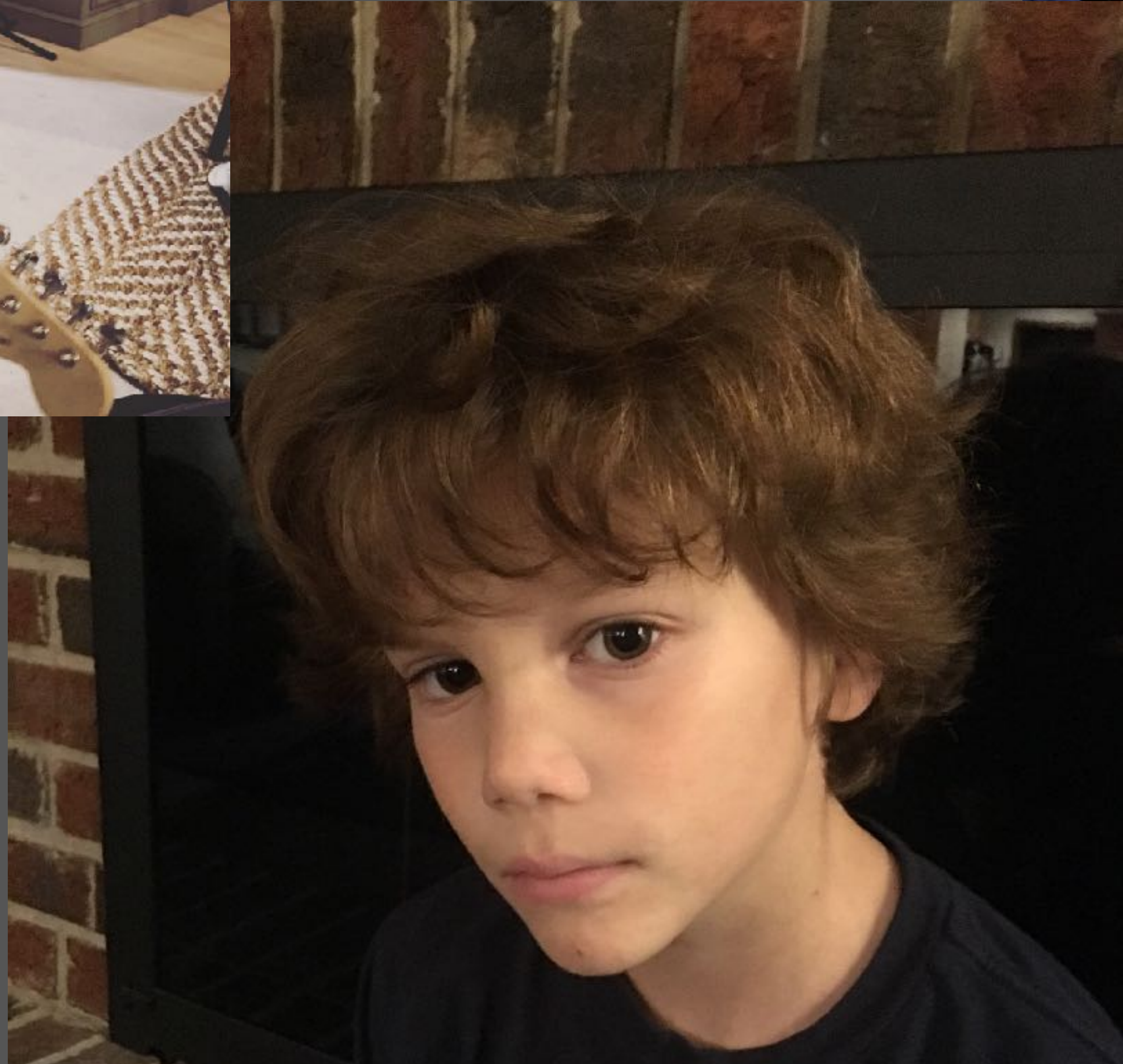


pagerduty

Incidents & Accidents

Matty Stratton, DevOps Evangelist, **PagerDuty**



**Disclaimer, part the first:
Learn from other industries,
do not take on their stresses.**

**Disclaimer, part the second:
This is a topic with a surprisingly
large number of details.**



PEACETIME

WARTIME



NORMAL

EMERGENCY



OK

NOT OK

Before, during, after




Before

**Have criteria defined for when to
have and not have a call.**

Any unplanned disruption or degradation of service that is actively affecting customers' ability to use the product.

**Post incident criteria widely.
Don't litigate during a call.**

Severities

Severity	Description
 SEV-1	<ul style="list-style-type: none">• SEV-2 co minutes.
 SEV-2	<ul style="list-style-type: none">• Notificati• Notifi• acco• Web• know• An event<ul style="list-style-type: none">• i.e. an• i.e. th• Configura• Custome• Problemsthe pdt-c
 SEV-3	<ul style="list-style-type: none">• Notificati• Email eve• Sales pip<ul style="list-style-type: none">• Marke• Signu• Configurasignifican• Configura

**Monitor the business criteria,
and act accordingly.**

People are expensive.

Practice still makes perfect.

“Know your role”

**Have a clear understanding
of who is supposed to be
involved in each role.**



NATIONAL INCIDENT MANAGEMENT SYSTEM

December 2008

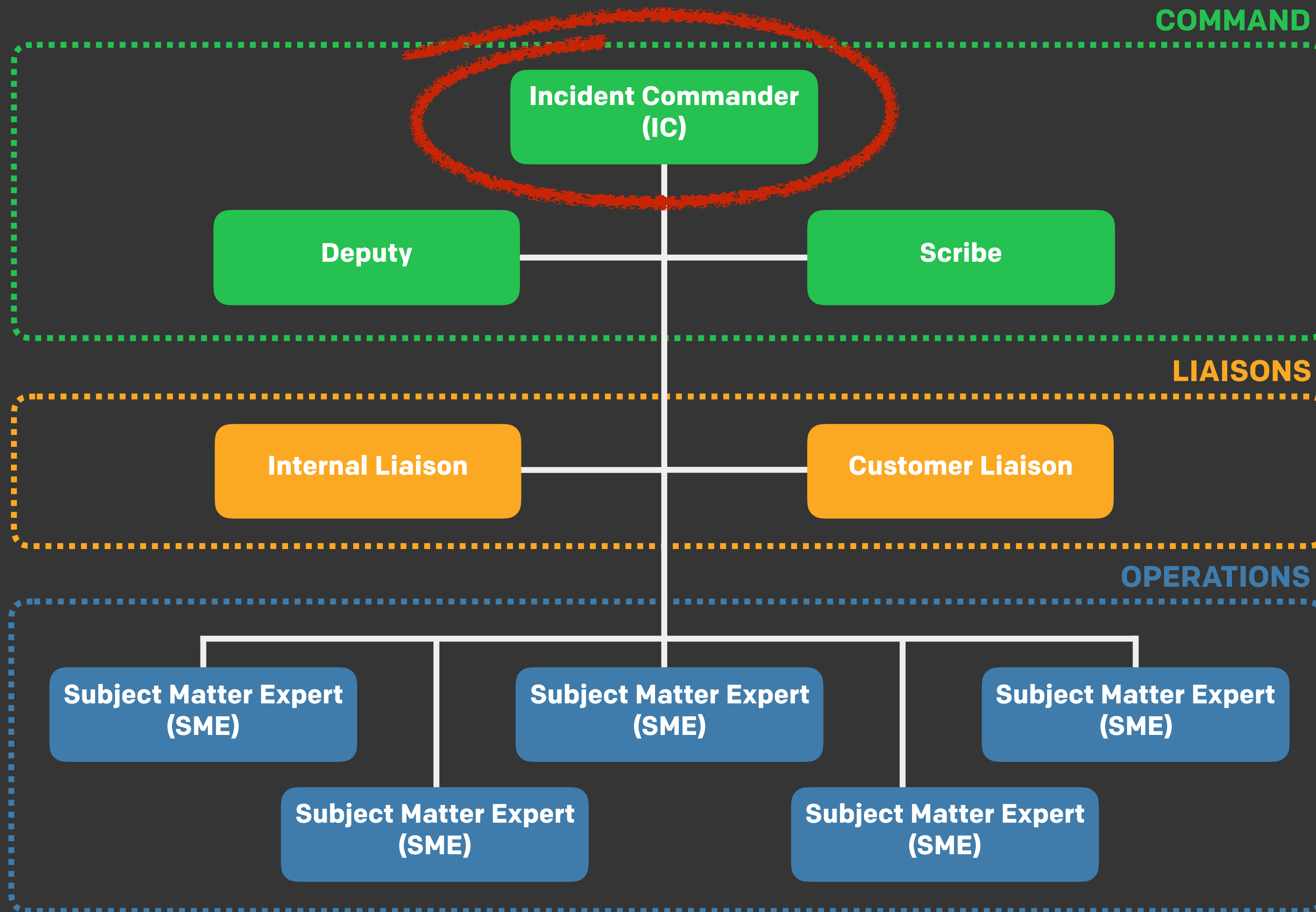
<https://www.fema.gov/national-incident-management-system>



 @mattstratton

- “National Incident Management System” (NIMS)
- Incident Command System (ICS).
- Standardized system for emergency response.
- Hierarchical role structure.
- Provides a common management framework.
- Originally developed for CA wildfire response.

pagerduty



During



I'm Matty.

I'm the Incident Commander.

Single source of reference.

Becomes the highest authority.

(Yes, even higher than the CEO)

**Not a resolver.
Coordinates and delegates.**



Let's get the IC on the RC, then get a BLT for all the SME's.

Clear is better than concise.

**The IC manages the
flow of conversation.**



What's wrong?



What actions can we take?



What are the risks involved?

“Can someone...”



Rich, I'd like you to investigate the increased latency, try to find the cause. I'll come back to you in 5 minutes. Understood?

Understood.



Humor is best in context.

DT5: Roger that

GND: Delta Tug 5, you can go right on bravo

DT5: Right on bravo, taxi.

(...): Testing, testing. 1-2-3-4.

**GND: Well, you can count to 4. It's a step in the right direction.
Find another frequency to test on now.**

(...): Sorry

**Have a clear roster
of who's been engaged.**

Rally fast, disband faster.

**Have a way to contribute
information to the call.**

**Have a clear mechanism for
making decisions.**

“IC, I think we should do X”
**“The proposed action is X,
is there any strong objection?”**

**Capture everything, and call out
what's important now vs. later.**

**“One last thing...”
(Assign an owner at the
end of an incident)**

After

**“After action reports”,
“Postmortems”,
“Learning Reviews”**

**The impact to people is a part of
your incident review as well.**

**Record incident calls,
review them afterwards.**

**Regularly review the
incident process itself.**

Have structure in place beforehand

Practice, practice, practice

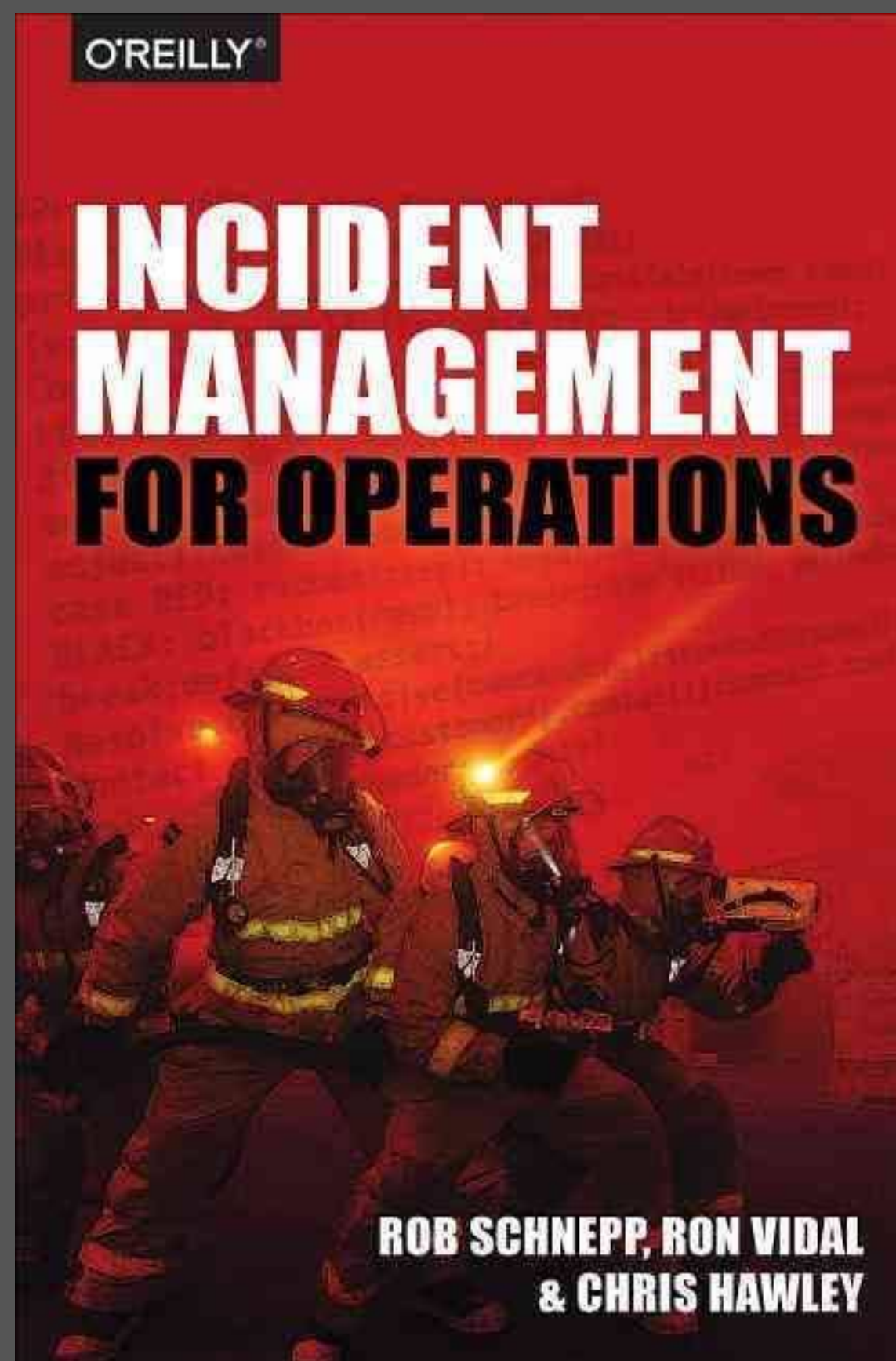
Have clearly delineated roles

Manage the conversation flow

Make clear decisions

Rally fast, disband faster

Review regularly



**Don't panic.
Stay calm.
Calm people stay alive.**



<https://response.pagerduty.com>

 REPO  67  417

Home

Getting Started

On-Call

Being On-Call

Who's On-Call?

Alerting Principles

Before an Incident

What is an Incident?

Severity Levels

Different Roles

Call Etiquette

Complex Incidents

During an Incident

During an Incident



So you want to be an incident commander? You've come to the right place! You don't need to be a senior team member to become an IC, anyone can do it providing you have the requisite knowledge (yes, even an intern)!

Purpose

#

If you could boil down the definition of an Incident Commander to one sentence, it would be,



Take whatever actions are necessary to protect PagerDuty systems and customers.

The purpose of the Incident Commander is to be the decision maker during an major incident; Delegating tasks and listening to input from subject matter experts in order to bring the incident to resolution.

The Incident Commander becomes the highest ranking individual on any major incident call, regardless of their day-to-day rank. Their decisions made as commander are final.

Your job as an IC is to listen to the call and to watch the incident Slack room in order to provide clear coordination, recruiting others to gather context/details. **You should not be performing any actions or remediations, checking graphs, or investigating logs.** Those tasks

Resources:

- Angry Air Traffic Controllers and Pilots - <https://youtu.be/Zb5e4SzAkkI>
- Blameless Post-Mortems (Etsy Code as Craft) - <https://codeascraft.com/2012/05/22/blameless-postmortems/>
- Incidents And Accidents: Examining Failure Without Blame (Arrested DevOps) - <https://www.arresteddevops.com/blameless/>
- PagerDuty Incident Response Process - <https://response.pagerduty.com/>

Thank you!

Questions?