EMV2 Approach

```
pedal_out : out
propagation{NoService
};
```

```
pedal : in propagation
{NoService};
cmd : out
propagation{NoValue};
```

```
in_pressure : in
propagation {Novalue};
out_pressure : out
propagation{NoValue};
```

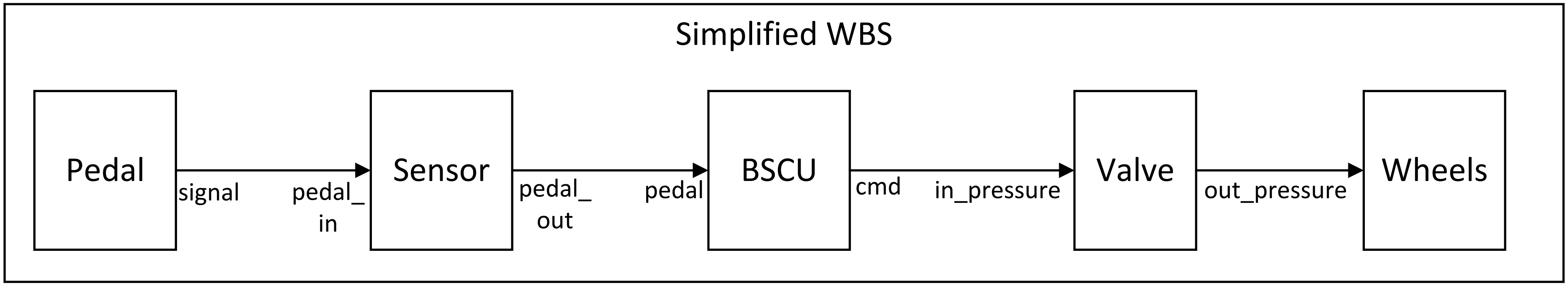
Component's Error Propagation

```
error source
signal{NoService};
```

```
error path
pedal{NoService}
-> cmd{NoValue};
```

```
error path
in_pressure{NoValue} -
>
out_pressure{NoValue};
```

Component's Error Flow



```
signal.val
>= 0.0;
```

```
pedal_out.val =
pedal_in.val;
```

```
(pedal.val >
0.0) =>
(cmd.val > 0.0)
```

```
out_pressure.val
=
in_pressure.val;
```

Component's Nominal Behavior in AGREE

```
"sensor output stuck at zero"
    pedal_out = if
    fault_trigger then
    0.0 else pedal_in;
```

Component's Faulty Behavior in Safety Annex

```
"pedal pressed implies valve pressure"
  (Pedal.signal.val > 0.0)
  => (Valve.out_pressure.val
  > 0.0)
```

System's property in AGREE

Safety Annex Approach