



# Bowman Avenue Dam



**Discovered:** DHS told city c. Sep 2013

**Sector:** Water: flood-control dam

**Systems Reached:** SCADA system

**Scale:** Bowman Avenue Dam,  
Rye Brook, New York

**Initial Access Vector:**  
Cellular modem, per a DHS summary  
as reported by the WSJ

**Attacker:** Hamid Firoozi, ITSec Team  
(indicted). Charged, not convicted

**Root Cause:** Undisclosed

**Malware:** Undisclosed

**Operational Impact:** None on  
the record. Sluice gate “manually  
disconnected for maintenance” (DOJ)

**Financial Impact:** Remediation over  
\$30,000 (DOJ). Total cost **undisclosed**

**Process Impact:** **None.** Read water  
level, temperature and gate status.  
DOJ: access “would normally have  
permitted” gate operation. No  
command on the record.

**Cross Reference:** Oldsmar · US Water  
Campaign · American Water

**In 2013 an intruder spent three weeks inside the control system of a small New York flood-control dam, reading water levels and the gate’s status. He could not move the gate. A maintenance crew had unhooked it.**

Every account of Bowman Avenue turns on one Justice Department sentence: the access would normally have let the intruder operate the sluice gate, and it did not, because the gate had been manually disconnected for maintenance. The thing between a remote session and a physical gate was not a control anyone designed. It was a work order. The crew did its job. This is not an argument about competence.

It is about which state the site was in. The rung above was closed for a temporary reason: a gate under maintenance goes back into service, and the city says this one first ran in spring 2014. What changed before then is on no record. This is BlastWave’s analysis, not a disclosed fact: the save was a state, not a design. A physical disconnect is the most honest control in OT, because it does not know who is asking. Build it in on purpose, with an alarm when it changes.

**What is not known:** How he got in is not on any record we could read. The cellular modem comes from a Homeland Security summary as reported in 2015, and the search engine discovery from people close to the investigation. Nobody has said who found the intrusion or whether any command was sent. The city that owns the dam described a standalone PC, not yet functional, logging levels; the Justice Department says the access would normally have permitted gate operation. The city says the gate first ran in spring 2014; what changed before then is undisclosed.

## Recommendation

### 1. Take the path away

No gate controller or supervisory PC at a remote water asset answers from the public internet or a carrier network. Find the modems first.

### 2. Remove standing remote command

Moving a gate takes a named, verified person in a scheduled window. Local becomes the default on purpose, and the operator station alarms whenever it changes.

### 3. Make read-only consumers read one way

Water level, temperature and gate position reach the office over a path that cannot write back, so seeing the dam never requires a door into it.



**The Car on the Lift**  
**Embedded** audio/file-013.m4a



**Bowman Avenue Short**  
External Link – Opens in Browser

**Sources:** DOJ release 16-348 and SDNY release, 24 Mar 2016 • FBI wanted notice, Hamid Firoozi • City of Rye statement, Dec 2015 • WSJ, 20 Dec 2015 (via The Register) • Newsweek, 30 Mar 2016. No advisory issued.

**Soft Spots:** The cellular modem is reporting of a DHS summary we have not read, and the indictment was not read as text. That a maintenance state, not a design, was the save is BlastWave’s analysis; what changed before the gate first ran is unknown.