INAUGURAL LECTURE

Safe and Secure Software Systems:
An Automated Reasoning Perspective

Professor Andrew Ireland

HERIOT WATT UNIVERSITY

H1: for_all (i__1: integer, ((i__1 >= ar_t__first) and (i__1 <= ar_t__last)) ->
    ((element(a, [i__1]) >= integer__first) and (element(a, [i__1]) <= integer__last))) .

H2: loop__1__i >= ar_t__first .

H3: loop__1__i <= ar_t__last .

H4: element(a, [loop__1__i]) >= 0 .

H5: element(a, [loop__1__i]) <= 100 .

H6: r >= integer__first .

H7: r <= integer__last .
    ->

C1: r + element(a, [loop__1__i]) >= integer__first .

C2: r + element(a, [loop__1__i]) <= integer__last .

C3: loop__1__i >= ar_t__first .

C4: loop__1__i <= ar_t__last .

subtype AR_T is Integer
type A_T is array (AR_T
...
procedure Filter(A: in A
is
    begin
        R:=0;
        for I in AR_T loop
        --# assert R >= 0
            if A(I)>=0 and A(
                R:=R+A(I);
            end if;
        end loop;
end Filter;
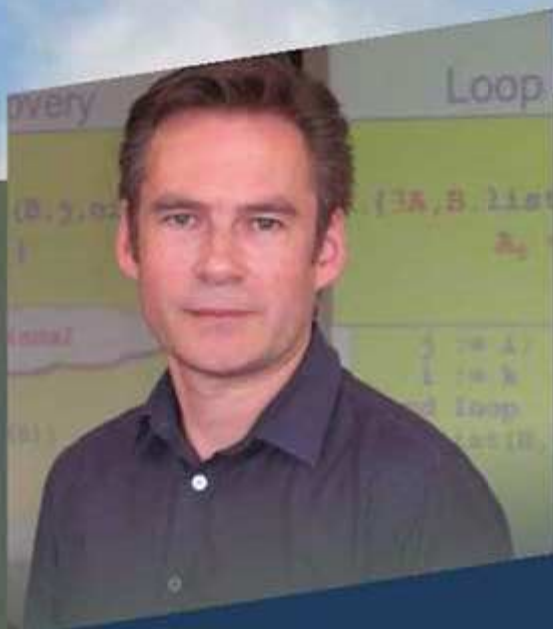
Wednesday 14 November 2012
Postgraduate Centre - Cairn Lecture Theatre
Start: 5:00pm (pre-talk refreshments 4.30pm)
Finish: 6:00pm, followed by a wine reception
RSVP: HWU-Lectures@hw.ac.uk

Distinctly Ambitious
www.hw.ac.uk