

Alex Hidalgo (@ahidalgosre)
Squarespace Site Reliability Engineering

- Earthquakes, Forest Fires
and Your Next
Production Incident

Saturday, September 27, 1970

Mount Laguna, California

● THE LAGUNA FIRE

- Third largest recorded California fire at the time
- Spread over 30 miles in just 24 hours

● THE LAGUNA FIRE

○ Impact:

- 175,425 acres of woodland
- 382 residences
- 16 humans

1970 CALIFORNIA FIRE SEASON:
576,508 ACRES
722 BUILDINGS
> \$1.5B IN DAMAGES





Alex Hidalgo

@ahidalgosre
alex-hidalgo.com

SRE @ Squarespace



The 1970 California
fire season was one
of the worst on
record.

● CHANGES IMPACT EVERYTHING

- New land-use legislation
- The Wilderness Act of 1964
- A growing population

○ **CHANGES EMIT CHANGES**



• NO GRAY WOLVES

- Elk less likely to move around
- Ate the same willow plants to the ground
- Beavers didn't have their supplies

Thursday, January 12, 1995

Reintroduction of Gray Wolves

• WITH GRAY WOLVES

- Elk more likely to move around
- Willows left more intact
- Beavers have supplies

MORE WOLVES =

MORE BEAVERS =

WATERSHED CHANGES

○ **BACK TO FOREST FIRES**

● CHANGES EMIT CHANGES

- New land-use legislation
- The Wilderness Act of 1964
- A growing population
- More responding agencies

Fall of 1970

A meeting of the minds

● RESPONDING AGENCIES MEET

○ Problems:

- Terminology differences
- Containment techniques
- Organizational structures
- Poor communications

92nd Congress of the US, 1971

Funding approved

FIRESCOPE

Firefighting
Resources of
Southern
California
Organized for
Potential
Emergencies

● SERIOUS RESEARCH COMMENCES

- Studies!
- Research!
- More studies!
- Collaboration!
- Feedback from others!

● AFTER LOTS OF RESEARCH

- Concluded requirements:
 - Formalized communications
 - Formalized hierarchies
 - Formalized response
 - No more freelancing!!!



Research continued
for many, many
years...

Fire Season, 1978

The Incident Command System is used

● SUCCESS!

○ As time progressed, ICS was adopted for:

- Other forest fires
- HAZMAT situations
- All natural disasters
- Urban Search & Rescue

Monday, November 25, 2002

ICS is mandatory

“

“Why do I care about any of this?”



The tech industry is hurtling towards adopting known processes instead of continuing to invent our own.

● ALMOST NOTHING IS NEW

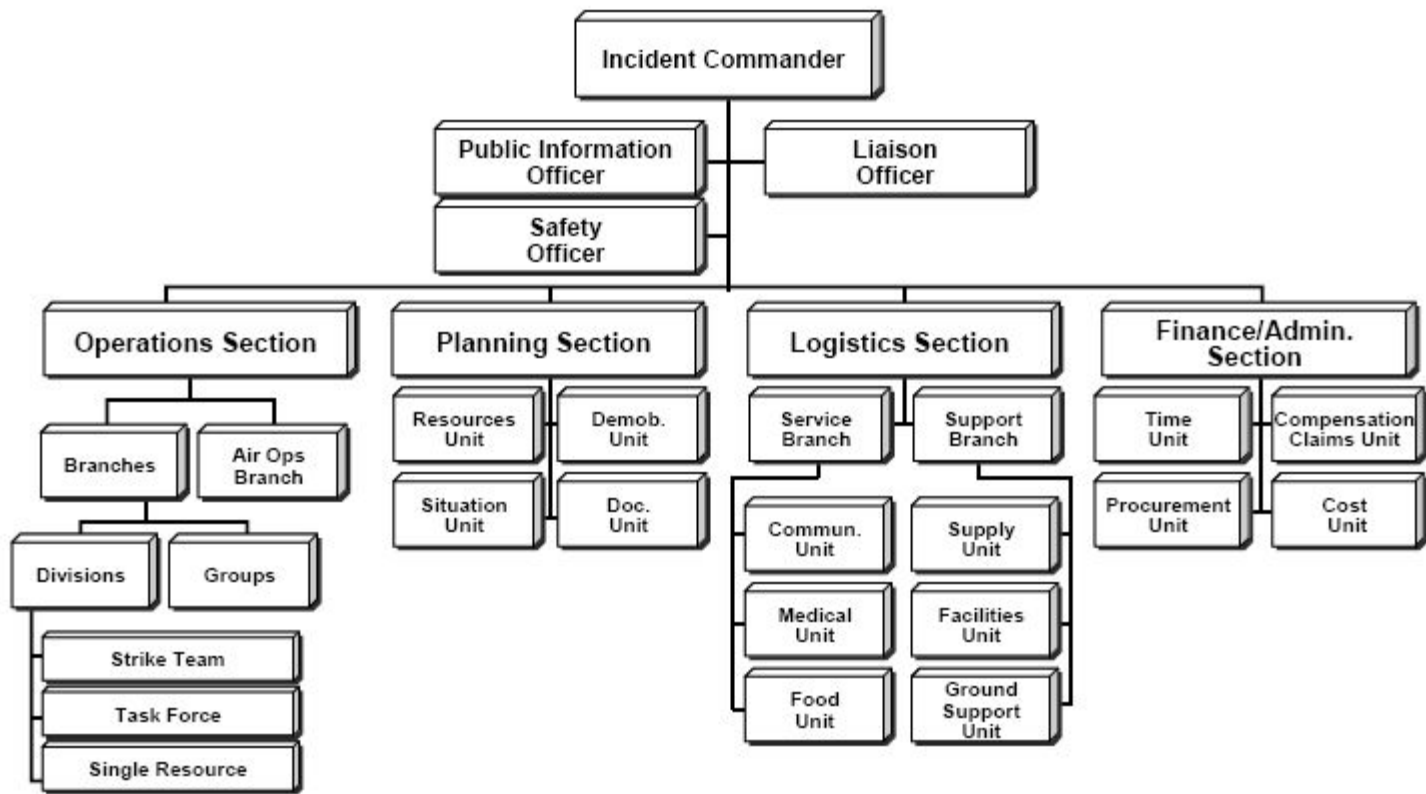
- Engineers have been focused on reliability for as long as humans have been building stuff
- Statisticians have been analyzing data for centuries
- The ICS has been around for decades

PROBLEMS THE ICS ADDRESSES

(that probably apply to you)


- Lack of insight
- Poor communications
- No established hierarchy
- Too much freelancing

○ It's gotten complicated...



“

“How can I use the ICS?”



Just one example of how
this might work...

- **A Easy And Effective ICS**
(for computer things)

INCIDENT
COMMANDER



● INCIDENT COMMANDER (IC)

- In charge of the incident and holds all high-level state about it
- This is the only role that must always exist during any incident response
- Is responsible for delegating other roles to other engineers

● INCIDENT COMMANDER (IC)

- If the other roles have not been delegated, it should be assumed the IC is also fulfilling those roles
- The role of IC can and perhaps should be handed off

INCIDENT
COMMANDER



OPERATIONS
LEAD



● OPERATIONS LEAD

- In charge of making changes to the system in order to mitigate or resolve the problem
- No one else should be touching the production besides the OL
- Often is the original responder

● OPERATIONS LEAD

- Actions taken should be documented in a command post
- This role is delegated, not free for anyone to pick up

● COMMAND POST

- Establish a clearly defined communications channel
- New or old is fine
- Text is preferred over voice
- IC should feel free to police this channel as much as needed

INCIDENT
COMMANDER



OPERATIONS
LEAD



COMMUNICATIONS
LEAD



• COMMUNICATIONS LEAD

- Responsible for all communications, both internally and externally
- Should be the only one updating things like your status page

• COMMUNICATIONS LEAD

- May also be a good option for keeping up an Incident State Documents (ISD)
- This role is delegated, not free for anyone to pick up

● INCIDENT STATE DOCUMENTS

- Used to consolidate the current state of the world
- Documents which roles have been defined and who currently has them
- Templates are good (tooling, too!)

○ `/copy` is a neat hack

**INCIDENT
COMMANDER**

```
graph TD; IC[INCIDENT COMMANDER] --> OL[OPERATIONS LEAD]; IC --> PL[PLANNING LEAD]; IC --> CL[COMMUNICATIONS LEAD];
```

**OPERATIONS
LEAD**

**PLANNING
LEAD**

**COMMUNICATIONS
LEAD**

● PLANNING LEAD

- In charge of supporting the other leads as needed
- Others Leads are focused on an immediate fix, the Planning Lead may be focused on future
- Responsible for finding new engineers

● PLANNING LEAD

- Support could extend as far as ordering dinner or fetching coffee
- This role is delegated, not free for anyone to pick up

ICS AND FLEXIBILITY

- The ICS has been deliberately designed to be able to expand and contract
- Make it work for *you*, don't just listen to me

- **An example of expansion**

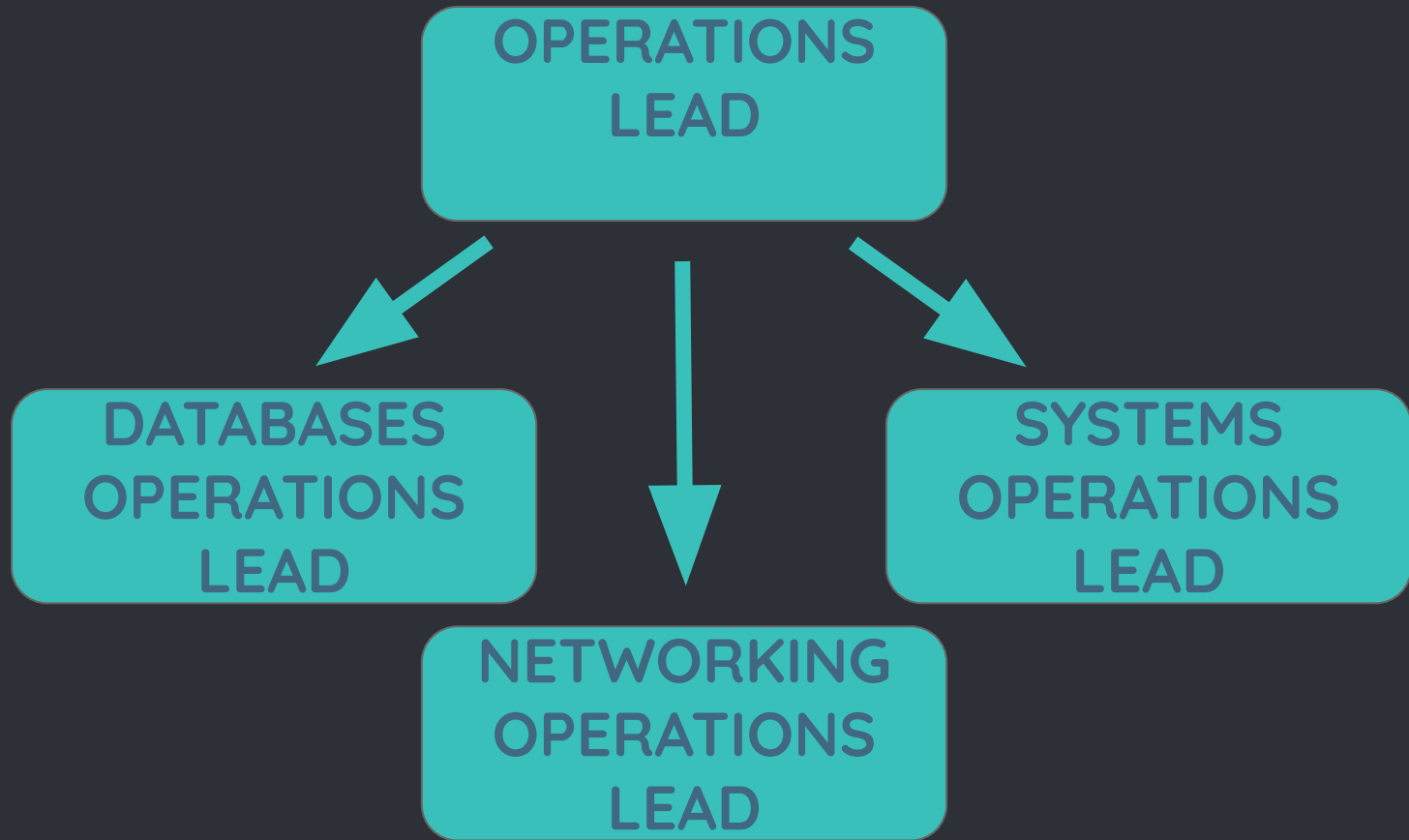
**INCIDENT
COMMANDER**

```
graph TD; IC[INCIDENT COMMANDER] --> OL[OPERATIONS LEAD]; IC --> PL[PLANNING LEAD]; IC --> CL[COMMUNICATIONS LEAD];
```

**OPERATIONS
LEAD**

**PLANNING
LEAD**

**COMMUNICATIONS
LEAD**



- **Handing off is important**

INCIDENT
COMMANDER 1



INCIDENT
COMMANDER 2



INCIDENT
COMMANDER 1



INCIDENT
COMMANDER 2

INCIDENT
COMMANDER 2



INCIDENT
COMMANDER 1

INCIDENT
COMMANDER 2



“

“Am I having an incident?!?”


● IS THIS AN INCIDENT?

- If you're wondering if it is, it probably is
- It's easier to declare an incident for something that turns out to be small than it is to apply the framework to an incident after time has passed

● IS THIS AN INCIDENT?

- Do not try to hide an incident.
- Stuff breaks! It's just how it is!

○ The ICS works... mostly...

An aerial photograph showing a residential neighborhood completely inundated with floodwater. The houses, with their brown and grey roofs, are surrounded by deep water. Some trees and debris are visible in the water. The text is overlaid in the upper center of the image.

2005: HURRICANE KATRINA
80% OF NOLA FLOODED
1826 DEATHS
> \$125B IN DAMAGES

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

**A Performance Review of FEMA's Disaster
Management Activities in Response to
Hurricane Katrina**



Office of Inspections and Special Reviews

OIG-06-32

March 2006

“

“The federal government, in particular the Federal Emergency Management Agency (FEMA), received widespread criticism for a slow and ineffective response to Hurricane Katrina. Much of the criticism is warranted.”

https://www.oig.dhs.gov/assets/Mgmt/OIG_06-32_Mar06.pdf

● LOTS WENT WRONG

○ Final lessons:

- Anticipate
- Train
- Test

● ANTICIPATE

- Incidents will occur.
- Make sure your version of the ICS is ready and documented

● TRAIN

- Develop workshops and training sessions
- Provide tooling and templates
- Conduct meaningful incident retrospectives and share them widely

● TEST

- Run test scenarios
- Use chaos engineering
- Operational underload can be as dangerous as operational overload



Have an Incident Commander

Delegate all roles and enforce them

Establish a command post

Communicate and document incident state

Expand and contract at will

Hand-off regularly

Test and train your processes and procedures

Use the ICS, because,
mostly, the ICS works.

Thank you!

Alex Hidalgo -  @ahidalgosre
alex-hidalgo.com

Shout Outs:

Squarespace Engineering

LFI Slack

Slidesgala.com