# PACS Controller Attacks

# PACS Relays

## Method One – Relay Bridging

There are **two locking mechanisms** for this PACS system – it's wired in a very non standard way because I wanted pretty LEDs.

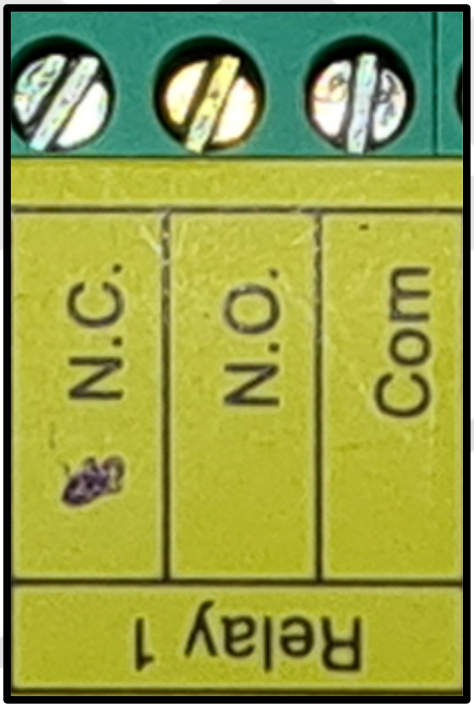
A successful card tap will trigger the relay, which can be wired to work through **normally open (NO) or normally closed (NC).**

**Normally open** means the circuit is **not completed** unless the relay is triggered. Thus the light will be off unless an authorised card is presented. This might be an **electrified strike.**

**Normally closed** means the **circuit is normally completed** and is disconnected when the relay is triggered. The light is on unless an authorised card is presented. This might be a **mag lock.**

Thus controller attacks can mean bridging a relay to complete a circuit or can mean you have to disconnect a circuit.

**This controller is wired as if there are both mag locks and electrified strikes.**




Try bridging these and see what happens.

# PACS Controller Attacks

# PACS Exit

## Method Two – Exit Button

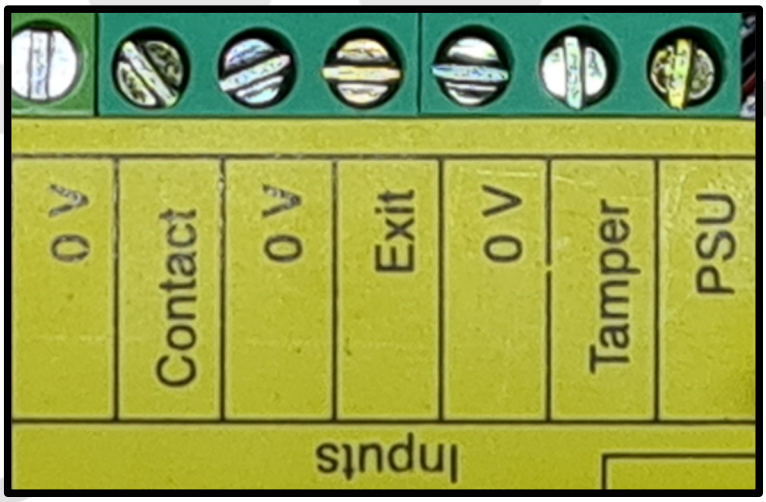
Here we can see the **door release** (“Push to Exit”) button is connected. This being said, **why is it connected where we have a single door with two readers**?

If it were not connected, we could ask **“has this button been properly disabled”** or has it just been left there? In this setting, we can ask if this is just legacy wiring that has been disconnected elsewhere and replaced with a reader.

**Bridging** these two connections will make the controller think the **door release has been triggered**. It will open the door unless it has been disabled in software. Conveniently, it’ll **trigger the relay and the timer**, opening it for a few seconds, giving us time to wedge it open whilst we put things back together.

The downside is the **system logs** will show this button was pressed. Whilst **alarms** integrated into the PACS system **will likely not sound** as the system is supposedly allowing **legitimate egress** from the secure area.

We can look at whether a separate alarm system is connected to the PACS controller, but this doesn’t tell us what integrations or alerts may be happening on the software side.




Bridge the exit connector to 0V and see what happens.