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};
```

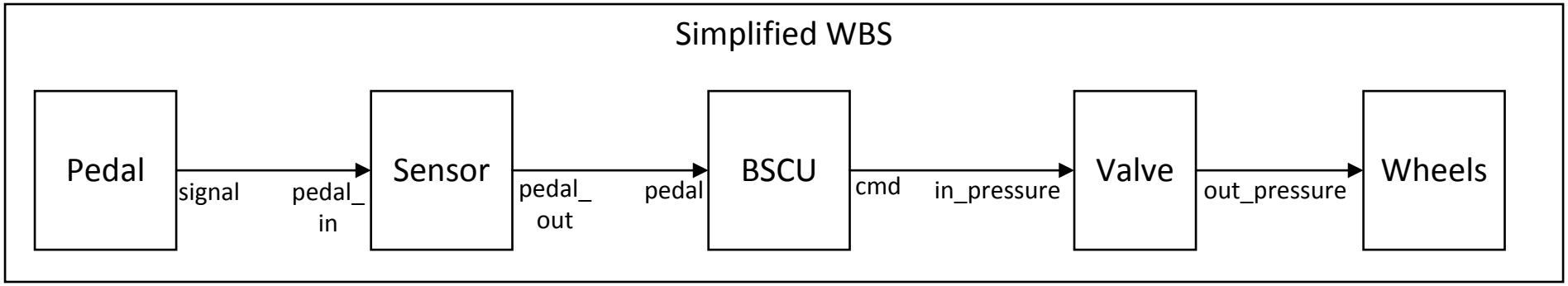
Component's Error Propagation

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

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

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

Component's Error Flow




```
guarantee
"signal
output
range is
>= 0.0"
```

```
guarantee
"passing
input to
output"
```

```
guarantee "pedal
pressed (> 0.0)
implies pressure
commanded (cmd  >
0.0)"
```

```
guarantee
"out_pressure is
equal to
in_pressure"
```

Component's Nominal Behavior in AGREE

```
fault stuck_at_zero
"pedal_out.val stuck
at zero"
```

Component's Faulty Behavior in Safety Annex

```
guarantee "pedal pressed (pedal signal
> 0.0) implies valve out pressure
(out_pressure > 0.0)"
```

System's property in AGREE

Safety Annex Approach