JACOBS

Gordon Powell,
ICS Cybersecurity
Principal Consultant

Jacobs Engineering
Cyber Security Group

Resilience: the ability to withstand an incident, respond, and make whole

JACOBS

200+ Cybersecurity focused personnel

Work with 12 of the 16 IC agencies

15 year track record in Cybersecurity

Dedicated Cybersecurity Innovation Lab

Established Methodology

Protection First
Monitor for Change
Defense Evolution

DOD CYBER FOOTPRINT

Within the Department of Defense, there are over 30 unique types of ICS. There are an estimated 2.5 million unique ICS systems that are used in over 300,000 buildings and over 250,000 linear structures.

And that’s just the buildings…

How do we Defend, Respond, and Recover?

We take a look at the tools, methods, and procedures at our disposal to first develop a strong Cybersecurity posture, then respond to an attack, and facilitate rapid recovery.

Resilience is a result…

…of a combination of unique factors working together to create a flexible yet strong, secure fabric

Like these guys =>

Why the Fantastic Four?

- Each has a unique skill
- These skills are complimentary
- They must work together to be effective
- Provide Defense in Depth
- They’re cool (who’s your favorite?)

Meet Johnny, the Human Torch

The personification of the latest in Firewalls. He possesses cool attributes like:

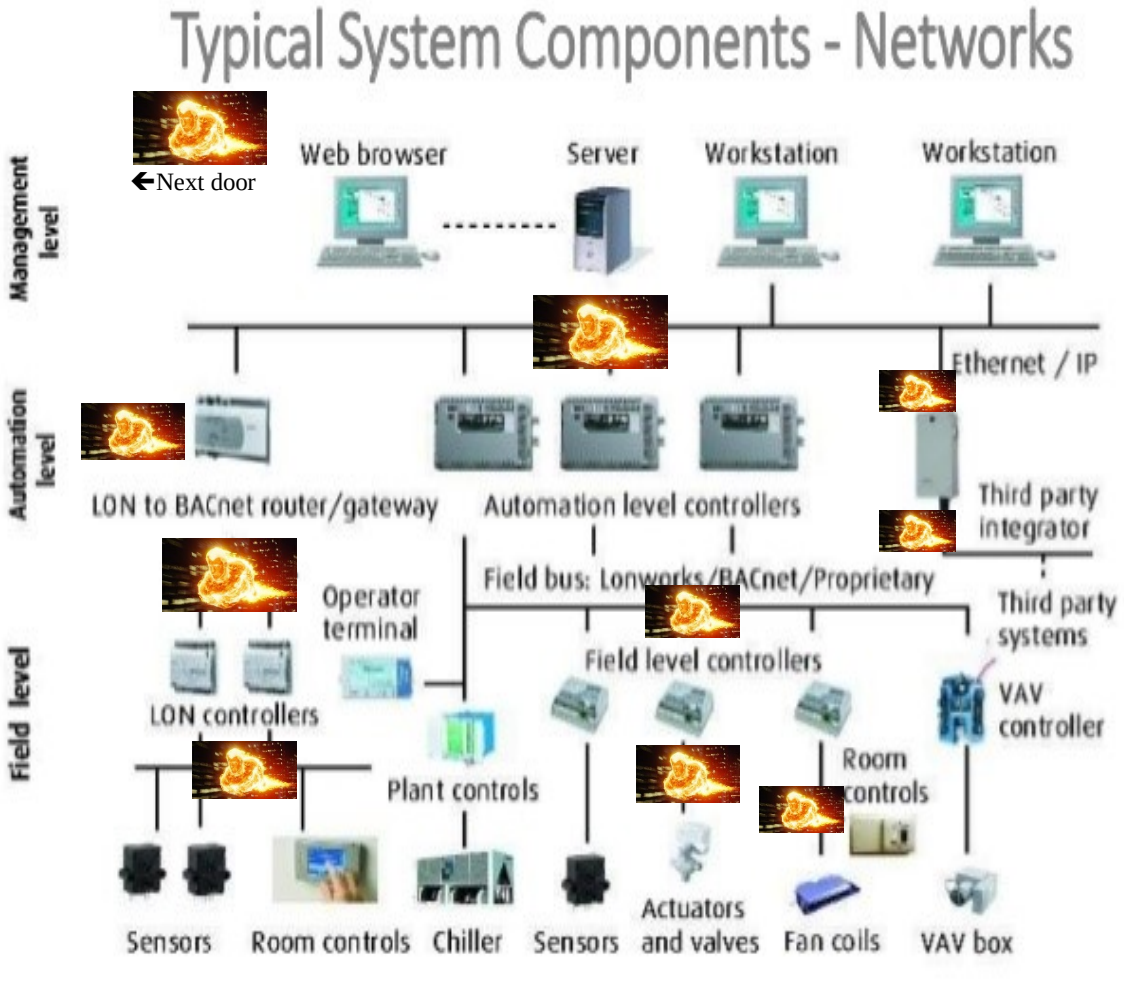
- He’s Stateful (goes to his head)
- He can be Distributed (flies too)
- He’s ICS Protocol Aware
- Can perform Sanity Checks
- Can do Deep Packet Inspection
- He likes to hang out in Routers and Switches too

Johnny likes to hang out at the front or back door.

Typical places Johnny hangs out:

- Between the humans and the backbone
- Between the traffic guys and the controllers
- Between controllers and field devices
- He also likes to live inside the comfort of the devices to make them intrinsically safe (He hangs with Ben there at times)

Overview....



Meet Susan, The Invisible Woman

The personification of the latest in Detection.

Susan scouts the infrastructure looking for devious anomalies, checks them out, and tells Reed (Ben and Johnny if necessary).

She has cool attributes (obviously)

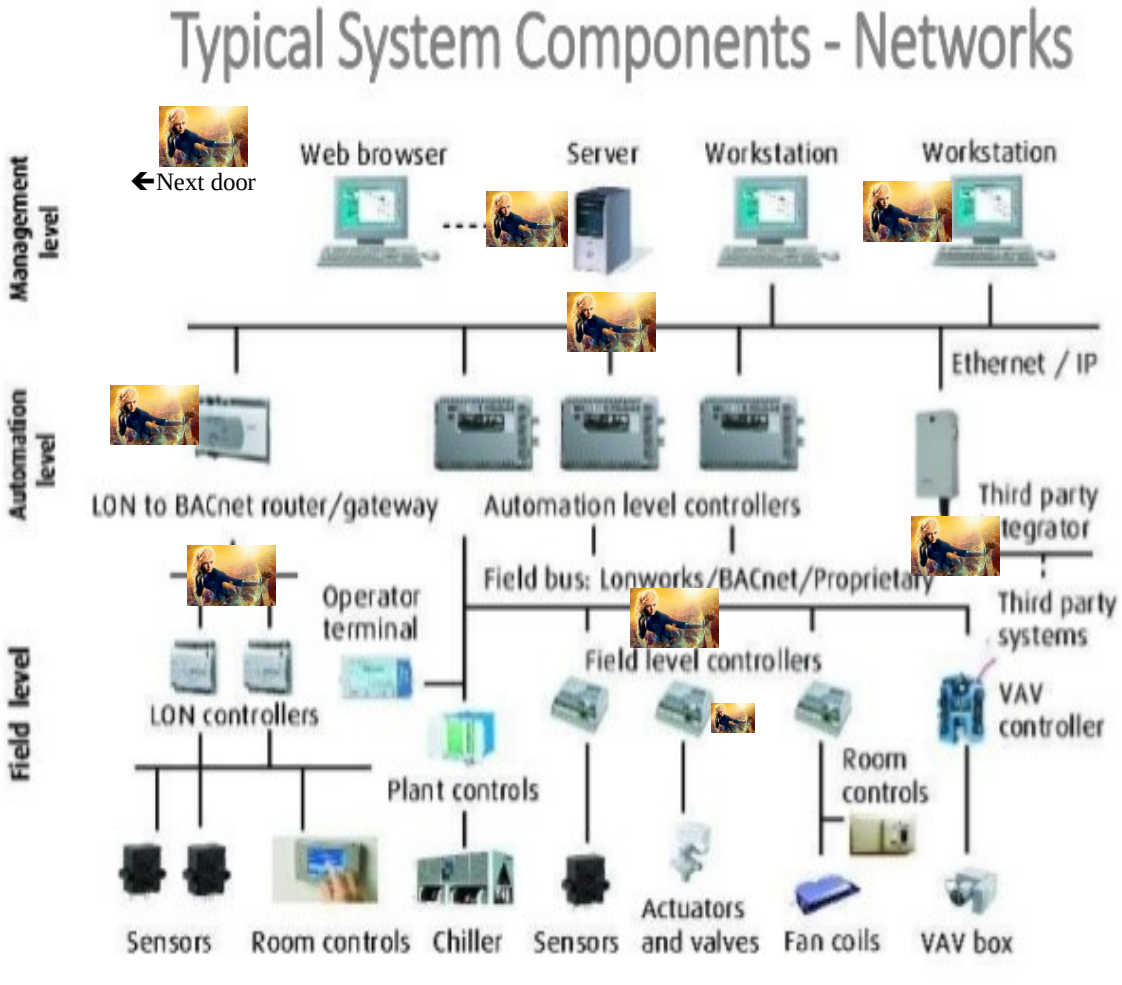
- Distributed (she's invisible, can go anywhere she wants!)
- Analytic (She does some work before giving it to the Boss, Reed)
- ICS Protocol Aware
- Able to do Deep Packet Inspection
- Identifies rules and roles violations (tells Reed, and maybe Johnny or Ben).

Susan is all over but has plenty of apartments.

She travels the network checking on devices and such, looking for intruders. She can park inside devices too (checking on Johnny and Ben). She can tell if someone has changed code and is trying to deliver it innocuously. You can try to catch her:

- She has appliances all over the various networks
- Sometimes she hangs out in routers/switches/firewalls (with Ben and Johnny)
- Frequently visits Hosts
- Inside Packets doing Deep Inspections

Overview....



Meet Ben, The Thing

He the personification the Defense in Depth plan.

He’s tough and likes everything around him to be. He has little tolerance for those who would invade his space! He has great attributes like:

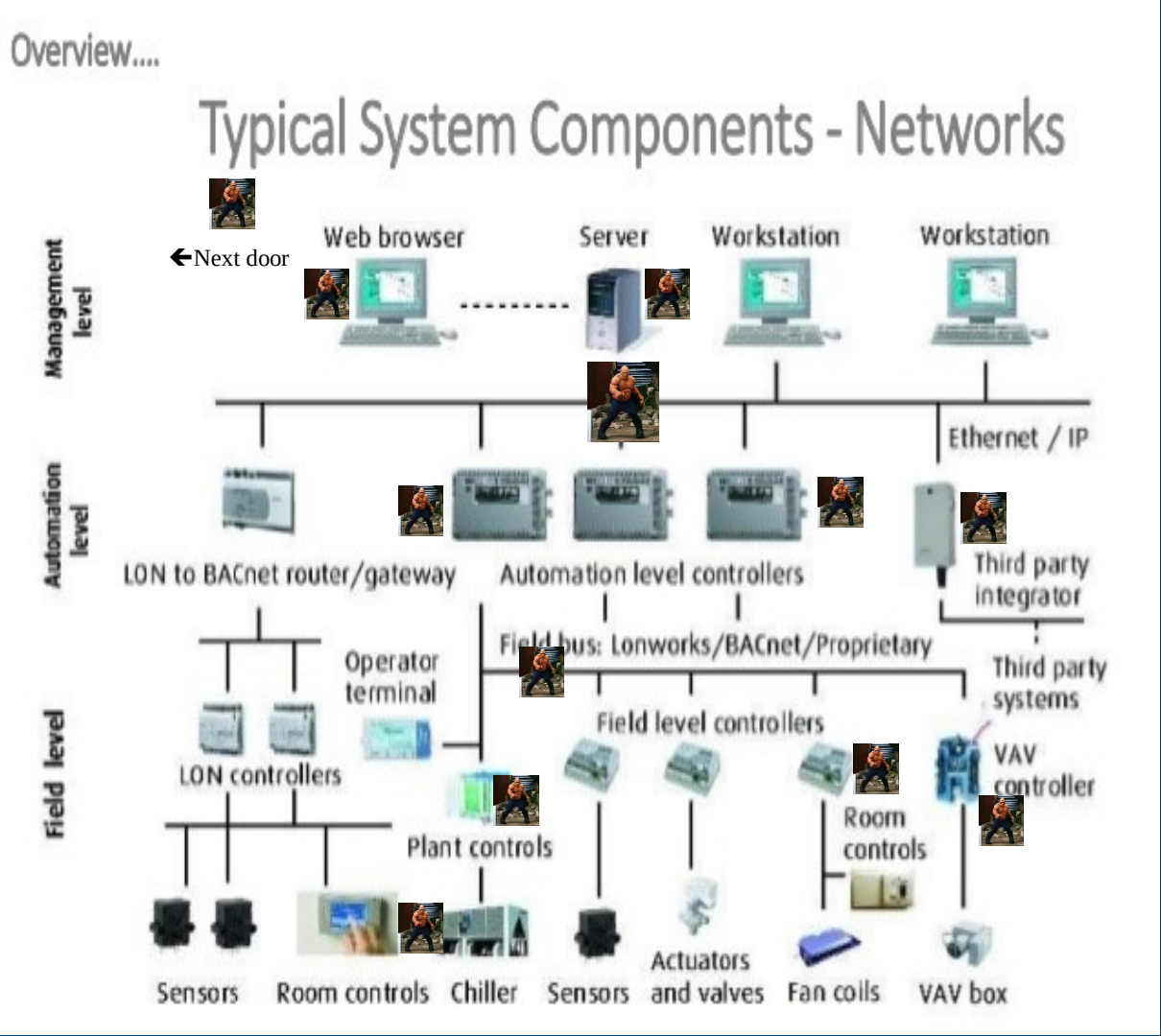
- Distributed (Standardized)
- Hardened (Hardware, Software, Firmware)
- Intrinsic Cyber Controls
- Whitelisting (only the good guys allowed)
- Crushes Virus and Malware
- He’s Cyber Physical

Ben (The Thing) gets around too.

He works inside making things stronger and crushes anything that might get past Johnny or Susan.

You can find him doing things like:

- Making OS, Apps, Firmware as dense as possible
- Cryptographically sign things
- Killing Viruses and Malware
- Filling security holes
- Helping the team respond to incidents
- Blocking CD/DVD/USB access



Meet Reed, Mr. Fantastic

The Brains behind it all.

He’s the Central Nervous System providing for the overall architecture, collection of data, audit, and analysis, Incident response and recovery mechanisms (I know it’s a lot, but hey, he’s the boss right?). Has the cool tools like:

- SIEM* – Collection and analysis
- Virtualization – (Stretch it!)
- SDN – Software Defined Networks
- IR – Incident Response (Director)
- Network/System design (Secure practices, Zones and Conduits, Wide Area)
- ICS Protocol/Standards Aware (Enforcer)

**Security Information and Event Management*

How do we make it happen?

With a little help from our friends!

Questions?