Artifact template

A09 – SCADA

ID	A09 – SCADA
Category	Traffic analysis
Difficulty	Easy
Description (This text could be shared with the participants if necessary)	
Additional material	Traffic capture
Technical requirements/ others	None
Preparation	
Resolution	Participants will be tasked with investigating why some wind turbines have stopped working. At the moment, the only clue available is a traffic capture from Schneider Electrics SR3 B261BD SCADA systems. Analyzing the file, it can be easily observed that the system's usual behavior consists of the exchange of 04: Input Registers (FC=04) messages, which read the values of certain registers. At a given moment, it is observed that a multitude of consecutive messages of type 05: Single Coil (FC=05) are sent, with the aim of opening or closing a valve.