



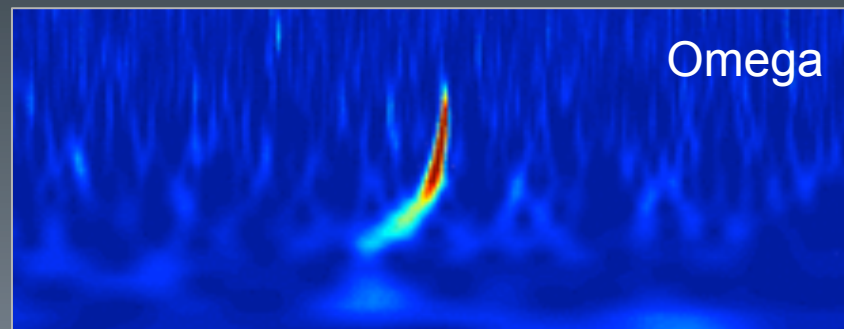
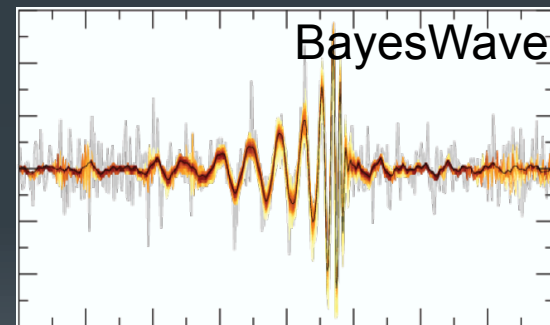
# How we know GW150914 was NOT an injection

Is GW150914 too perfect to be real?

(a collection of work and ideas of many, many people)

# Introduction

- GW150914 happened in the early hours of September 14, during ER8
- The signal has a high SNR and appears to be a perfect binary black hole coalescence
- Both the timing of the signal (during an ER, when software was still being tested) and the size and quality of the signal have raised questions about its veracity
- Could GW150914 be a fake?



# How are injections normally done?

- Software Injections
  - a signal is added to the strain channel (hoft) after it is recorded
  - they do not appear in raw frames, or in any other channels
- Hardware Injections
  - an actuator is used to push on an end mirror in the interferometer to mimic a GW induced strain
  - these injections appear in hoft and in many monitor channels
  - “Hardware” is a misnomer – this is done via the digital system
- Blind Injections
  - a hardware injection which is done via an “off-limits” channel

# GW150914 was NOT a “normal” injection

- This was checked shortly after the event was discovered
- No injection was made, and in fact we didn't even know HOW to make hardware injections at the time of the event. (Inverse actuation filters for L1 had not been computed.)



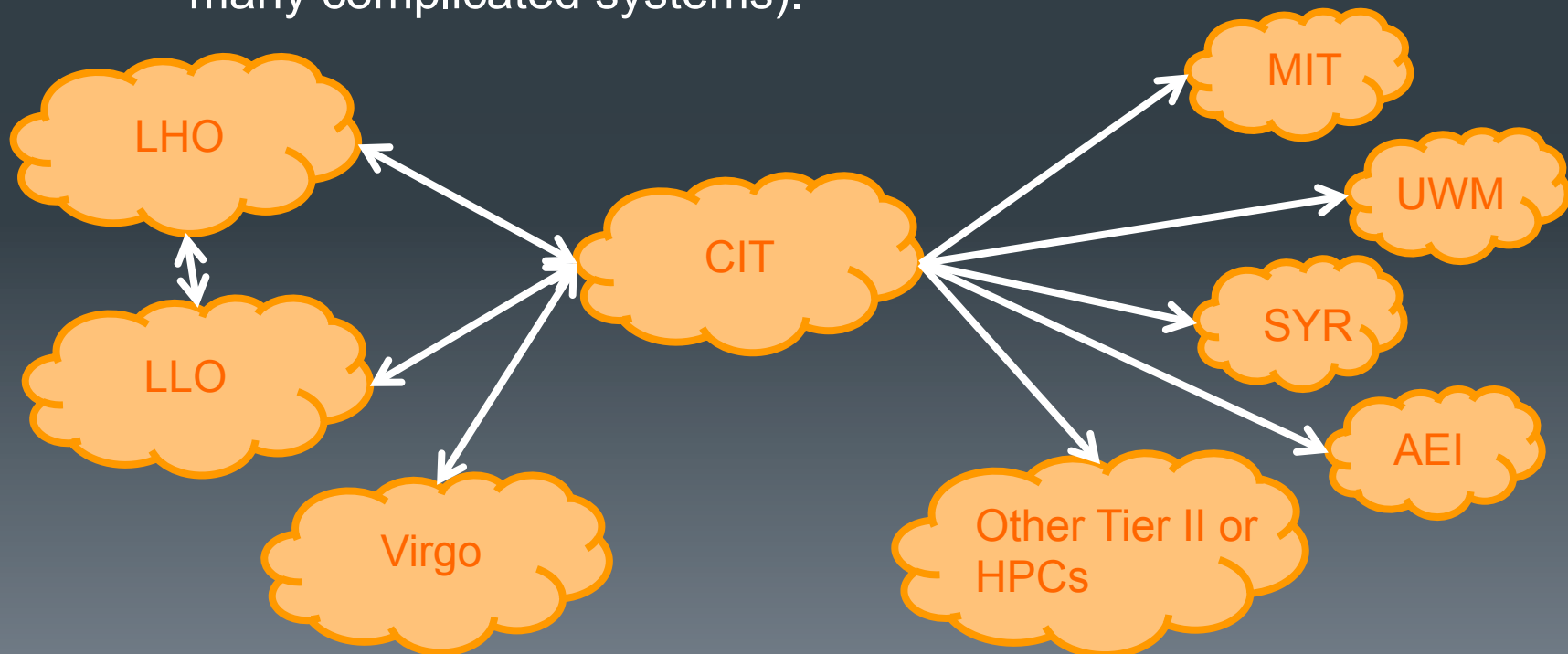
# What about “Rogue injections” ? (injections that don’t follow the rules)

- Frame Spoofing
  - replace the original frames with fake frames that contain an event which was not there before
- Double Blind Injections
  - an injection into the interferometer control computer
    - like a normal blind injection, but not recorded in “the envelope”
    - or injected via some non-standard path (e.g., PCAL)
  - Easter Egg Hacks – modifications of the digital system
- Analog Hacks
  - added hardware which changes the signals in analog before they are recorded

Note: All reference are on a slide at the end.

# From strain to your computer

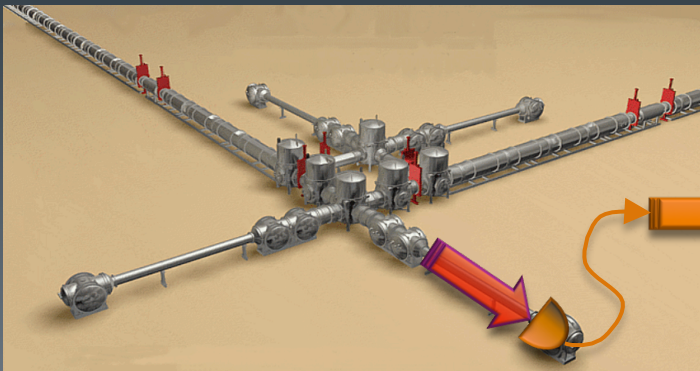
- How does data flow from the interferometer to the analysis pipelines?
- Data from the observatories is quickly distributed, so if you want to fake it you must work at the source (or hack many, many complicated systems).



# At the observatories

- The gravitational wave is imprinted on the light in the interferometer
- That imprint is converted into an analog signal on the photodetectors, which is then digitized and sent to the digital control system (CDS)
- The digital control system passes this signal on for storage and distribution (LDAS)

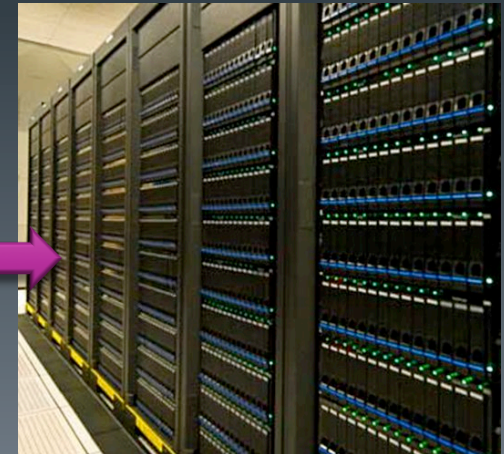
Interferometer



Digital Controls



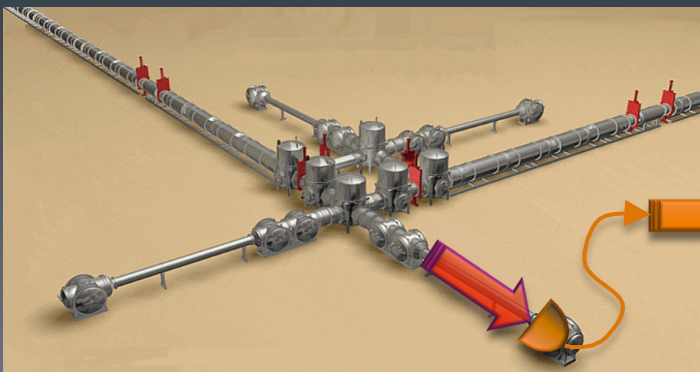
Data Storage



# Frame Spoofing...

- Wouldn't it be easy to just replace the frames with ones that contain a signal after they are written to disk?
- If someone did this before they were distributed, and they did it at both observatories, how would we ever know?

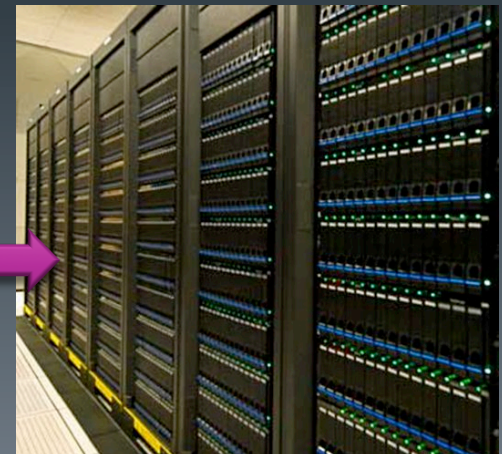
Interferometer



Digital Controls



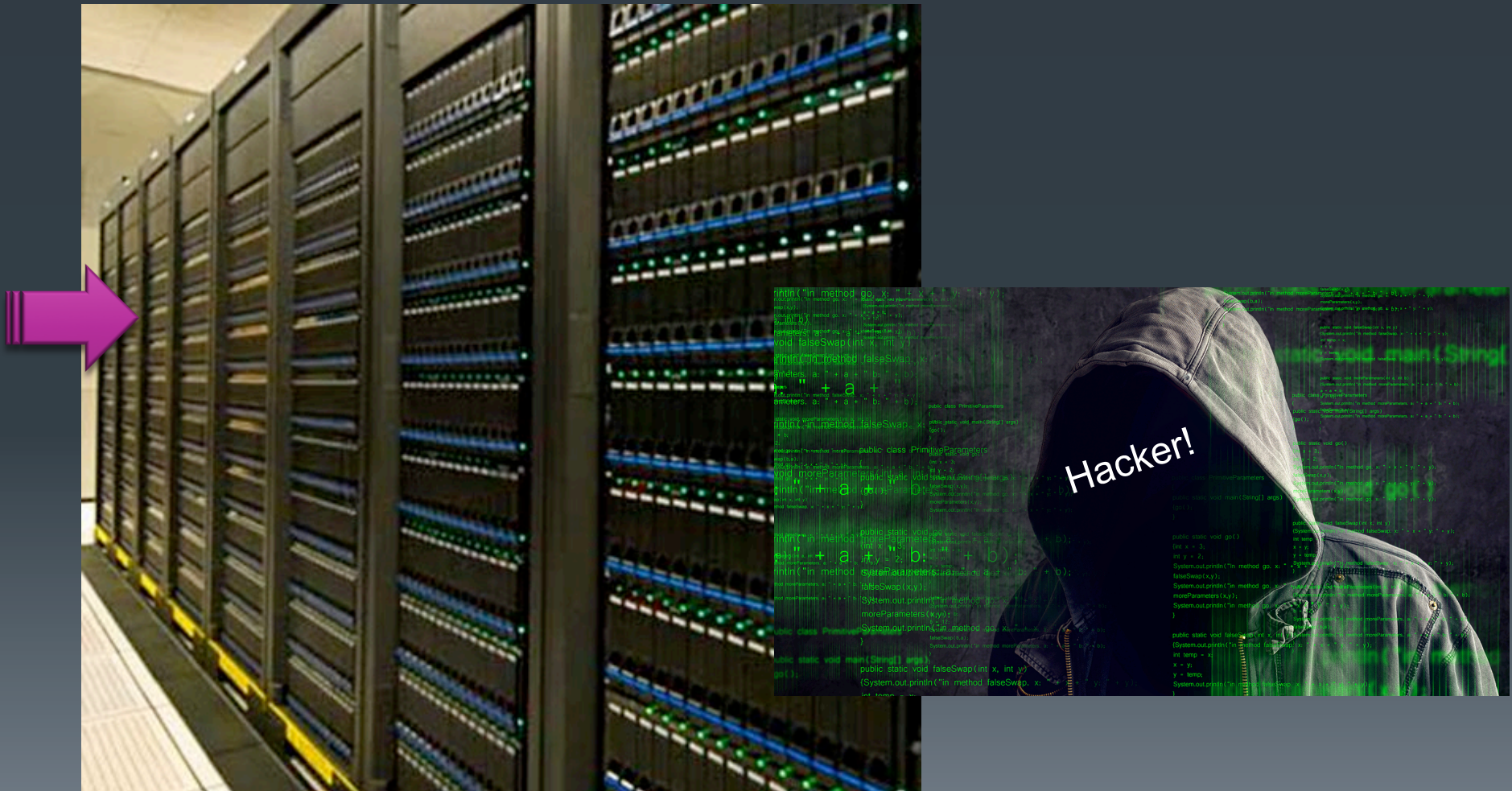
Data Storage





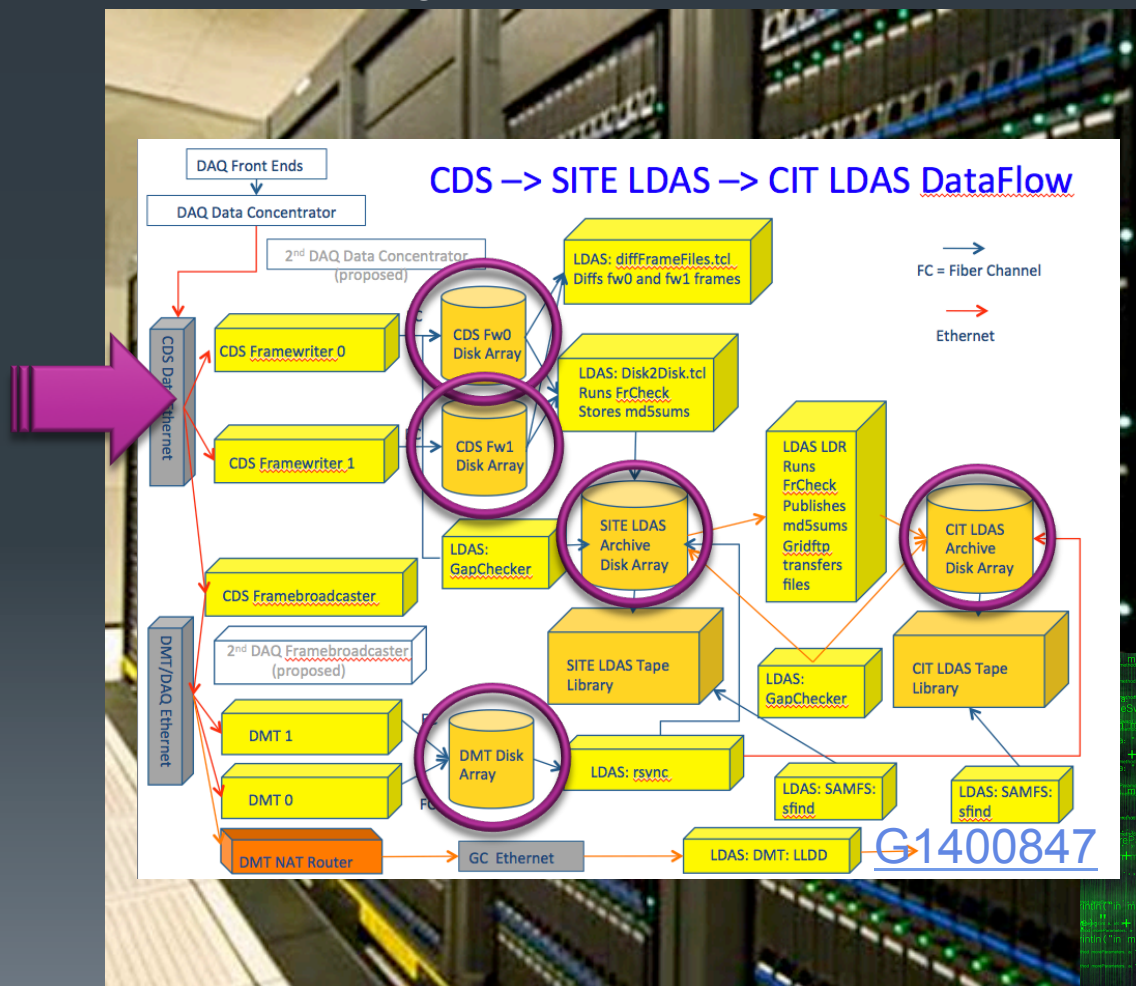
# Frame Spoofing!

Data Storage



# Frame Spoofing???

## Data Storage



The data goes from CDS to 3 separate systems, 2 for redundant storage and 1 for distribution. Checksums are quickly generated, and data is cross checked.

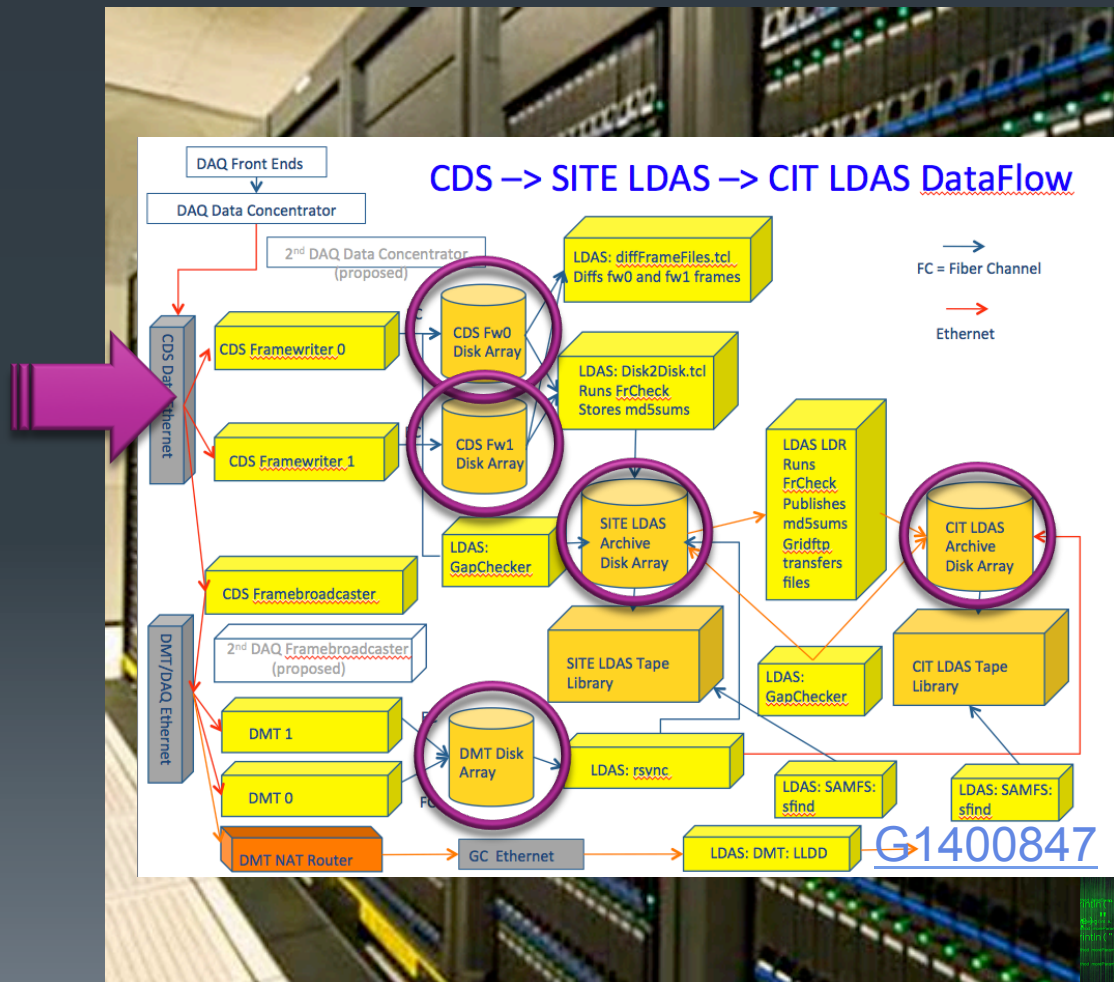
Frame spoofing would have to be done simultaneously on multiple servers at LHO, LLO and CIT. All traces of activity, including remotely stored log files, would need to be erased.





# Frame Spoofing: a major operation due to security and redundancy.

## Data Storage



Hacking LHO, LLO and CIT and replacing all redundant copies of the data is not impossible (what is?), but that is not the end of the story...

What exactly is “the data” that would need to be replaced?

Just the strain channel?



# Frame Spoofing: what would need to be spoofed?

Digital Control System (CDS)

Analog DARM

Strain (hoft)


DARM = Differential Arm ~ Strain

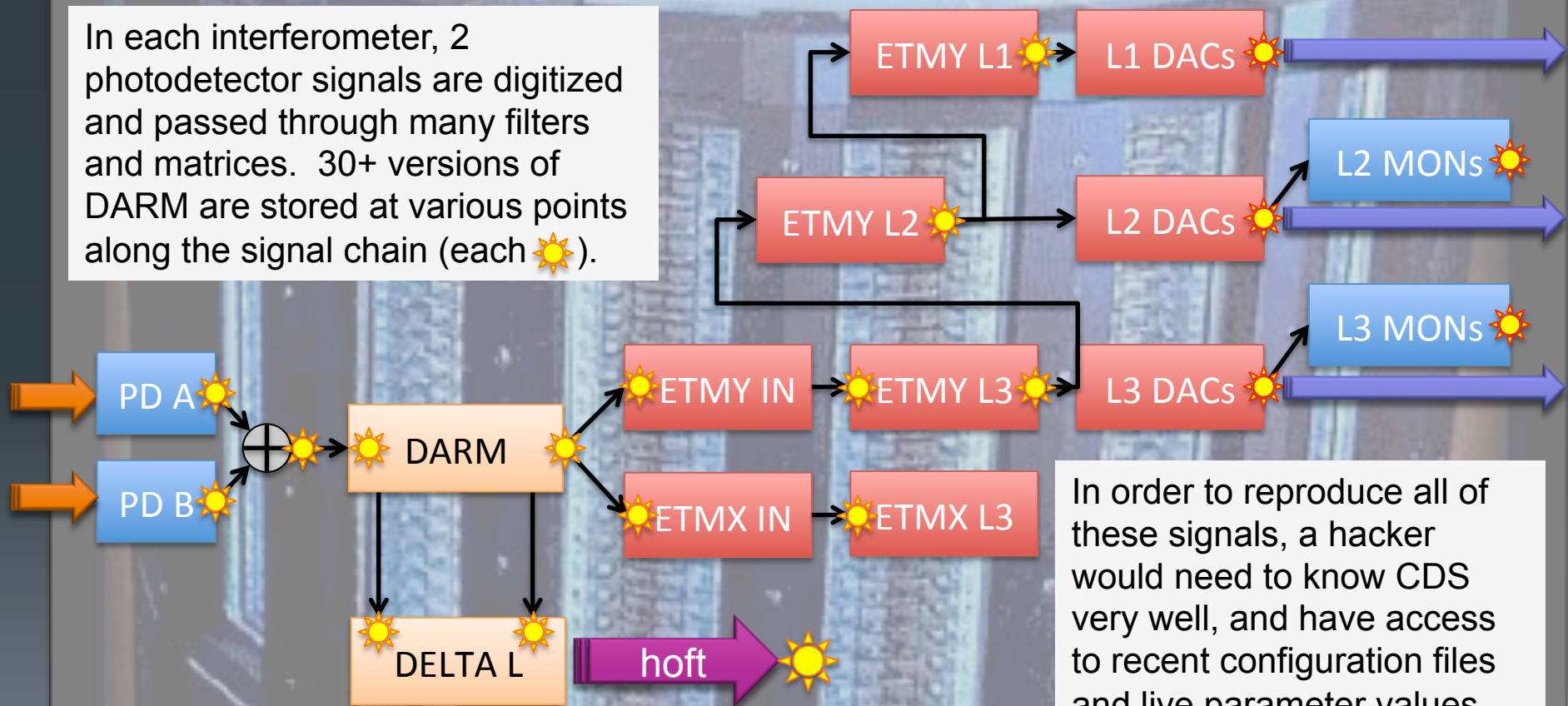




# Frame Spoofing: what would need to be spoofed?

## Digital Control System (CDS)

In each interferometer, 2 photodetector signals are digitized and passed through many filters and matrices. 30+ versions of DARM are stored at various points along the signal chain (each ).



In order to reproduce all of these signals, a hacker would need to know CDS very well, and have access to recent configuration files and live parameter values.

# No Frame Spoofing

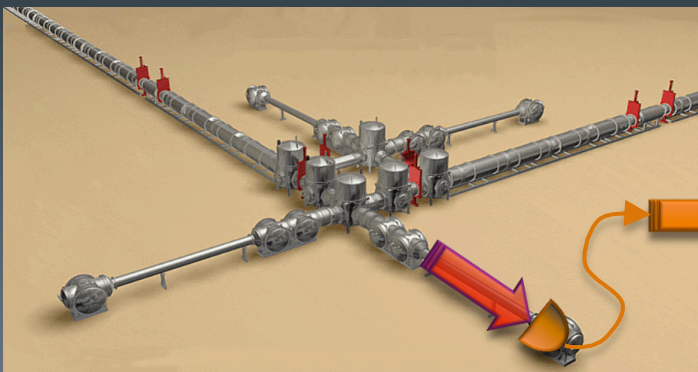
- This attack, while apparently simple, turns out to be a monumental feat (one might call it “impossible”)



# Double Blind Injections...

- Isn't it possible that someone injected a signal into the digital control system (CDS) before it went to LDAS for storage?
- We do this regularly... heck, it might have even happened by accident, right?
- If it went in through the BLIND channel, but was not recorded in "the envelope" we would never know! Would we?

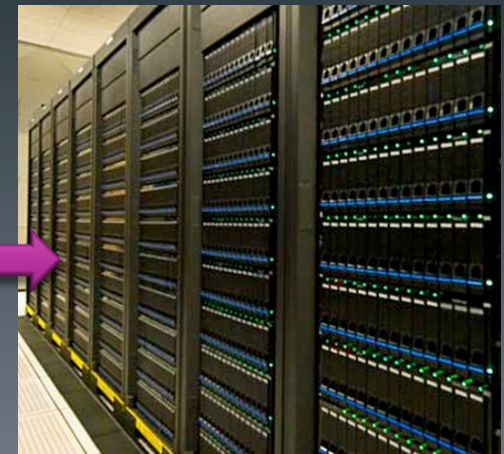
Interferometer



Digital Controls



Data Storage





# Double Blind Injections

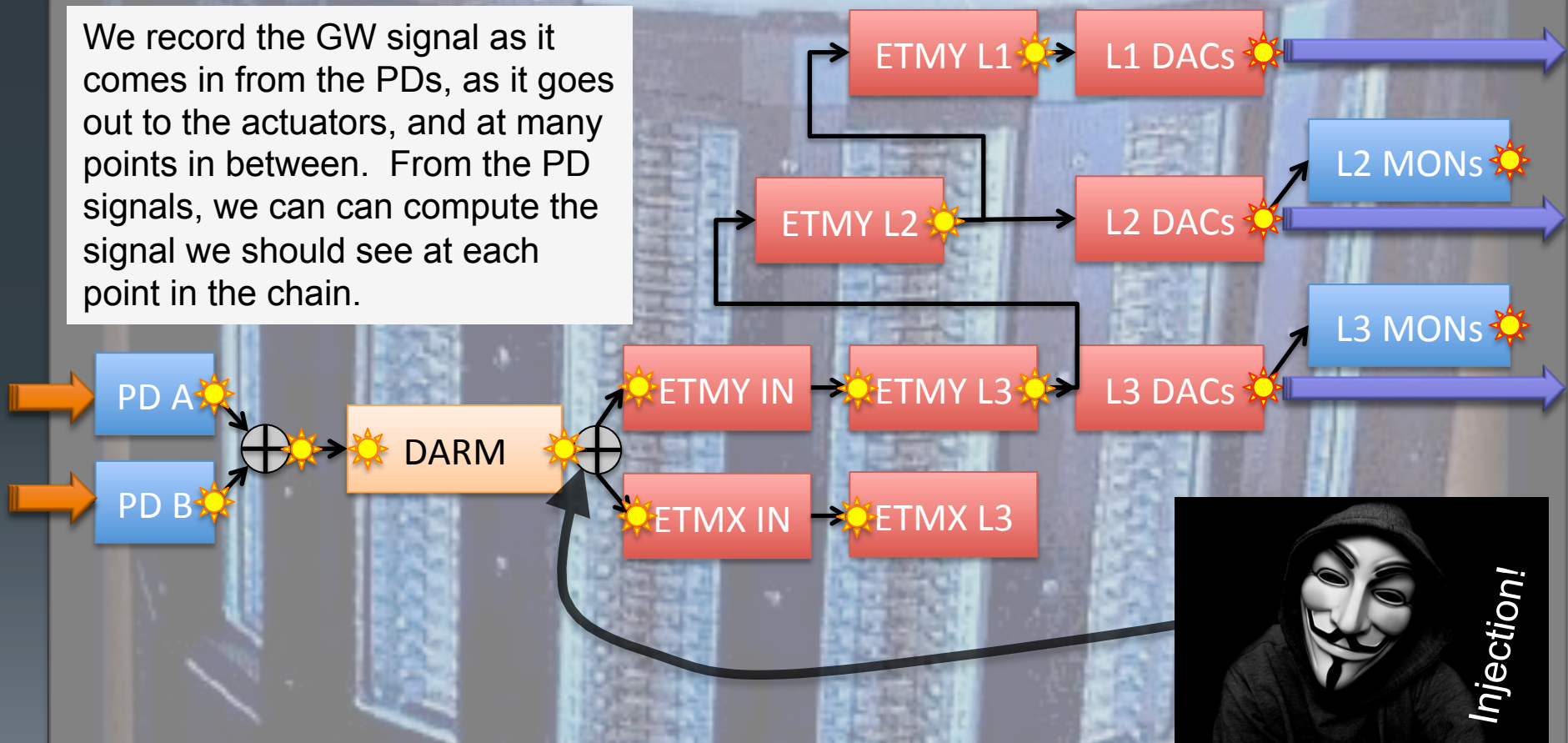
Digital Control System (CDS)



# Double Blind Injections

## Digital Control System (CDS)

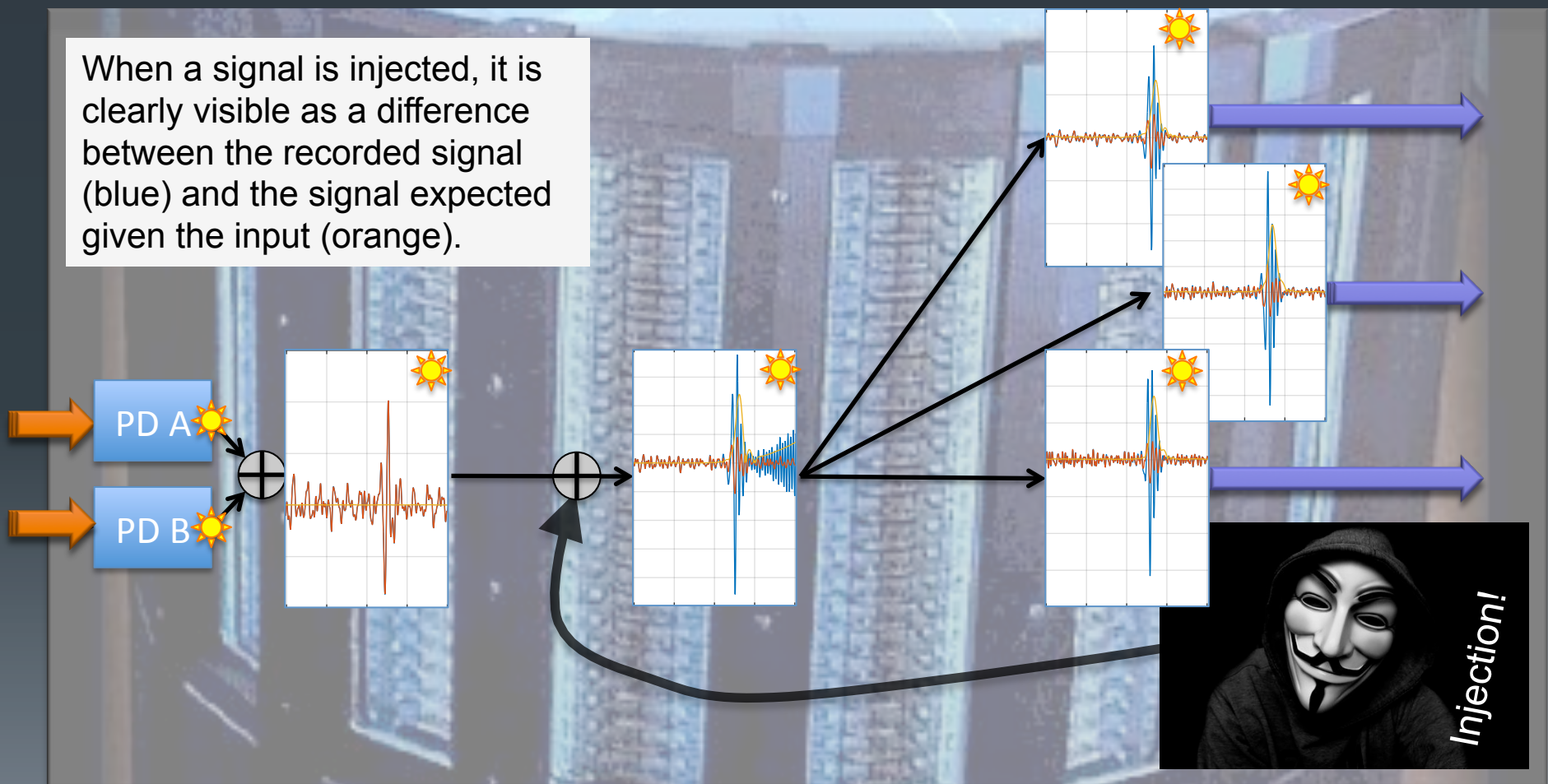
We record the GW signal as it comes in from the PDs, as it goes out to the actuators, and at many points in between. From the PD signals, we can compute the signal we should see at each point in the chain.



# Double Blind Injections: injections are clearly visible

## Digital Control System (CDS)

When a signal is injected, it is clearly visible as a difference between the recorded signal (blue) and the signal expected given the input (orange).



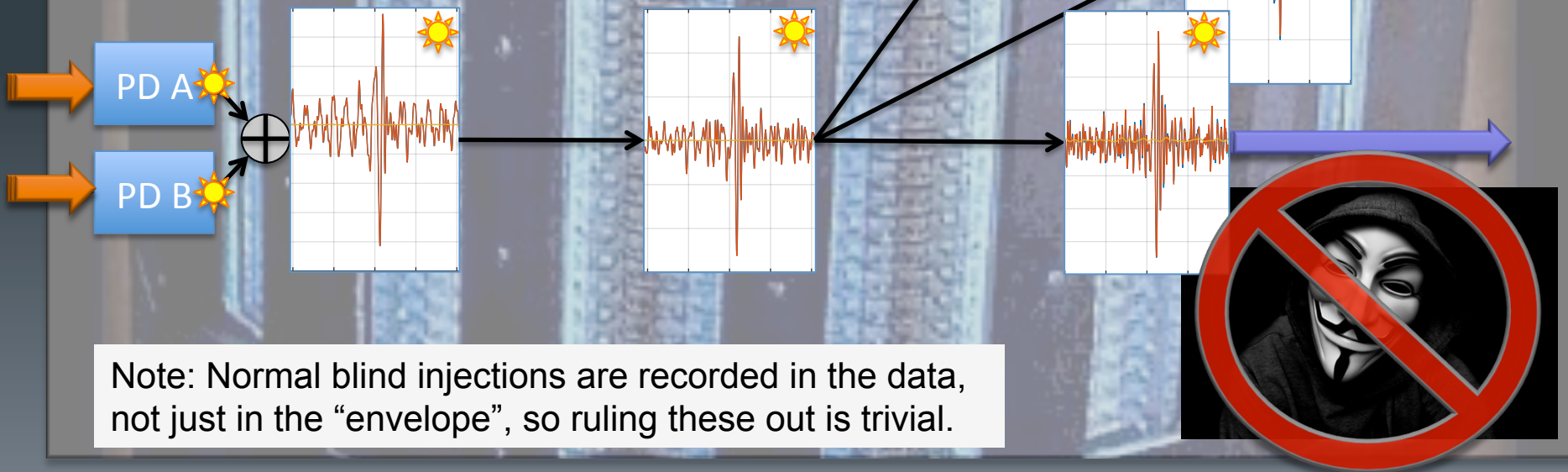


# Double Blind Injections: no injection during GW150914

## Digital Control System (CDS)

At the time of GW150914, the DARM signal propagates through the loop as expected.

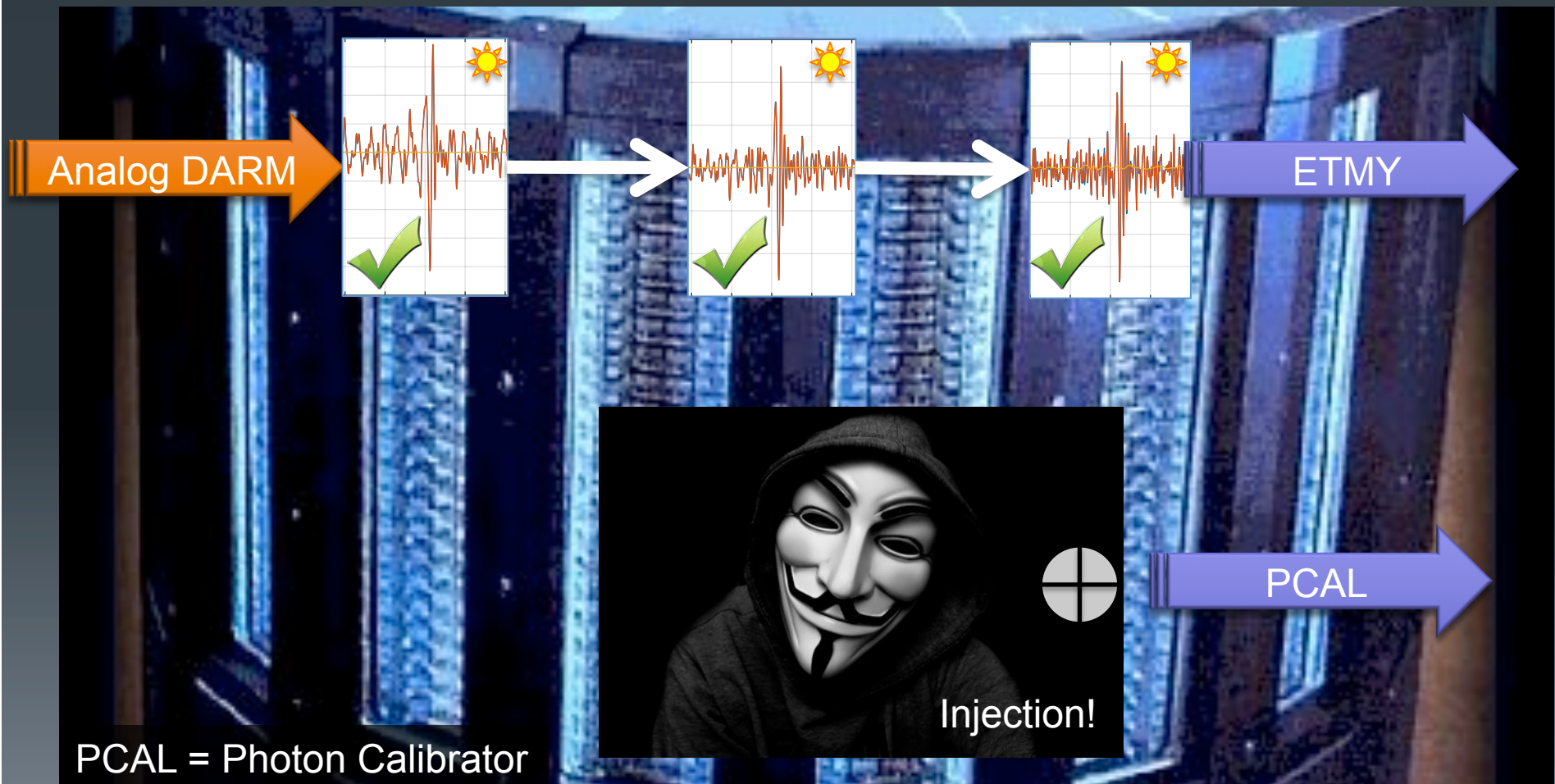
Nothing is added at any point, which rules out all kinds of injections into DARM, including “blind” injections and front-end software bugs.



Note: Normal blind injections are recorded in the data, not just in the “envelope”, so ruling these out is trivial.

# Double Blind Injections: what about injecting elsewhere?

Digital Control System (CDS)



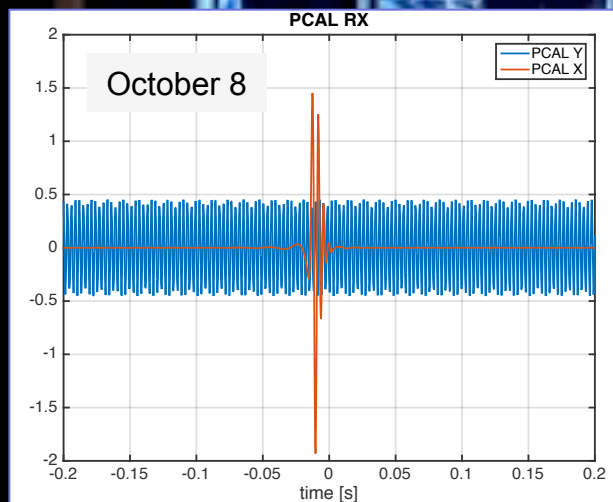


# Double Blind Injections: what about injecting elsewhere?

## Digital Control System (CDS)

An injection into PCAL, or anywhere else that DARM is not normally found, results in a transient which is coincident with the event in DARM. This leaves a clear signature in the corresponding auxiliary channel.

Injections of this sort also pose a significant problem: the coupling to DARM must be known and inverted to produce an injection signal. No such inverse filter existed for PCAL until Oct 2.



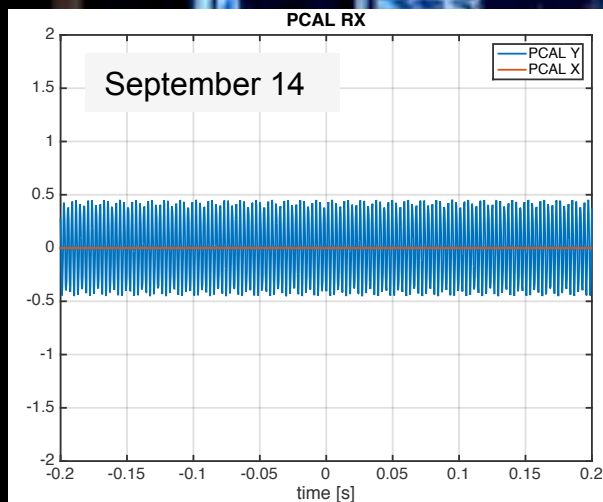
PCAL

# Double Blind Injections: what about injecting elsewhere?

## Digital Control System (CDS)

PCAL and ALL other auxiliary channels have been checked repeatedly and exhaustively. No significant transient was found at the time of GW150914.

Essentially, this means that all signals which should contain the event (e.g., DARM) do so as expected, and all the signals which should NOT contain the event do not.



PCAL

# No Double Blind Injections

- Injections are recorded in many ways, so there is no way for an accidental injection to be mistaken for a real signal
- Blind injections are only blind by convention and are as easy to uncover as any other injection
- The inverse filters needed to make injections were not in place on September 14
- There is no sign of an injection around GW150914





suggested by “AL”,  
who will remain otherwise  
nameless

Matthew Evans

10/24/15

24

## Detailed Example: PCAL injection followed by frame spoofing

- PCAL is one of the easiest injection points to invert, and somewhat disconnected from the rest of the DARM loop, so it appears to be an easy target
- If a PCAL injection is made, it will only appear in
  - the digital excitation itself (EXC\_SUM)
  - the monitor diodes (TX and RX)
- This “easy” hack requires
  - generating a time-domain CBC waveform (easy for some)
  - offline PCAL coupling inversion (easy for some)
  - hacking a control machine, or physical access (easy for a few)
  - defeating security to replace many redundant frames (hard)



# Easter Egg Hacks

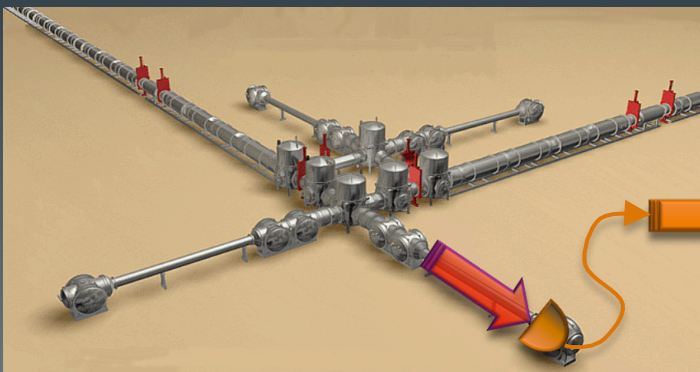
- A large class of attacks involve the replacement of some part of the digital system with malicious code capable of performing an injection without leaving a record
- This avoids the need to change the frames after they have been disseminated, reducing the scope of the hack
- It would require:
  - signal generation and actuator inversion, as usual
  - CDS administrator privileges at both observatories
  - in depth knowledge of CDS system
  - removal of malicious code before the post-event inspection, or code hidden well enough to avoid detection



# Analog Hacks

- What if someone got to the interferometer analog electronics and added something there?
- Couldn't a signal be injected into one of the test-mass actuators after the monitor points?
- This would probably just require a couple of iPod nanos and some clip leads!

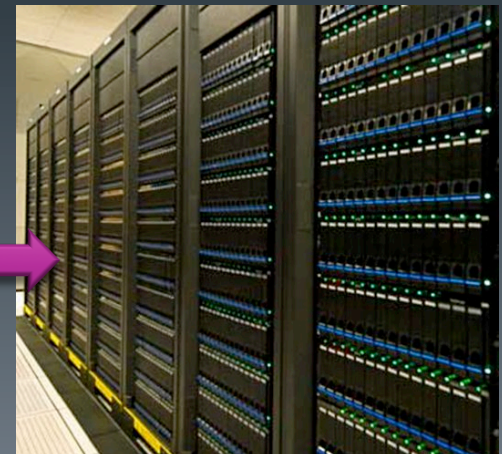
Interferometer



Digital Controls

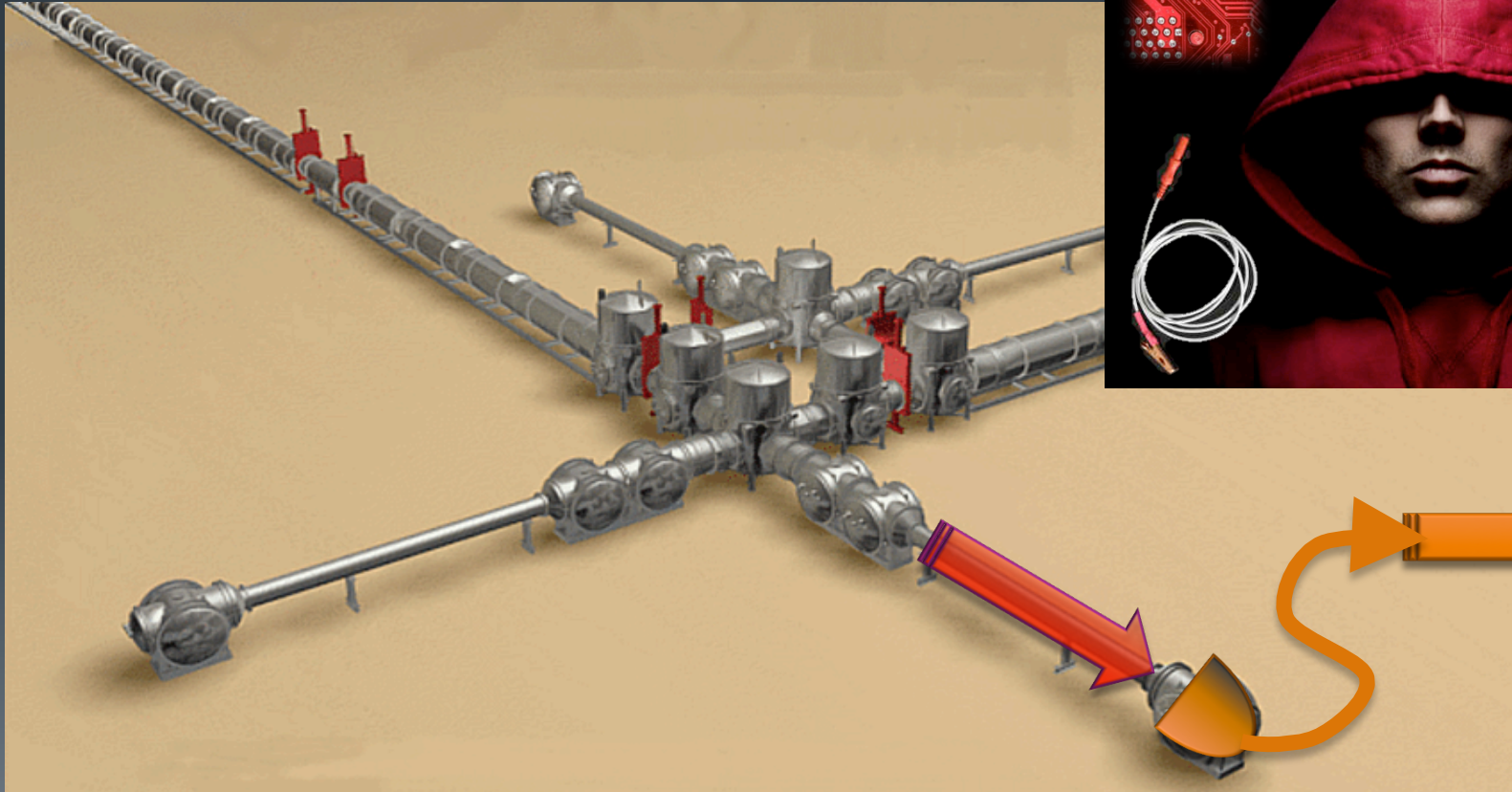


Data Storage



# Analog Hacks

Interferometer

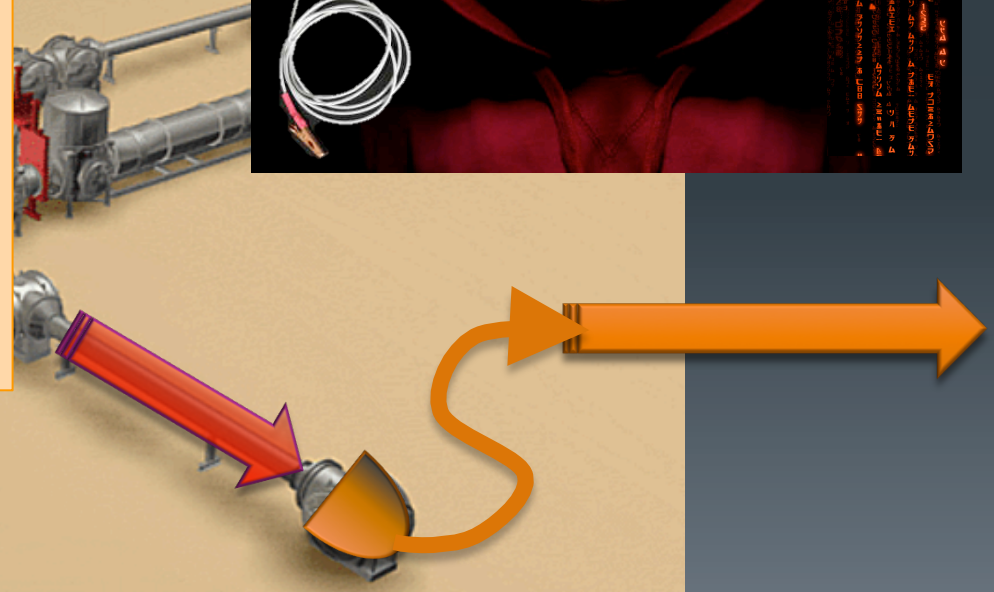


# Analog Hacks

## Interferometer

### Analog Hack Requirements:

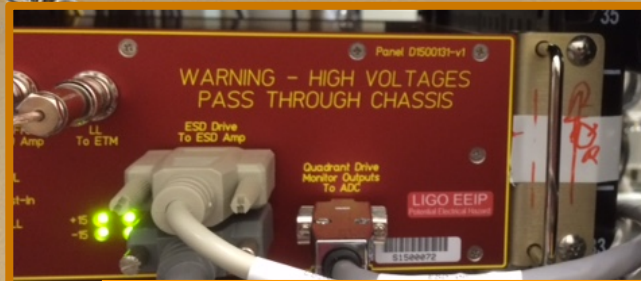
- 1) free access to VEAs at both sites
- 2) in-depth knowledge of the interferometer electronics (e.g., schematics)
- 3) sufficient understanding of electronics and/or mechanical systems to invert the DARM coupling
- 4) programmable injection devices with millisecond absolute timing resolution
- 5) production and filtering of time-domain CBC waveforms





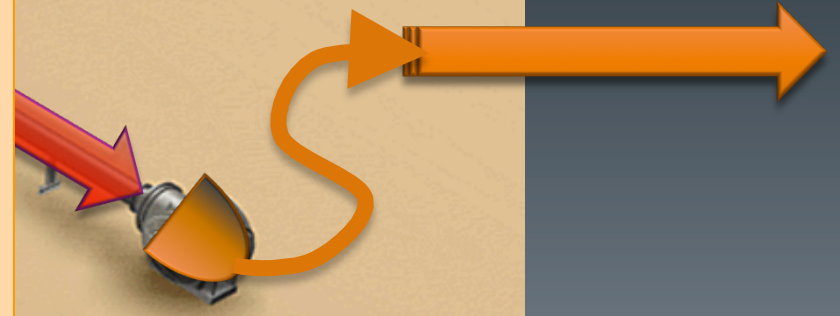
# Analog Hacks

## Interferometer



### Analog Hack Concealment:

- 1) All electronics racks were inspected and photographed after the event. Nothing suspicious was found.
- 2) VEAs have card readers on the doors and entries are logged (better at H1 than L1). No unauthorized entries were made. PEM sensors can also be used to reveal activity.
- 3) Sensitive electronics will be inspected internally after the run, in the meantime they have been sealed.





## Detailed Example: The Electrostatic Drive Test Inputs

- The ESDs (which push on the interferometer test masses) have test inputs which could be used to inject a signal
  - An injection at this point would escape our monitors (not obvious)
- Here is how this “obvious” analog hack would go
  - write an app for your favorite mobile audio device (e.g., iPod) which can output a pre-computed waveform with good timing accuracy
  - produce desired CBC waveforms and filter them to invert the ESD response. (They are different between H1 and L1, with the differences noted only in the aLOG, but anyway...)
  - travel to both sites, or recruit conspirators, to plant the injection devices (“iPods”). (There are very few people who travel to both sites and spend long hours in the VEAs.)



## Detailed Example: The Electrostatic Drive Test Inputs (2)

- place the iPods inside of the drivers
  - If you just plug in to the front you get caught in the post-event inspection, and you can't get in to remove the device without being caught since VEA entries are recorded.
  - Since you are opening the boxes, you will need time when nothing is on to disconnect the ESD and remove it from the rack. A few hours of alone time in the VEA should do, but it will be hard to do this unnoticed (unless you work there).
- find an opportune time to remove the iPods
  - The electronics have been photographed and sealed, so you will need to either do a very careful reconstruction or recruit more conspirators.
  - At least a few more hours alone with the electronics will be required to leave an undisturbed looking scene

**This is the EASIEST hack I can think of, and I don't know anyone who could do it all.**

# No Analog Hacks

- This kind of operation would require a multi-person inside job in order to
  - cover both observatories
  - have the full range of skills required
  - avoid discovery



One might wonder why some think the “perfection” of GW150914 suggests that it is a fake. Which has a better track record, hardware injections or GR? If it didn’t match GR, wouldn’t we be *more* suspicious?

## Conclusion

- While several kinds of hacks seem plausible when first considered, careful investigation reveals many challenges
- The LIGO data flows from the interferometers into a digital system with a great deal of redundancy
- As the signal moves farther from the source both security and redundancy grow, making spoofing essentially impossible
- Closer to the source the signal is protected by the natural complexity of hardware systems, as well as layers of physical security
- Meticulous investigations have revealed no evidence of tampering
- We can’t say that faking GW150914 was impossible, but we can say that faking it would have required an internal conspiracy of our most knowledgeable people



# References

- Frame spoofing
  - see EVNT logs [11383](#), [11376](#) and [11325](#) (11196, 11198, [11376](#))
- Double Blind Injections
  - see [T1500536](#) (DARM), [T1500541](#) (CDS), [T1500544](#) (ESD Mon)
  - see EVNT logs [11253](#), [11288](#), [11267](#), and [11414](#) (11195, 11209, 11258, 11268, 11273, 11274, 11288, 11308, [11335](#), 11336)
  - Easter Eggs, see 11260, 11266, 11318, 11329, [11330](#)
- Analog Hacks
  - see [T1500514](#) (IFO), [L1500138](#) (Site), [L1500139](#) (Inspection)
  - access and inspection logs 11214, 11232, 11313, 11317, 11323, [11382](#), [11432](#)