Breach Workshop
Waterplant

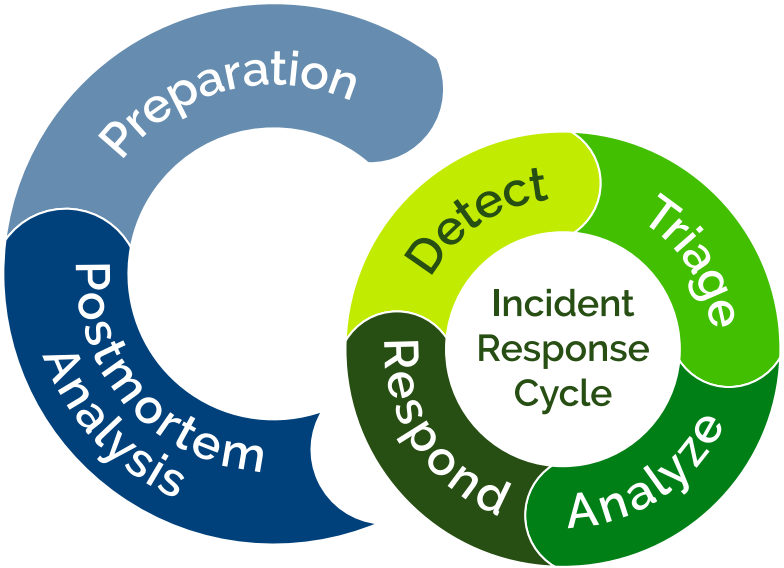
Nadi, Fiji
Serge Droz
2020

FIRST

Copyright

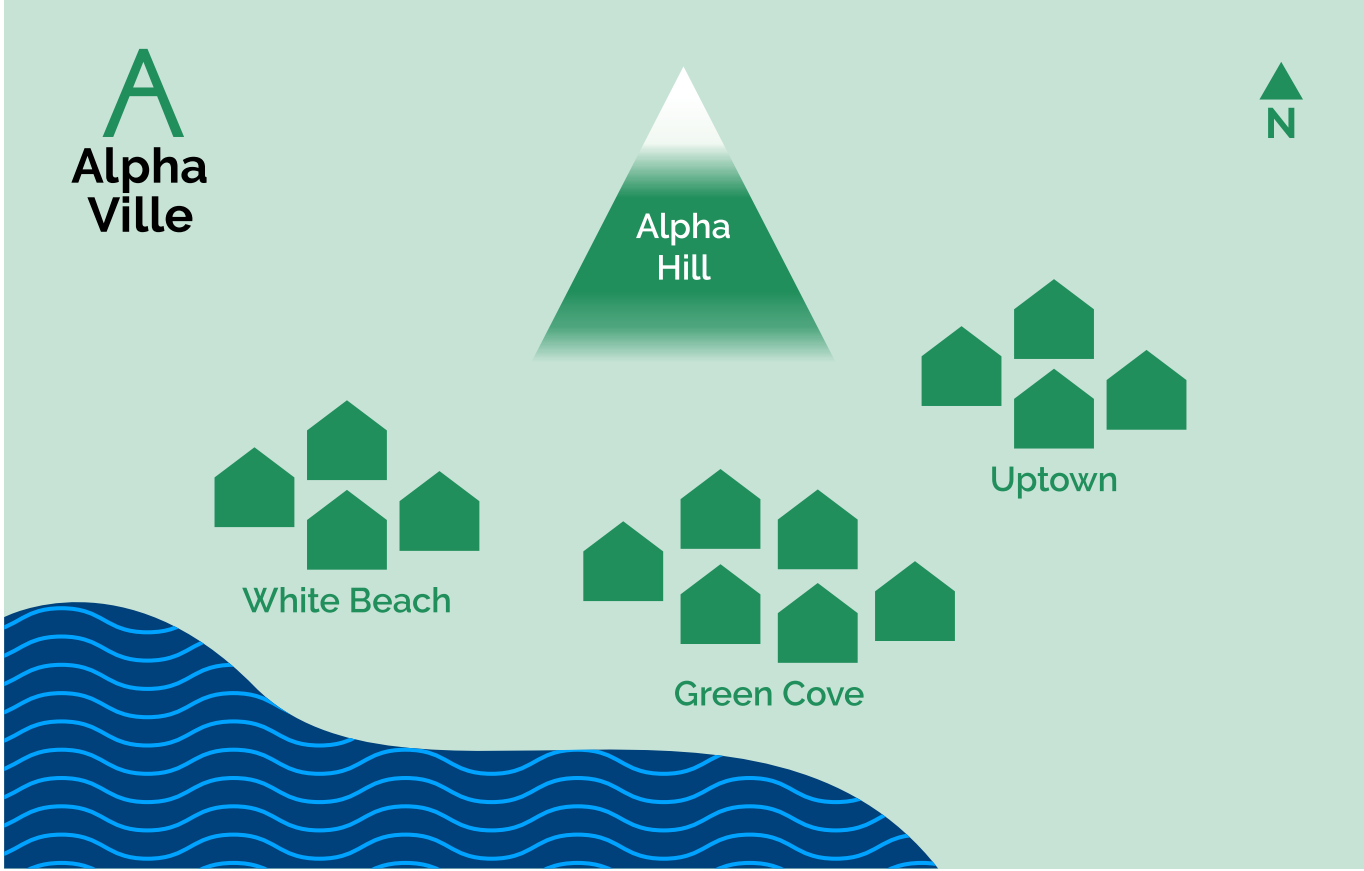
Before we start let's have a look at the...

Incident Management



Welcome to Alpha Ville

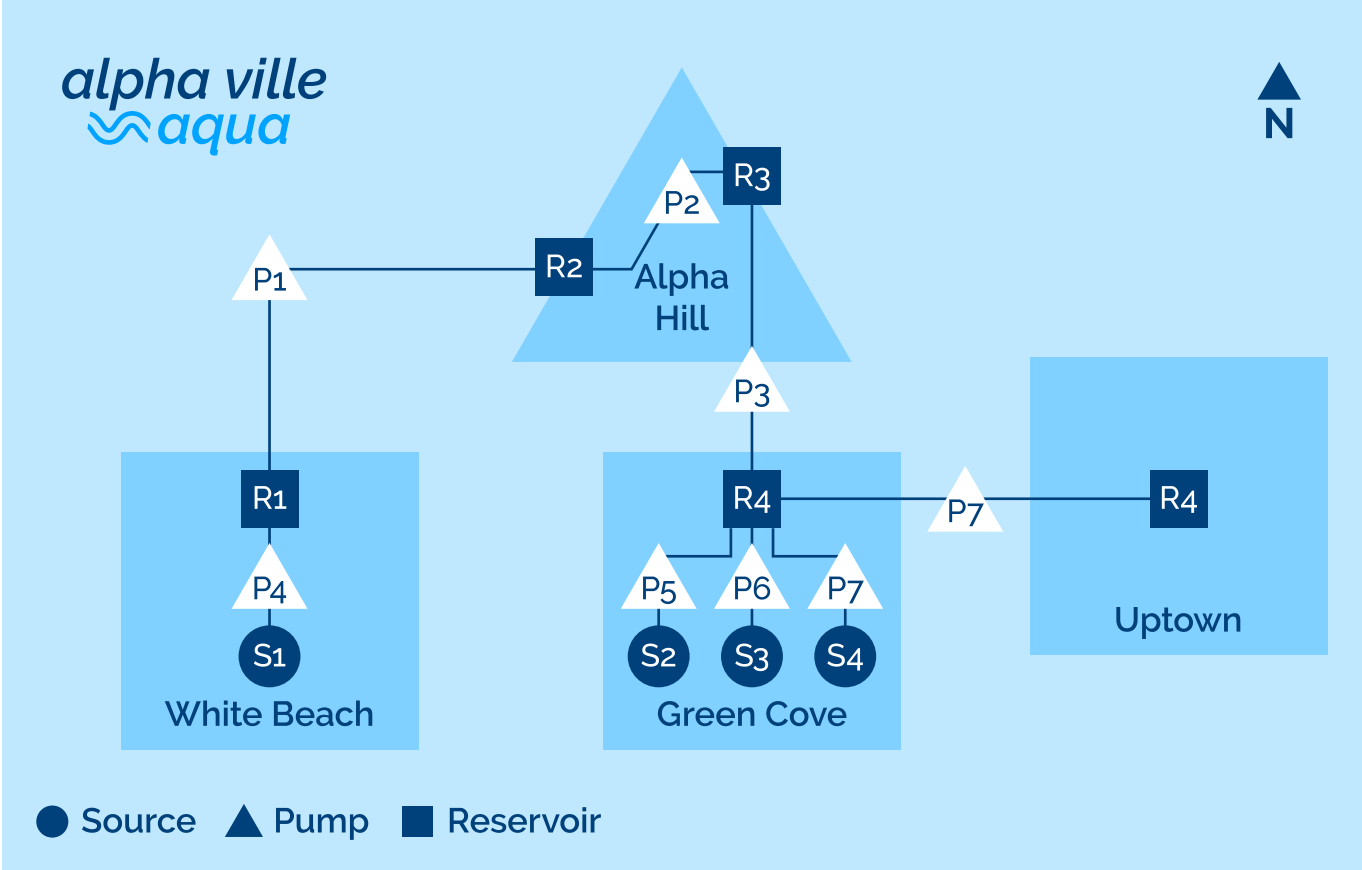
We are in a water plant in a midsize municipality. There are no other sources of clean water available nearby, but the plant produces more than enough supply.



Workshop Progress

The plant gets power from the public grid and operates a hand full of reservoirs. Two are higher up an can supply water without pumps for at most 1 ½ days to the lower areas.

This is a well developed place with functioning authorities. The city has three neighbourhoods that each have their own water reservoir.



Workshop Progress

Introducing the involved organisations

Alpha Ville

The municipal service is the owner of Alpha Ville Aqua and the Cyber Center

alpha ville aqua

Alpha Ville Aqua is an organisation unit of the City of Alpha Ville

Cyber Center

The Cyber Center is an organisation unit of the City of Alpha Ville

ALPHA VOICE

Alpha Voice is a local and independent media enterprise, its main channels are radio and a web journal

Introducing the players

alpha ville aqua

Board: Oversees the organisation and does not usually participate in operational duties.

Executive board: CEO, CIO, CFO*, COO.

IT, two units: Office IT and Production IT report to the COO.

Machine Team: Responsible for infrastructure, Pumps, valves etc.

A 7x24 **duty officer**.

Laboratories: A couple of chemists ensuring water quality*

*Not needed at this time

Preparation

alpha ville aqua

The C* should define their teams, there is a max of 9 people to use for all management teams, including the lead engineers of the other units.

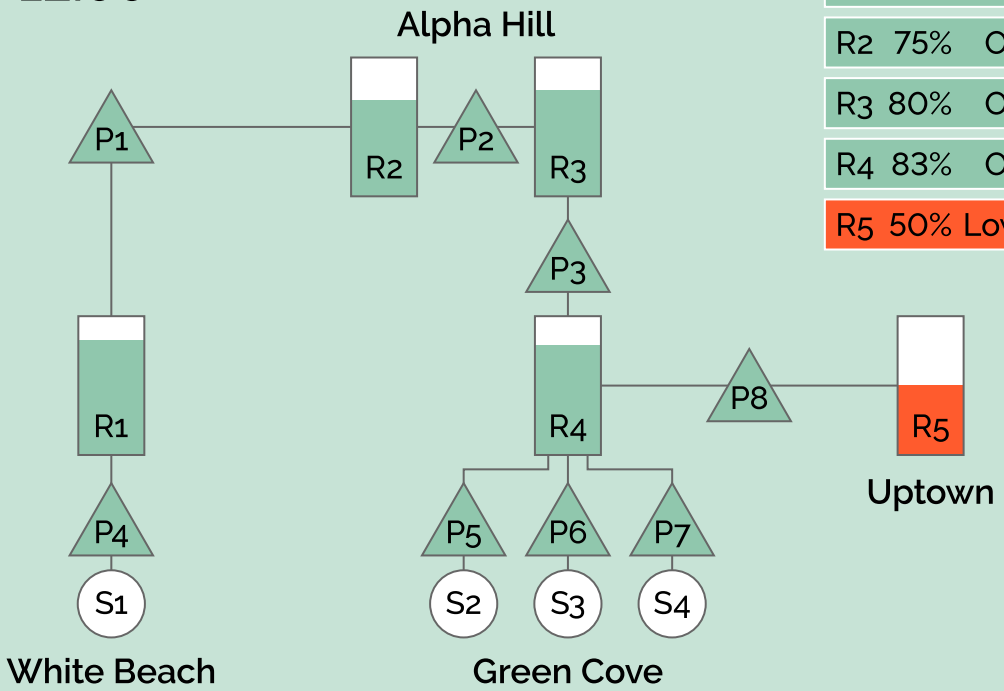
Negotiate who gets how many people and functions.

What is a typical day?

An ordinary day in Alpha Ville, the sun is shining...

It's a Friday during an ongoing hot period. Forecast sees no cooling in sight. Water consumption is up because of the heat.

Friday 12:00



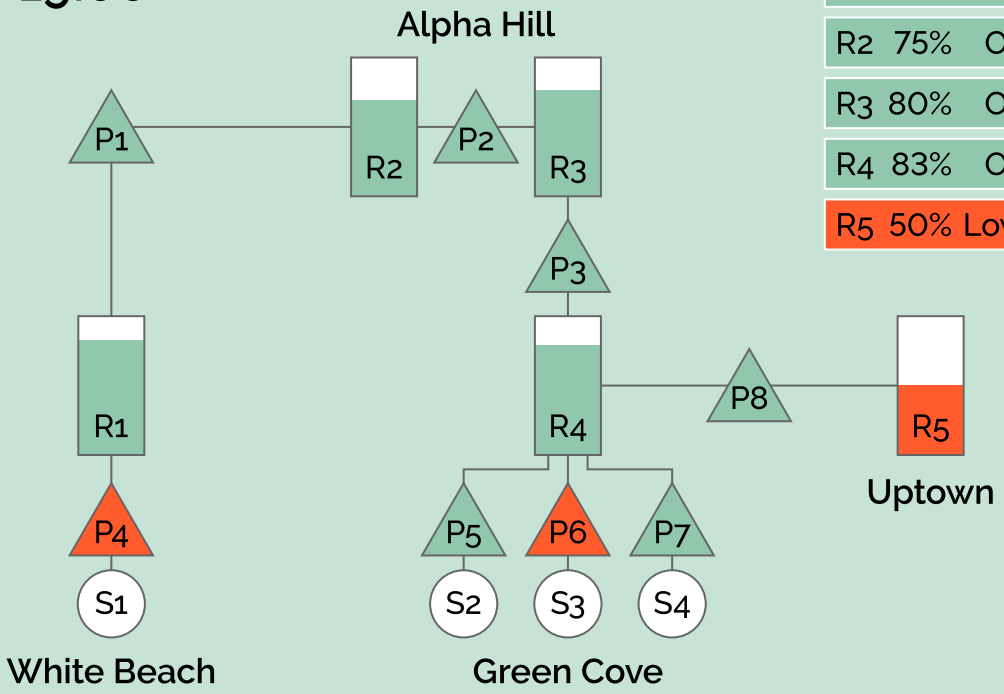
Reservoirs		
R1	89%	Ok
R2	75%	Ok
R3	80%	Ok
R4	83%	Ok
R5	50%	Low

Pumps		
P1	0%	Ok
P2	25%	Ok
P3	0%	Ok
P4	83%	Ok
P5	50%	Ok
P6	0%	Ok
P7	83%	Ok
P8	50%	Ok

Strange things occur!

On 19:00 a report indicates the malfunction of the two pumps P4 and P6. R1–R3 have enough water to cover the night. P6 is not needed if the others are fine. There have been issues with P4 in the past month, and a spare part is expected in the coming days. The operator decides to wait till next morning.

Friday 19:00



Reservoirs		
R1	89%	Ok
R2	75%	Ok
R3	80%	Ok
R4	83%	Ok
R5	50%	Low

Pumps		
P1	0%	Ok
P2	25%	Ok
P3	0%	Ok
P4	0%	Err.
P5	50%	Ok
P6	0%	Err.
P7	83%	Ok
P8	50%	Ok

Also, the city council seems to send mails around asking people to save water as the wells seem are draining a nature reserve. The attachment contains a pdf with more details.

Alpha Ville

Please help conserving water

We all enjoy the wonderful hot summer this year. Unfortunately the warm weather has lead to increased consumption of water. The increased consumption threatens to damage the Alpha Ville nature reserves, which hosts most of our water wells. We thus ask you to save water.

The attached PDF file gives you ten hints tips to save water without impacting your life style.

Sincerely,
Your city council

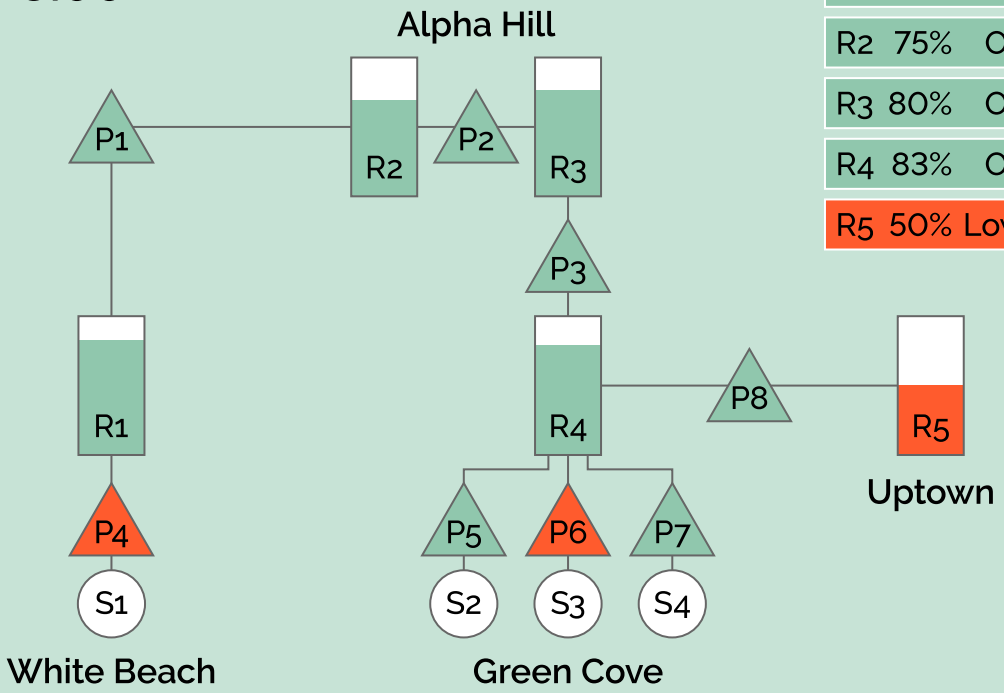
1 attachment: 10 top tips to conserver water.pdf (102 kB)

8:00 The machine picket checks P4 and P6 but does not find an issue. But it cannot start the pumps.

The duty officer was not informed about these e-mails and doesn't really know what to say to the journalist from the local radio station.

15 Minutes:
Who does what?

Saturday 8:00



Reservoirs		
R1	89%	Ok
R2	75%	Ok
R3	80%	Ok
R4	83%	Ok
R5	50%	Low

Pumps		
P1	0%	Ok
P2	25%	Ok
P3	0%	Ok
P4	0%	Err.
P5	50%	Ok
P6	0%	Err.
P7	83%	Ok
P8	50%	Ok

Workshop Progress

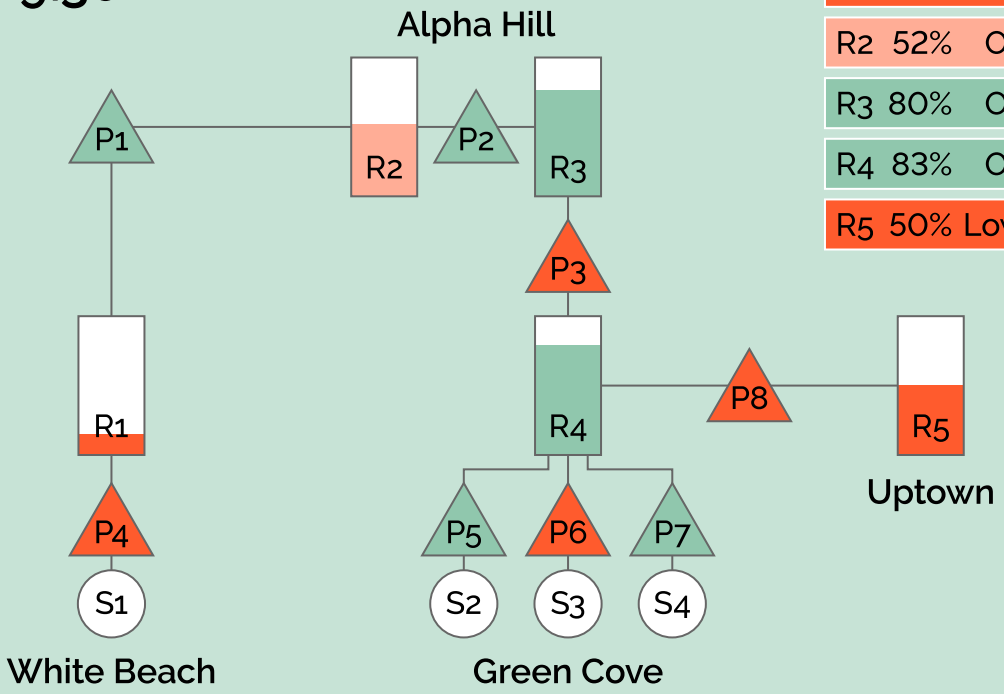
9:30 P3 stops working

10:15 P8 Stops working

11:00 The local radio news reports that the pump stations have been shut down by the city do save water (they drove by the sites, and all seems off and quiet). Some people in White Beach complain, that water pressure is low.

15 Minutes:
Who does what?

Saturday 9:30



Reservoirs		
R1	15%	Ok
R2	52%	Ok
R3	80%	Ok
R4	83%	Ok
R5	50%	Low

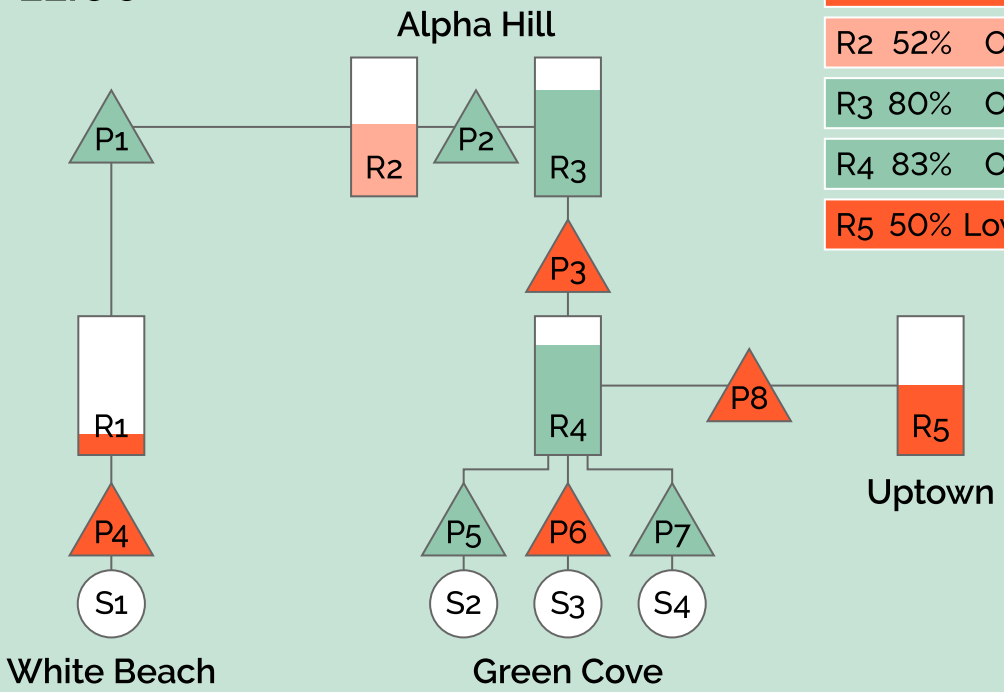
Pumps		
P1	0%	Ok
P2	25%	Ok
P3	0%	Ok
P4	0%	Err.
P5	50%	Ok
P6	0%	Err.
P7	83%	Ok
P8	0%	Ok

ALPHA VOICE

Hi this, this Nosy Jones from the local radio station. It seems that many of the water pumps are switched off to save water. Yet at the same time citizens in White Beach complain that water is only dribbling.

Isn't the city over reacting here?

Saturday 11:00



Reservoirs			Pumps		
R1	15%	Ok	P1	0%	Ok
R2	52%	Ok	P2	25%	Ok
R3	80%	Ok	P3	0%	Ok
R4	83%	Ok	P4	0%	Err.
R5	50%	Low	P5	50%	Ok
			P6	0%	Err.
			P7	83%	Ok
			P8	0%	Ok

13:30 The national Cyber Security centre puts out an advisory, that the the PDF in the mail contains an exploit.

The media pick this up and keep asking the duty officer if there is a connection. He denies, after all what do have pumps to do with e-mails.

15 Minutes:
Who does what?

Cyber Center

Advisory

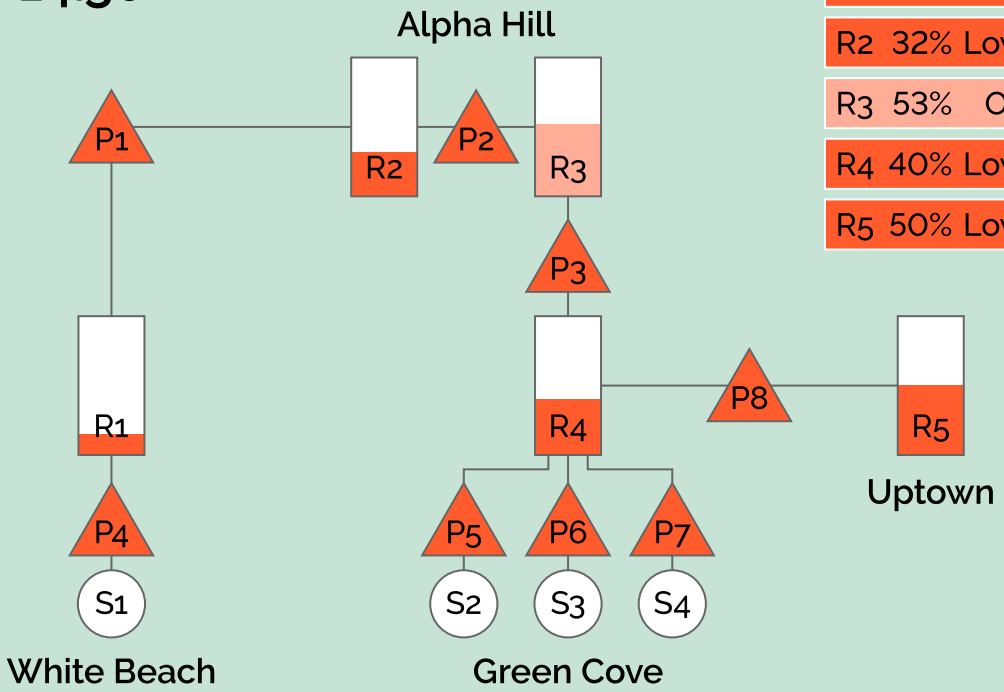
A recent spam wave has been observed, calling citizens to save water. The attached PDF file contains malware which installs keyloggers. Once inside the network the malware seeks to infect further hosts by deploying the eternal blue exploit.

14:30 The full board is now assembled as all the remaining pumps fail.

R1–R3 have enough water for ¼ day only for White Beach. It continues being hot.

15 Minutes:
Who does what?

Saturday 14:30

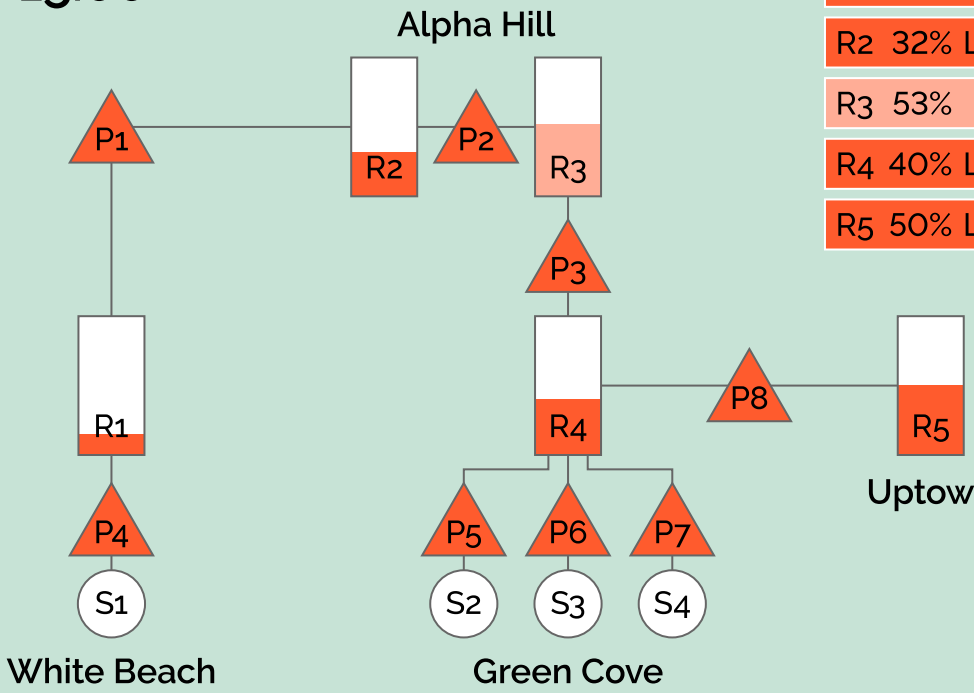


Reservoirs			Pumps		
R1	15%	Low	P1	0%	Err.
R2	32%	Low	P2	0%	Err.
R3	53%	Ok	P3	0%	Err.
R4	40%	Low	P4	0%	Err.
R5	50%	Low	P5	0%	Err.
			P6	0%	Err.
			P7	0%	Err.
			P8	0%	Err.

15:00 It turns out that Friday operations officer has also received such a mail on Friday and has opened it.
16:00 The IT teams are now in and check the office infrastructure. The junior intern suggesting that the control network should be investigated too is told that it is protected by a firewall and not vulnerable.

15 Minutes:
Who does what?

Saturday 15:00



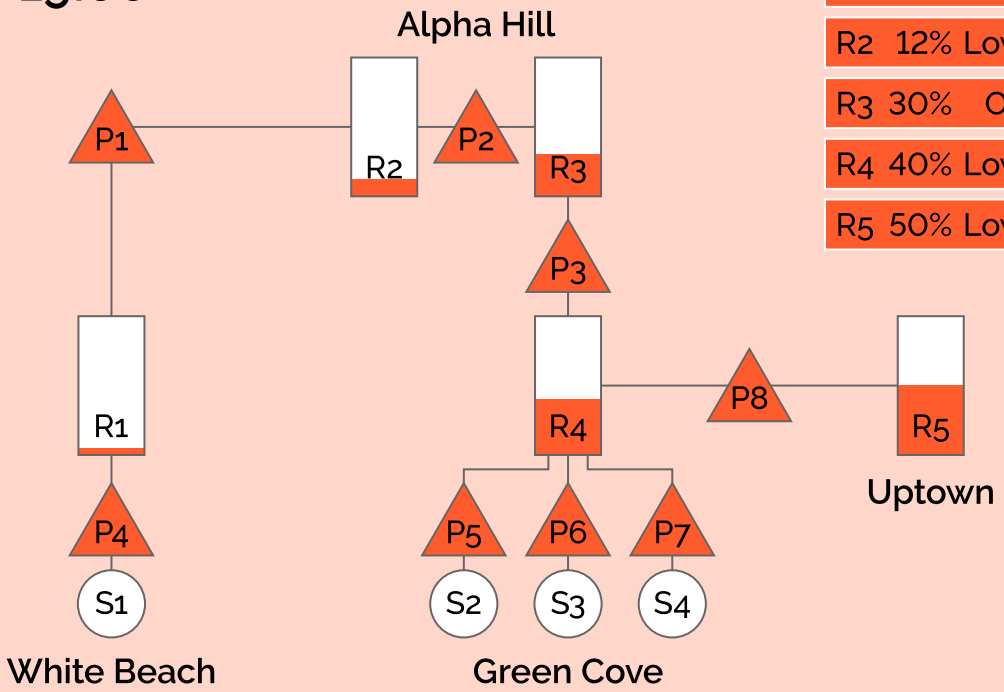
Reservoirs			Pumps		
R1	15%	Low	P1	0%	Err.
R2	32%	Low	P2	0%	Err.
R3	53%	Ok	P3	0%	Err.
R4	40%	Low	P4	0%	Err.
R5	50%	Low	P5	0%	Err.
			P6	0%	Err.
			P7	0%	Err.
			P8	0%	Err.

19:00 Alpha Ville now has a water shortage.

The head engineer that was retired last you on short notice (but with a good package) to save costs calls in offering help. He suggests to put the pumps into manual mode which requires staff on site, but seems to work.

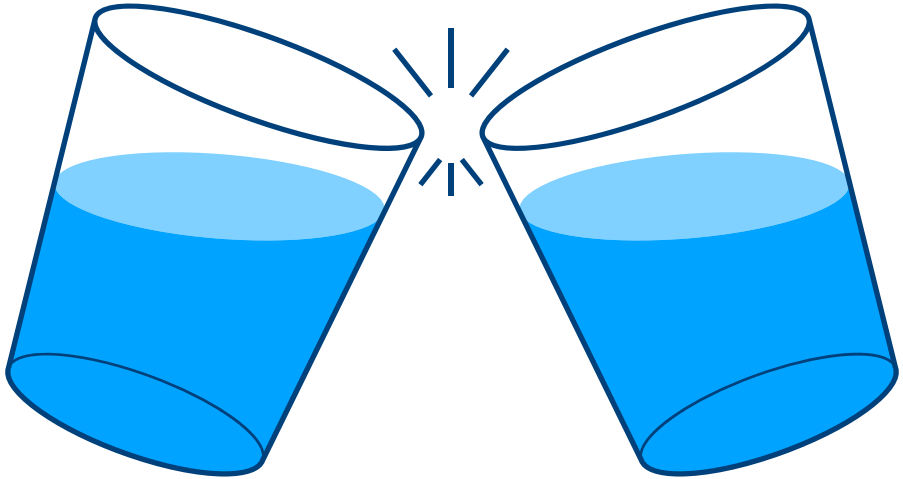
15 Minutes:
Who does what?

Saturday 19:00



Reservoirs			Pumps		
R1	5%	Low	P1	0%	Err.
R2	12%	Low	P2	0%	Err.
R3	30%	Ok	P3	0%	Err.
R4	40%	Low	P4	0%	Err.
R5	50%	Low	P5	0%	Err.
			P6	0%	Err.
			P7	0%	Err.
			P8	0%	Err.

End



Discussion

What went well?

What wend bad?

How could this happen?

ICS systems are often not built for an internet environment. They assume that all traffic is benign.

A simple scan (as the virus probably did) could lock critical components up.

**The malware installs keyloggers:
Maybe this is a targeted attack?**

We don't know without further work...

Communication

That is often one of the main issues.

Talking to the press?

Is info passed across shifts?

Is there an emergency communication plan?

Would you organize your org different now to account for this, e.g. only one IT department?

Legacy code


Rem0te
Follow
I found COBOL code with a customer. Good. Mainframe. Nothing unusual. The last comment is from 1985. From my mother.
7:13 AM - 25 May 2018
1,685 retweets 5,117 Likes
Rem0te
That was then the WTF moment of the year ... The face of the technical manager included.

This will never happen...

...but something similar or totally different might.