# Automated Distribution System

## 1 General Description

We consider an automated distribution system that consists of a circuit breaker ($CB$) and four load points ($LP$). Figure 1 shows the distribution system.

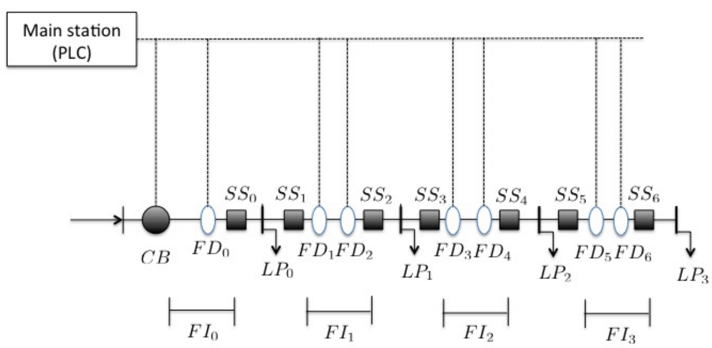


Figure 1: Automated Distribution System

We assume that each load point is equipped with two section switches ($SS$) and a fault detector exists besides each section switch. When a fault occurs on the line between two load points, the fault is detected by the fault detectors and the main station is updated about the occurrence. Then, the main station enables the circuit breaker and the circuit breaker de-energizes the whole distribution line.

Based on where the fault occurred, the main station enables the section switches on the faulted line in order to isolate the specific section of the distribution line. Then, the main station closes (disables) the circuit breaker and energizes the load points prior to the faulted line. When the fault is fixed, the enabled section switches are disabled and the whole distribution line is re-energized.

## 2 Fault case

The following case describes the above described operation when a fault occurs on the line between $LP_1$ and $LP_2$.

- Step 1: A fault occurs on the line between $LP_1$ and $LP_2$ ($FI_2$).
- Step 2: The main station enables the circuit breaker and the distribution line is de-energized.
- Step 3: Fault detectors at $LP_1$ and $LP_2$, $FD_3$ and $FD_4$ respectively, report the location of the fault to the main station ($FI2$), the main station enables the section switches $SS_3$ and $SS_4$, and the line between $LP_1$ and $LP_2$ is isolated.
- Step 4: The main station closes the circuit breaker and energizes $LP_1$ and $LP_2$.
- Step 5: Once the fault is repaired, section switches $SS_3$ and $SS_4$ are disabled and all the four load points are energized.

## 3 Algorithm

The following algorithm describes the operation of the system.

```
I = # of load points
SS_i = 0 for i = {0, ..., 2I − 1}
FD_j = 0 for j = {0, ..., 2I − 1}
FI_k = 0 for k = {0, ..., I − 1}
if CB = 1 then
    count_faults ← 0
    for j = 0 : 2 : 2I − 2 do
        k ← 0
        if j > 0 then
            if (FD_{j−1} = 1 and FD_j = 1) then
                k ← j/2
                FI_k ← 1                                  ▷ Locate the fault
                SS_{j−1} ← 1                              ▷ Isolate the faulted section
                SS_j ← 1
                count_faults ← count_faults + 1
            end if
        else
            if FD_0 = 1 then
                FI_0 ← 1
                SS_0 ← 1
                count_faults ← count_faults + 1
            end if
        end if
```

**end for**
$CB \leftarrow 0$ ▷ Close the circuit breaker
**for** $j = 0 : 2 : 2I - 2$ **do**
$k \leftarrow 0$
**if** $j > 0$ **then**
$k \leftarrow j/2$
**if** $FI_k = 0$ **then** ▷ When the fault is repaired
$SS_{j-1} \leftarrow 0$ ▷ Re-energize the previous faulted section
$SS_j \leftarrow 0$
**end if**
**end if**
**end for**
**end if**

# 4 Normal Operation

On the implementation using the Ladder logic, we assume that when all of the switches (fault detectors) are off, there is no fault on the distribution line and all the section switches are off. A combination of switches with value on, can cause a fault. When a fault occurs, a fault indicator (LED) is enabled at the output of the PLC. We can assume that each fault indicator energizes a pair of section switches in order to isolate the faulted section on the distribution line. This part is no physically implemented. After a fault is detected and located, and the faulted section is isolated, the circuit breaker is closed and the distribution line is re-energized up to the point where the fault occurred. In order to open/close the circuit breaker, we assign one input switch at the circuit breaker in order to control it. We also assume that a fault is repaired when the status of the fault detectors that correspond to the faulted section is off and thus the fault indicator at the output of the PLC is de-energized.

The mapping to the PLC registers is as follows:

- Input I0.0: Circuit Breaker
- Input I0.1: Fault Detector 0 ($FD_0$)
- Input I0.2: Fault Detector 1 ($FD_1$)
- Input I0.3: Fault Detector 2 ($FD_2$)
- Input I0.4: Fault Detector 3 ($FD_3$)
- Input I0.5: Fault Detector 4 ($FD_4$)
- Input I0.6: Fault Detector 5 ($FD_5$)
- Input I0.7: Fault Detector 6 ($FD_6$)
- Output Q0.0: Circuit Breaker LED

- Output Q0.1: Fault Indicator 0 ($FI_0$)
- Output Q0.2: Fault Indicator 1 ($FI_1$)
- Output Q0.3: Fault Indicator 2 ($FI_2$)
- Output Q0.4: Fault Indicator 3 ($FI_3$)

# 5 Possible Attacks

- Attack 1: Change the status of the circuit breaker LED

  When a fault occurs and the circuit breaker is enabled try to de-energize the output Q0.0 in order to indicate that the circuit breaker is disabled and there is power on the distribution line.

- Attack 2: Change the status of a fault detector

  When the is no fault detected, change the status of a fault detector (input switches) in order to indicate that a fault occurred.

- Attack 3: Change the status of the fault indicator LED

  When a fault occur, change the status of the corresponding fault indicator LED at the output in order to hide the location of the fault.