Boiler code review for TRV1.5

DHD20160621 / DE20160621

All code and line numbers used in this review are taken from:
https://github.com/DamonHD/OpenTRV/tree/20160608-REV10-Secure-BHR-test
https://github.com/opentrv/OTRadioLink/tree/20160608-REV10-Secure-BHR-test
https://github.com/opentrv/OTAESGCM/tree/1.0.0-production-branch
This code was built with Arduino IDE 1.6.8 for the review.

Brief

Aim is to review (and externally document) semantics and code for:

1. Boiler control path (% open and call-for-heat flag) from REV7 to REV10 as boiler controller.
2. Semantics of boiler control algo, including with only some valves ‘smart’.
3. Failure mode analysis (including low-battery failure).
4. Semantics and handling of call-for-heat and % open, and any special meanings for (eg) frost protection and holiday mode and any ‘special’ threshold values.

Review is public.

Not-quite-Fagan! https://en.wikipedia.org/wiki/Fagan_inspection

Nothing about system operation should fail the current requirements (would be a major failure), and should ideally not prejudice the ‘eventually’ likely future requirements.

System Objectives

Current

1. Save carbon and money: don't heat where people aren't going to get any benefit.
2. Save carbon with minimal effort/thinking by the human who have better things to do with their mental effort.
3. Don't make the humans feel cold.
4. Anticipate the humans' return and *delight* them with a warm room.
5. Don't let pipes freeze and burst.
6. Don't encourage mould growth (eg via condensation in less-used rooms).
7. Don't short cycle the boiler.
8. Do run the boiler efficiently. Assuming combi gas boiler or similar in 1hr-thermal-response house for now, but maybe other sorts later.
9. Don't run the boiler into closed valves to avoid upsetting it.
10. Respond immediately to 'boost' to make users feel in control.
11. Play nicely in a system which is not all OpenTRV, eg not all OpenTRV valves, or other gadgets that need to share control of the boiler.
12. Have well defined radio, data, and other interfaces.
13. Prevent 3rd parties calling for heat + being able to see when someone is in the house from heat calls (this is basically AESGCM + extra random tx).

Future

14. Eventually support a 'holiday mode' boiler button (for frost protection only).
15. Eventually support 'ripple control' grid response.
16. Eventually support smartphone/Internet control.
17. Eventually Interop eg with OEM, OpenHAB, OpenTherm, etc.
18. Eventually control DHW and heat storage.
19. Eventually support better optimisations with cloud-based calcs, weather forecast input, and actual fuel-use tracking.

Boiler Hub Control Algorithm

Intended Semantics of Call-For-Heat Flag in ‘O’ Frame

Valve Percent Open Value

Normally an OpenTRV boiler control unit uses thresholds on ‘valve percent open’ values received from its associated OpenTRV valves to decide when to call for heat from the boiler.

This ‘valve percent open’ value is in the range 0 to 100, or 127 to indicate no such value is available (eg for a pure sensor that is not a valve, or where for example the valve has not yet calibrated and does not wish to indicate a definite position). (Any received value above 100 should for now be treated as ‘invalid’ and equivalent to 127.)

In particular:

- If all valves associated with a boiler controller are less than the DEFAULT_VALVE_PC_SAFER_OPEN threshold value (50%) then the boiler will be turned off. This threshold helps protect the boiler from running into nearly-closed valves since many may not be significantly open below this value.
- A valve reporting itself as open at or beyond the DEFAULT_VALVE_PC_MODERATELY_OPEN threshold (67%) is a strong call for heat that will usually be honoured, and quickly so.
- A valve at 100% (either because ‘boost’ has been requested or a room is well below target) is a very strong call for heat that will almost always be honoured, and quickly so.

The exact on/off thresholds may be adjusted dynamically within those limits or even above them to improve boiler efficiency, and to respond to (for example) smart-grid controller requests. For example, a boiler control may temporarily raise the ‘call’ threshold to 100% to attempt to conserve energy, or may not be able to call for heat from the boiler until the minimum off time has passed.

The most common reason for not responding immediately to values around the named thresholds is timing restrictions, eg minimum on and off times, to avoid boiler short-cycling.

The boiler unit can be in a mode where it defers calls for heat unless they are urgent/critical, in which case the boiler control unit may insist on:

- A much higher percentage open threshold.
- A longer time (eg an hour or more continuous).
- Multiple valves being above the open threshold.

Call-For-Heat Flag

There is a ‘call for heat’ boolean flag value in the ‘O’ message which indicates an urgent call for heat. This flag must default to false, eg a valve not using it explicitly must send false.

Example reasons for using the call-for-heat flag are:

- For frost protection when the valve or valve controller is noticing very low temperatures, eg below normal frost-protection temperature thresholds.
- To try to respond immediately when the user has selected ‘quick heat’, ie a boost.
- For valves whose actual working open range is much below the 50% to 67% implied by the normal named thresholds (though scaling the values may be better in many cases);

A boiler control unit is allowed to ignore the call for heat flag temporarily in order to avoid boiler short cycling or entirely if an open percentage in the range 1 to 99 is not provided at the same time.

A valve is permitted to always send a ‘false’ call for heat flag value, and may instead/also attempt to rely on opening fully to indicate a strong call for heat.

Note that a boiler unit that has a holiday mode (eg ignores 100% open for extended periods or indefinitely) MUST NOT ignore the call-for-heat flag and must respond within 15 to 30 minutes where there are other time restrictions (such as short-cycling) in place, and must not be used with valves that cannot send a true call-for-heat for frost protection.

As of 2016/06 no valve sends a true call-for-heat flag value, and no boiler control unit processes an incoming call-for-heat flag nor has a ‘holiday mode’ setting.

Documentation

remoteCallForHeat()

In V0p2_Main>control.cpp: line 1629

The aim of this code is:

- To avoid boiler short cycling.
- To deal with the fact that most (gas) combi-boilers can generate far more power than necessary for space heating (and usually operate more efficiently at high power).

What it does:

Minutes into cycle	**Aim**	**Action**
0-15	Avoid running boiler.	Set higher threshold.
16-31	Encourage running boiler.	Set lower threshold.
32-63	Encourage keeping the boiler on if it is already running (hysteresis).	Set a lower threshold if boiler is on. Set a higher threshold if boiler is off.

Step by step:

- Run a 64 minute cycle (0x3f = 63)

```
const uint8_t boilerCycleWindowMask = 0x3f;
const uint8_t boilerCycleWindow = (minuteCount & boilerCycleWindowMask);
```

- If in the first 15 minutes of a cycle, considerPause is set.

```
const bool considerPause = (boilerCycleWindow < (boilerCycleWindowMask >>
2));
```

- If between 15-31 minutes of a cycle, encourageOn is set if considerPause is not already set.

```
const bool encourageOn = !considerPause && (boilerCycleWindow <
(boilerCycleWindowMask >> 1));
```

- In the rest of the cycle, neither flag is set.
- Set the final threshold:
    - If considerPause is set, the threshold is set to the higher of minvro or `DEFAULT_VALVE_PC_MODERATELY_OPEN-1`(66)
    - Otherwise, if encourageOn is set or the boiler is on, the threshold is set to minvro.

```
const uint8_t threshold = (!considerPause && (encourageOn || isBoilerOn())) ?
minvro : OTV0P2BASE::fnmax(minvro, (uint8_t)
(OTRadValve::DEFAULT_VALVE_PC_MODERATELY_OPEN-1));
```

Results

V0p2_Main/messaging.cpp

- Line 401:

```
const uint8_t percentOpen = secBodyBuf[0];
if(percentOpen <= 100) { remoteCallForHeatRX(0, percentOpen); }
```

    - Hub does not process Call-For-Heat flag.

V0p2_Main/control.cpp

- Line: 1184
    - Valve cannot pass Call-For-Heat flag into secure frame generator.
- Line: 1629
    - Sets the threshold with reasonable values.
    - Not convinced by how well they work dynamically.
    - See remoteHeatCall() in documentation
- Line 1748: processCallsForHeat
    - Needs better documentation of _h and heardIt + truth checks.
    - Should refactor to make easier to follow.
    - Only supports FS20 protocol - no support for 8 byte valve IDs.

OTRadioLink/OTRadioLink_SecureableFrameType.cpp

- Line: 676: generateSecureOFrameRawForTX
    - Call-For-Heat flag not part of interface.
    - Should create overloaded function with relevant interface (additional Call-For-Heat flag); only caller is in a position to choose its value, it cannot be deduced at the OTRadioLink level.

Conclusion

The boiler control code paths from the valve to the boiler have been checked and are fit for purpose. The boiler is run if one or more valves are open beyond the DEFAULT_VALVE_PC_MODERATELY_OPEN threshold, and stopped if no valves are open beyond the DEFAULT_VALVE_PC_SAFER_OPEN threshold. Furthermore, short cycling of the boiler is avoided.

Appendix 1: Boiler Code Magic Numbers

From OTRadioLink, OTRadValve_AbstractRadValve (2016/06/20, master):

```
// Default minimum valve percentage open to be considered actually/significantly open; [1,99].
// Anything like this will usually be shut or very minimal flows.
// Setting this above 0 delays calling for heat from a central boiler until water is likely able to flow.
// (It may however be possible to scavenge some heat if a particular valve opens below this and the circulation pump is already running, for example.)
// DHD20130522: FHT8V + valve heads in use have not typically been open until around 6%; at least one opens at ~20%.
// DHD20151014: may need reduction to <5 for use in high-pressure systems.
// DHD20151030: with initial dead-reckoning direct drive impl valves may not be open until ~45%.
// Allowing valve to linger at just below this level without calling for heat when shutting
// may allow comfortable boiler pump overrun in older systems with no/poor bypass to avoid overheating.
static const uint8_t DEFAULT_VALVE_PC_MIN_REALLY_OPEN = 15;

// Safer value for valves to very likely be significantly open, in range [DEFAULT_VALVE_PC_MIN_REALLY_OPEN+1,DEFAULT_VALVE_PC_MODERATELY_OPEN-1].
// NOTE: below this value is likely to let a boiler switch off also,
// ie a value at/above this is a definite call for heat.
// so DO NOT CHANGE this value between boiler and valve code without good reason.
// DHD20151030: with initial dead-reckoning direct drive impl valves may not be open until ~45%.
static const uint8_t DEFAULT_VALVE_PC_SAFER_OPEN = 50;

// Default valve percentage at which significant heating power is being provided [DEFAULT_VALVE_PC_SAFER_OPEN+1,99].
// For many valves much of the time this may be effectively fully open,
// ie no change beyond this makes significant difference to heat delivery.
// NOTE: at/above this value is likely to force a boiler on also,
// so DO NOT CHANGE this value between boiler and valve code without good reason.
// Should be significantly higher than DEFAULT_MIN_VALVE_PC_REALLY_OPEN.
// DHD20151014: has been ~33% but ~66% more robust, eg for tricky all-in-one units.
static const uint8_t DEFAULT_VALVE_PC_MODERATELY_OPEN = 67;
```