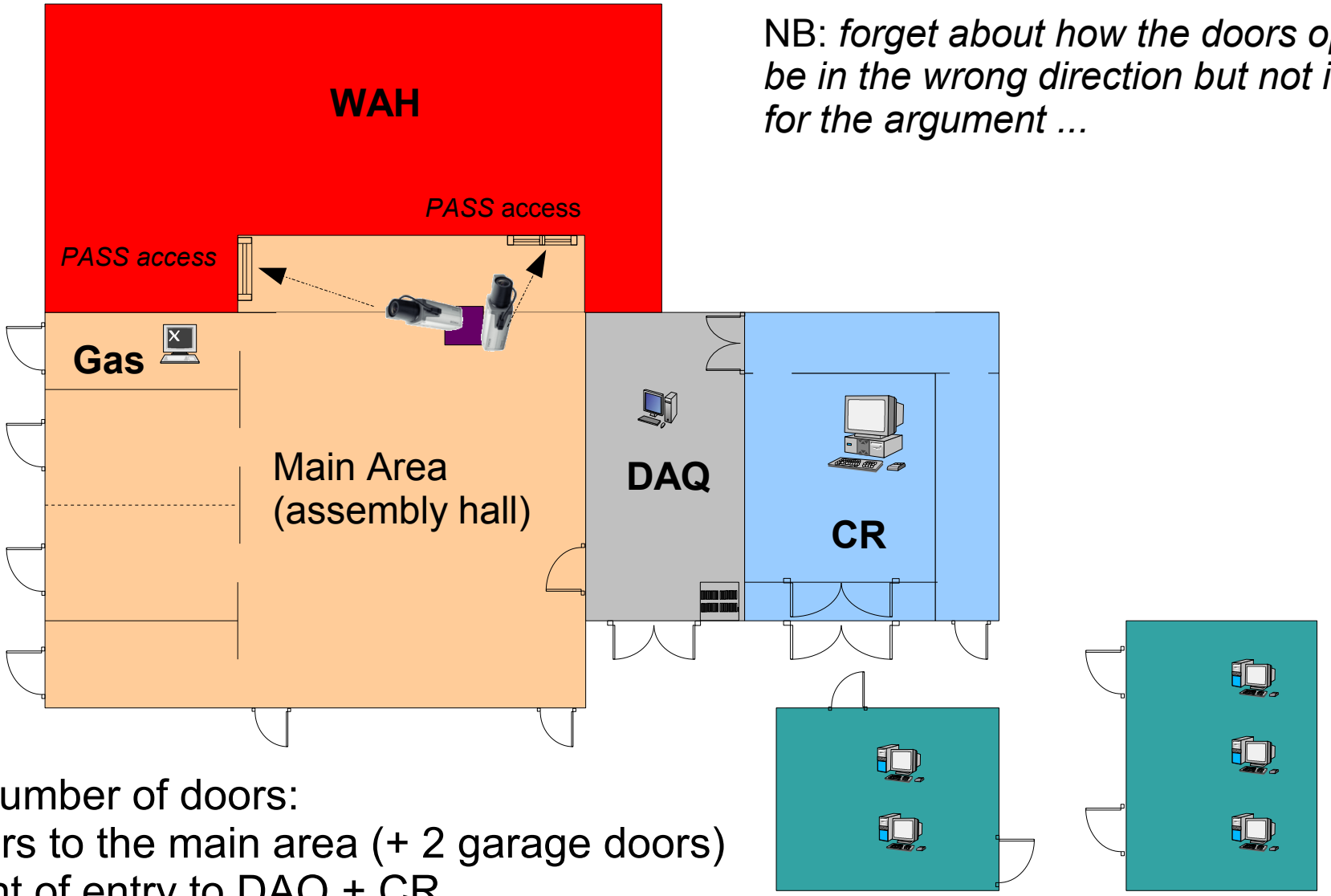
General layout of the building

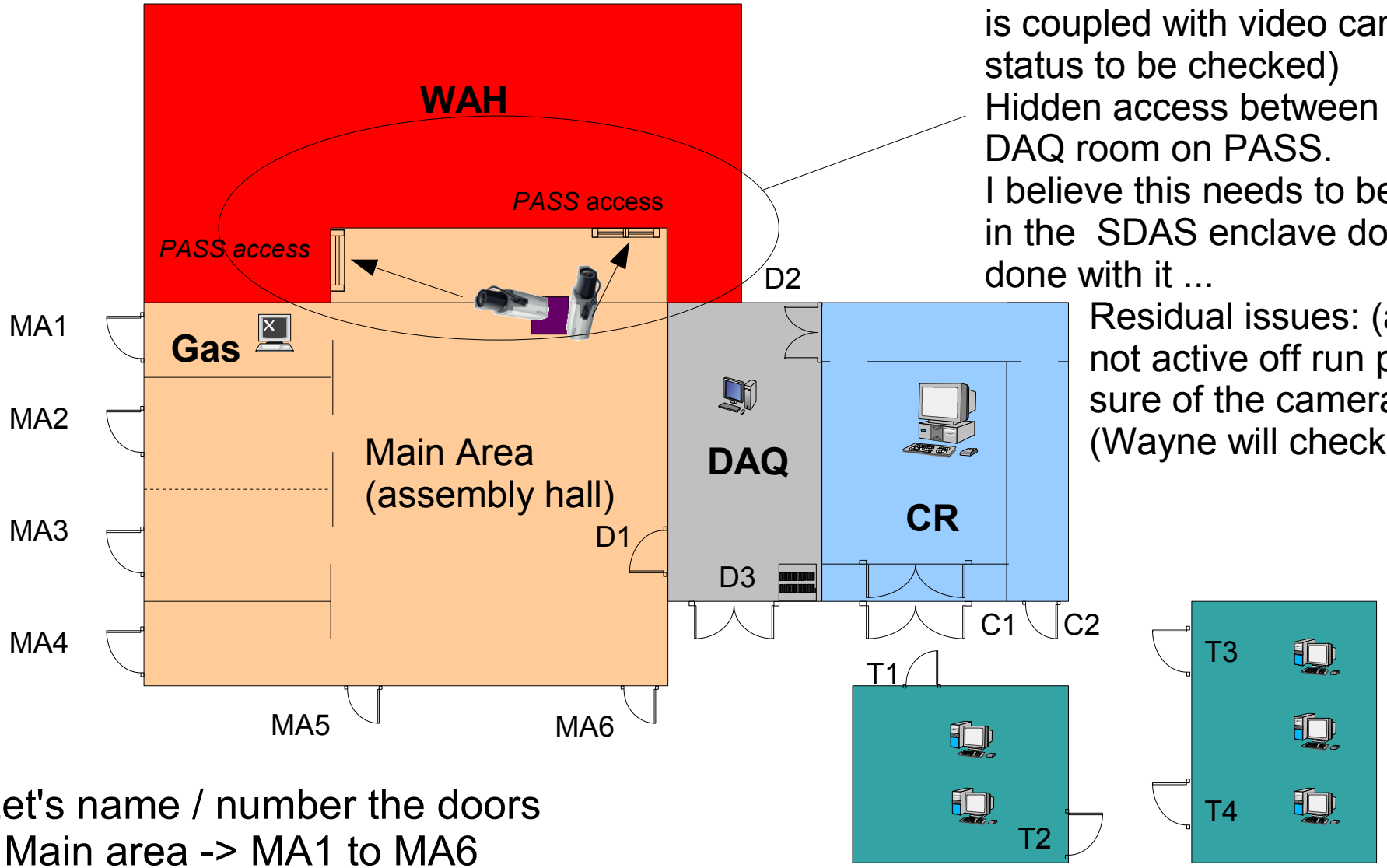


NB: *forget about how the doors open, may be in the wrong direction but not important for the argument ...*

Total number of doors:
- 6 doors to the main area (+ 2 garage doors)
- 4 point of entry to DAQ + CR
- 2 Entries to WAH
  - All under PASS
  - Two video surveillance cameras to PASS
- One hidden from WAH to DAQ (tunnel)
- 2 doors for each “trailer”

Jerome Lauret, 2007/01/12

General layout of the building



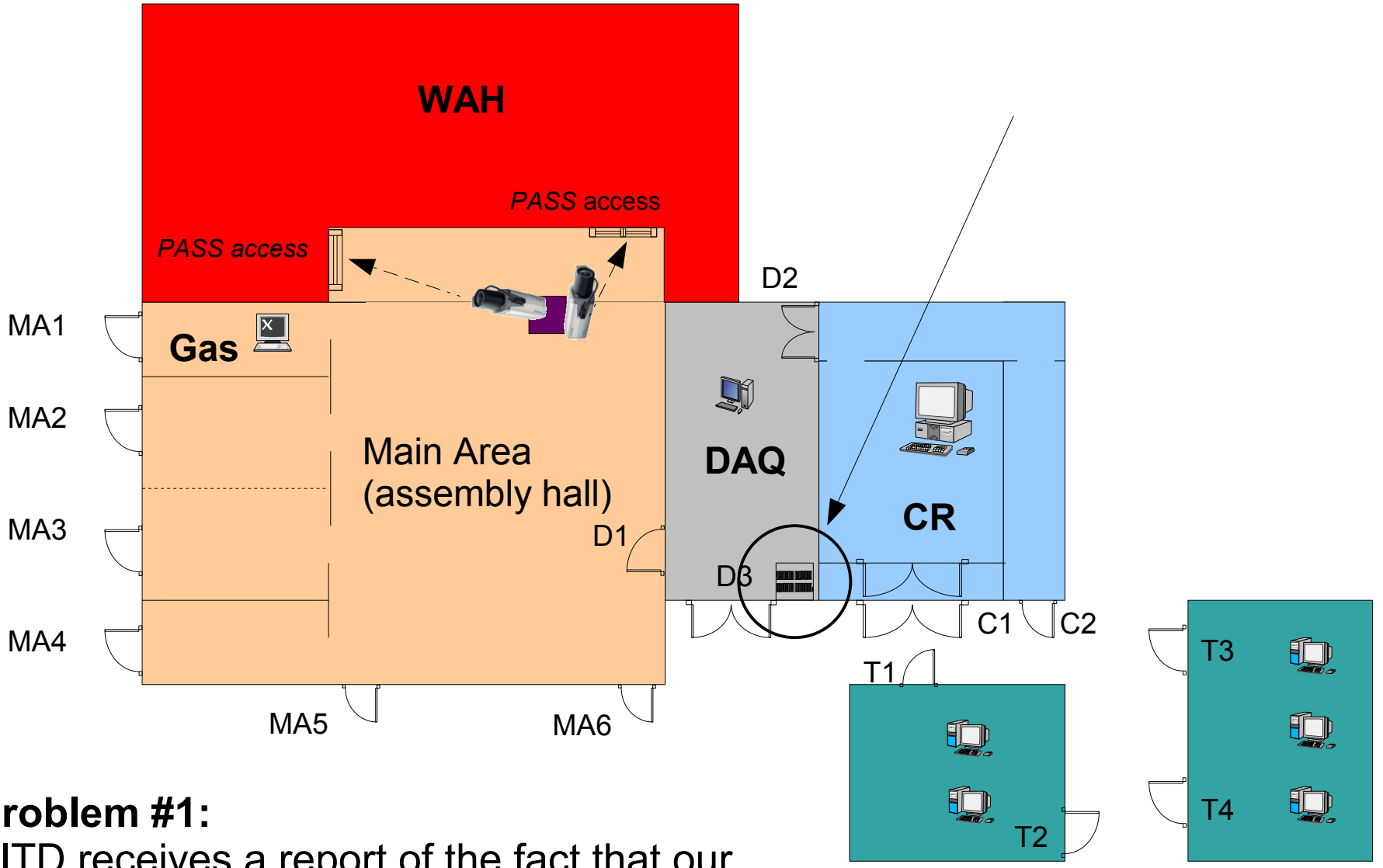
The entire PASS access system is coupled with video cameras (feed status to be checked)
Hidden access between WAH and DAQ room on PASS.
I believe this needs to be described in the SDAS enclave document and done with it ...

Residual issues: (a) PASS is not active off run period (b) not sure of the camera feed status (Wayne will check this)

Let's name / number the doors
- Main area -> MA1 to MA6
- DAQ Room: D1, D2, D3
- Control Room can be accessed via C1 or C2
- Trailers: T1 to T4

Jerome Lauret, 2007/01/12

Problem statement – A bit late for this one ...



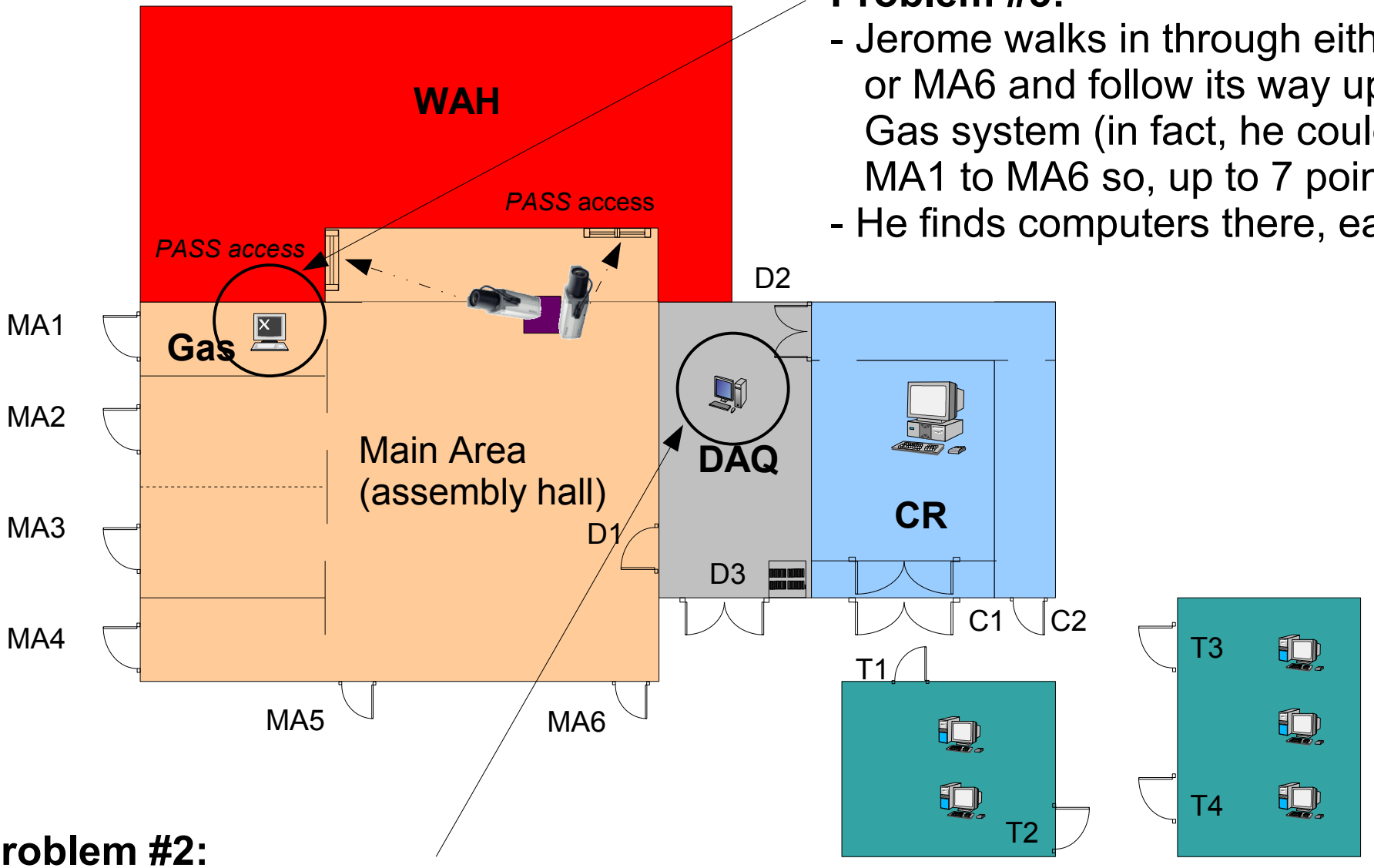
Problem #1:

- ITD receives a report of the fact that our network equipment is unsecured (circled and marked with an arrow)
- ITD literally walks through C1, pass D2 and access the equipment. Wayne (the only one online then) follows as he notices but after ITD pass D2 and reach the equipment
- ITD concludes (and report) easy physical access
- **<u>Consequence</u>: a cage is being built around the equipment**

Problem statement - Jerome put himself in a Cyber security reviewer shoes for 2/5 mnts ...

Problem #3:

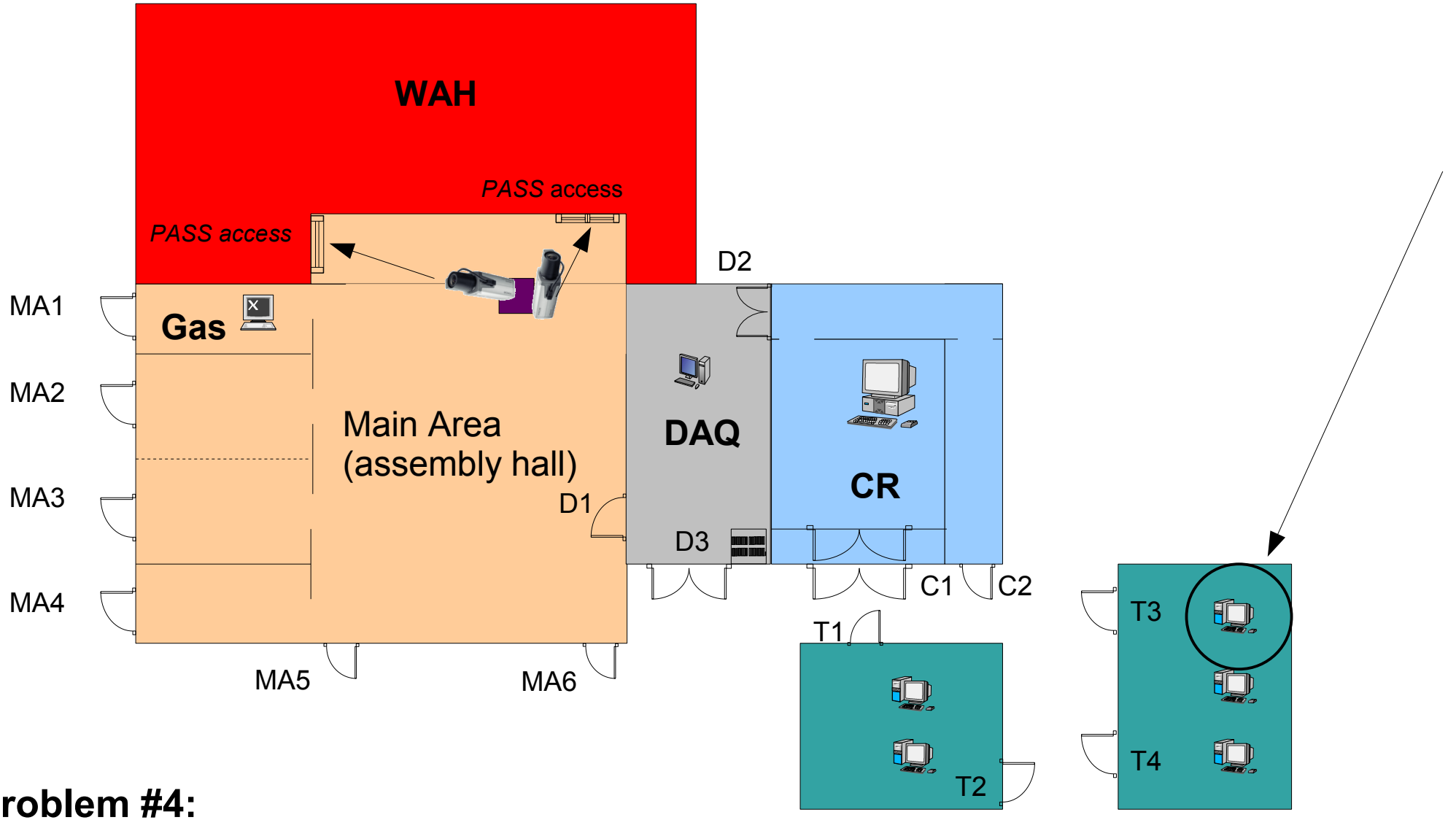
- Jerome walks in through either C1, D3 or MA6 and follow its way up to the Gas system (in fact, he could also use MA1 to MA6 so, up to 7 point of entry)
- He finds computers there, easy access



Problem #2:

- Jerome walks through C1, passes D2, reaches additional equipment in the DAQ room without encountering ANY Physical access barrage ... Depending on time of day, the entire area may be empty (so, a Red Team officer would be un-challenged)
- He reads things like “Warning: if powered down, magnet will crash”
- He accesses many network equipment of vital operational importance

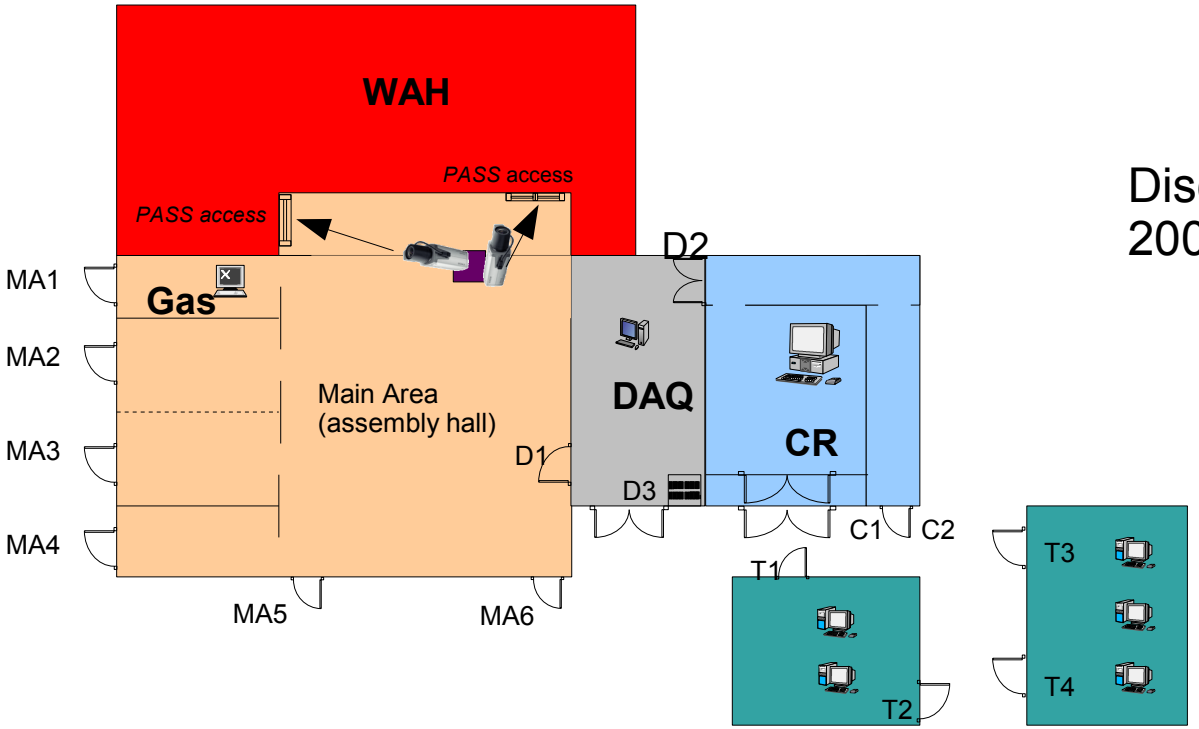
Problem statement - Jerome put himself in a Cyber security reviewer shoes for another 5 mnts ...



Problem #4:

- Jerome walks through T3, finds NO-ONE and access R.B. computer. The screen is unlocked, allowing access to all documents. Not the only one in this trailer.
- *Potential consequence*: we would basically immediately fail a review of our BNL CSPP

Proposed plan to address (too) easy Physical Access



Discussed with Bob Soja & Wayne Betts
2006/01/12

We propose (minimally)

- **Card sweeper based access control to D1, D3, C1 and C2 + Combination based locks on T1, T2, T3 and T4 + secure computing equipment (keyboard lock, unlock by experts only) in the main area + apply base line security in trailers**
- **Purpose:**

[a] would allow controlled access to both trailer and DAQ+CR, card sweep would "log" who accesses the rooms and when.

[b] Allow leaving the Gas computer without further Physical Security access. Depending on price, plan could add card sweep access to MA1 to MA6 (+6 doors)

[c] Escorted access to our desktop would show consistency with CSPP