**Cyber-Physical Stress-Testing Platform for Water Distribution Networks**

*Author: Dionysios Nikolopoulos; Georgios Moraitis et. al*

[note: This paper is mentioned in DHALSIM paper. It is known as RISKNOUGHTl. This is quite comprehensive paper]

**Tell the problem or define the problem**

It solves the same problem as DHALSIM, simulates a complete cyber physical system for water distribution network so that cyber attacks can be simulated and tested.

**Why is the problem important?**

Same as DHALSIM

**contribution of the paper**

It shows exploitation of zero day vulnerability on attack scenario 2. It also shows DoS attack with insider knowledge in attack scenario 4 and 5.

**What approaches are followed**

This is actually very comprehensive paper. It is similar to DHALSIM. For physical layer emulation it uses WNTR and for cyber layer it uses NetworkX python package. It presents an architecture similar to DHALSIM and uses C-Town water network for the physical part. The paper shows how cyber attack can cause wrong readings of supply demand on SCADA server.

The paper presents 5 attack scenarios:

1. Attack Scenario 1: Manipulation of Sensors
2. Attack 2: Exploitation of Actuators
3. Attack 3: SCADA DoS Attack
4. Attack 4: SCADA DoS Attack with Insider Knowledge
5. Attack 5: SCADA DoS Attack with Insider Knowledge on a Semidistributed System

**What is missing or shortcomings**

1. This does not discuss industrial network protocol, only mention master-slave type protocol.
2. Code is not available. Even though it mentions code can be available for authors, it looks like now it has now evolved to become a commercial product.