# Synergy between sound and unsound tools

## *It's not sound to have to choose sound or unsound*

**An attempt at the impossible task of giving this topic justice in only 20 min….**

**Just some thoughts to share**

Matt Rhodes

SATE VI, McLean VA

19 September 2019

*“I do not pretend to start with precise questions. I do not think you can start with anything precise. You have to achieve such precision as you can, as you go along.”*

*Bertrand Russell*

The Philosophy of Logical Atomism, p. 49 (1918).

Reflection on the nature of analytic philosophy.

# Some provisions of both unsound and unsound analysis

## Unsound

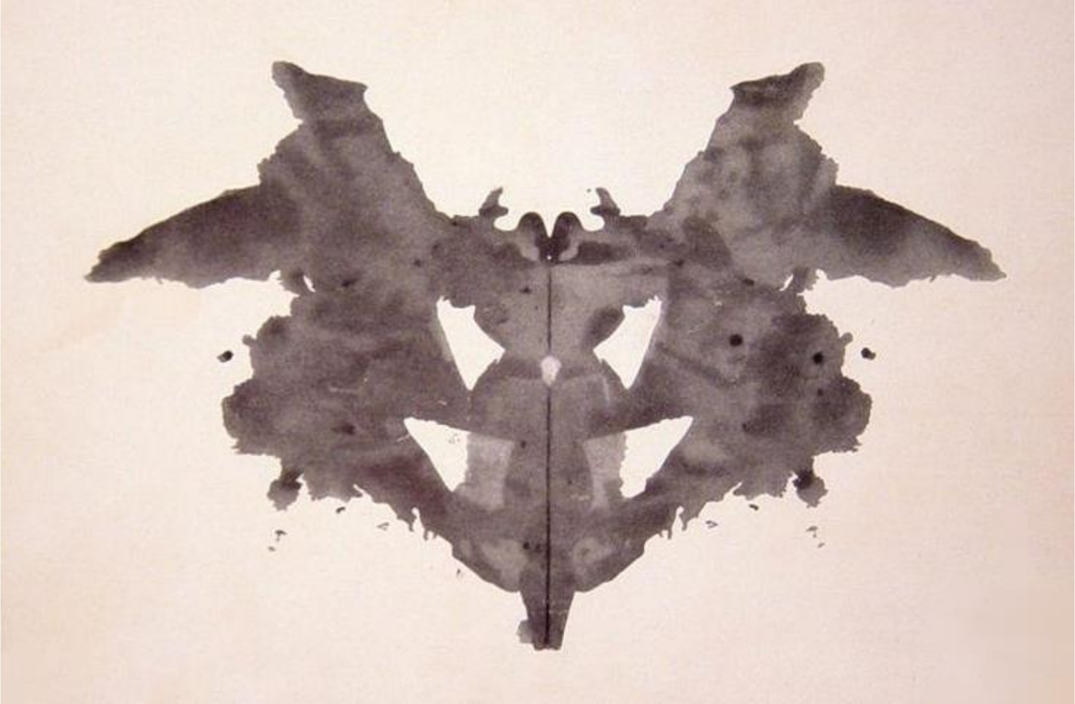
- Speed
- Rules compliance
- Guidance

## Sound

- Confidence
- [Specification] completeness
- Precision

*“The precision of naming takes away from the uniqueness of seeing.”*

*Pierre Bonnard*

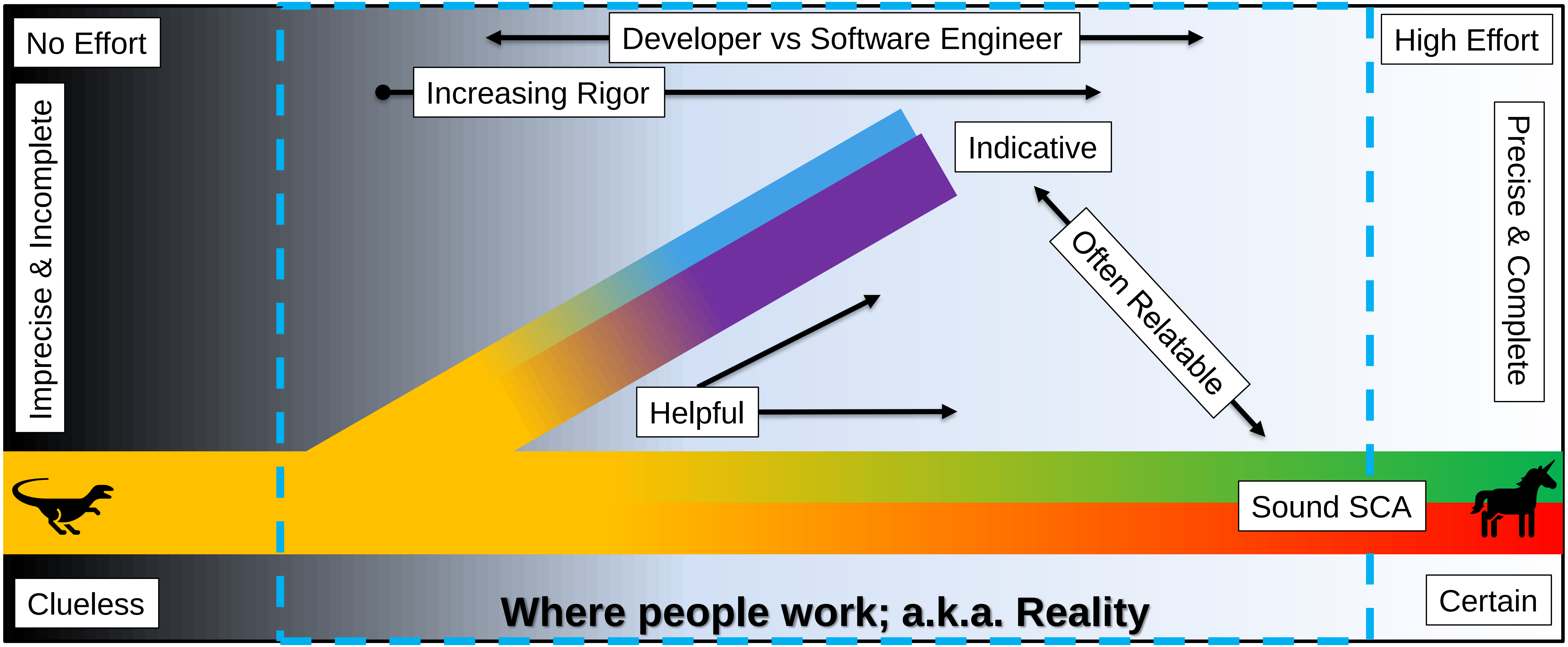


**Hermann Rorschach might suggest the opposite…**

**When it comes to applying SCA, its not simply a question of sound or unsound. There are many dimensions to applying each. It’s a very complex and imprecise spectrum.**

Image by Hermann Rorschach, died 1922, public domain, sourced from https://en.wikipedia.org/wiki/Rorschach_test#/media/File:Rorschach_blot_01.jpg

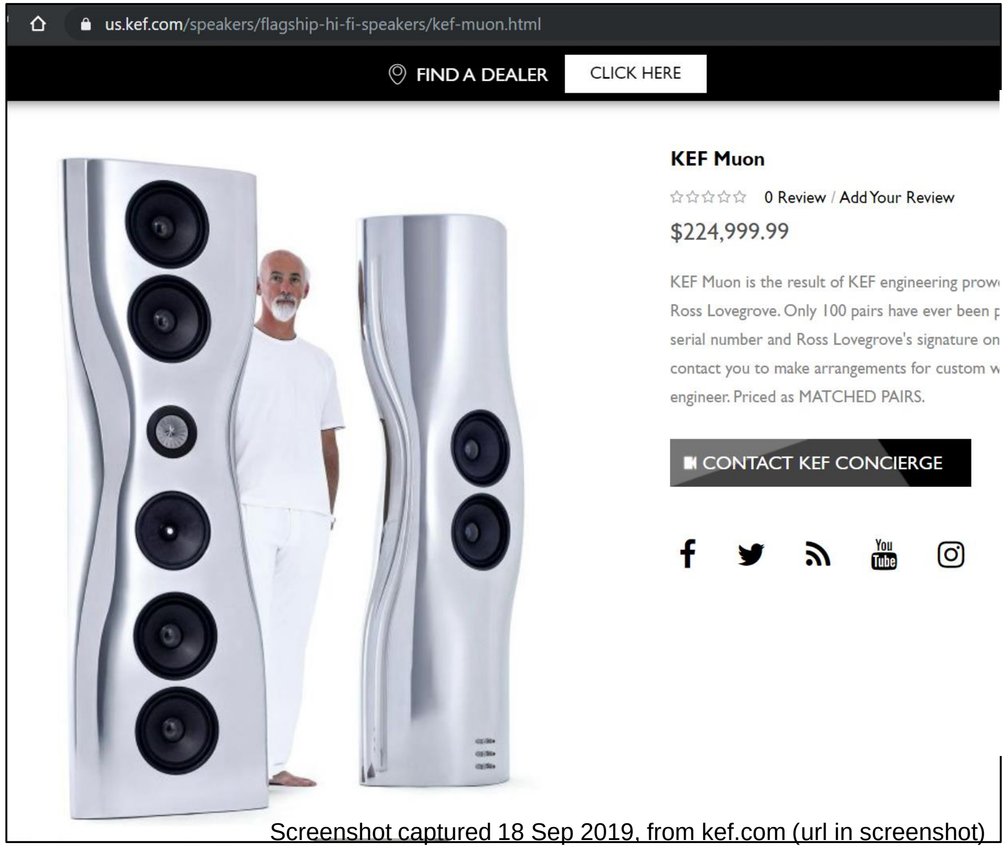
# The complex and imprecise* spectrum of applying SCA



*Try not to think too hard about the flattened depiction of multiple-dimensionality – there are just too many relationships

*“It is the mark of an educated mind to rest satisfied with the degree of precision which the nature of the subject admits and not to seek exactness where only an approximation is possible.”*

*Aristotle*



us.kef.com/speakers/flagship-hi-fi-speakers/kef-muon.html

FIND A DEALER CLICK HERE

**KEF Muon**

☆☆☆☆☆ 0 Review / Add Your Review

$224,999.99

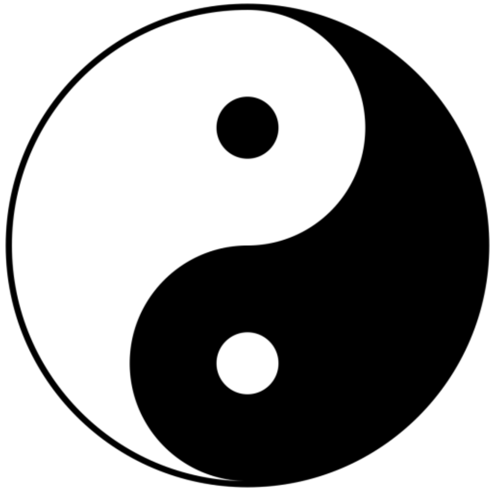
KEF Muon is the result of KEF engineering prow
Ross Lovegrove. Only 100 pairs have ever been p
serial number and Ross Lovegrove's signature on
contact you to make arrangements for custom w
engineer. Priced as MATCHED PAIRS.

CONTACT KEF CONCIERGE

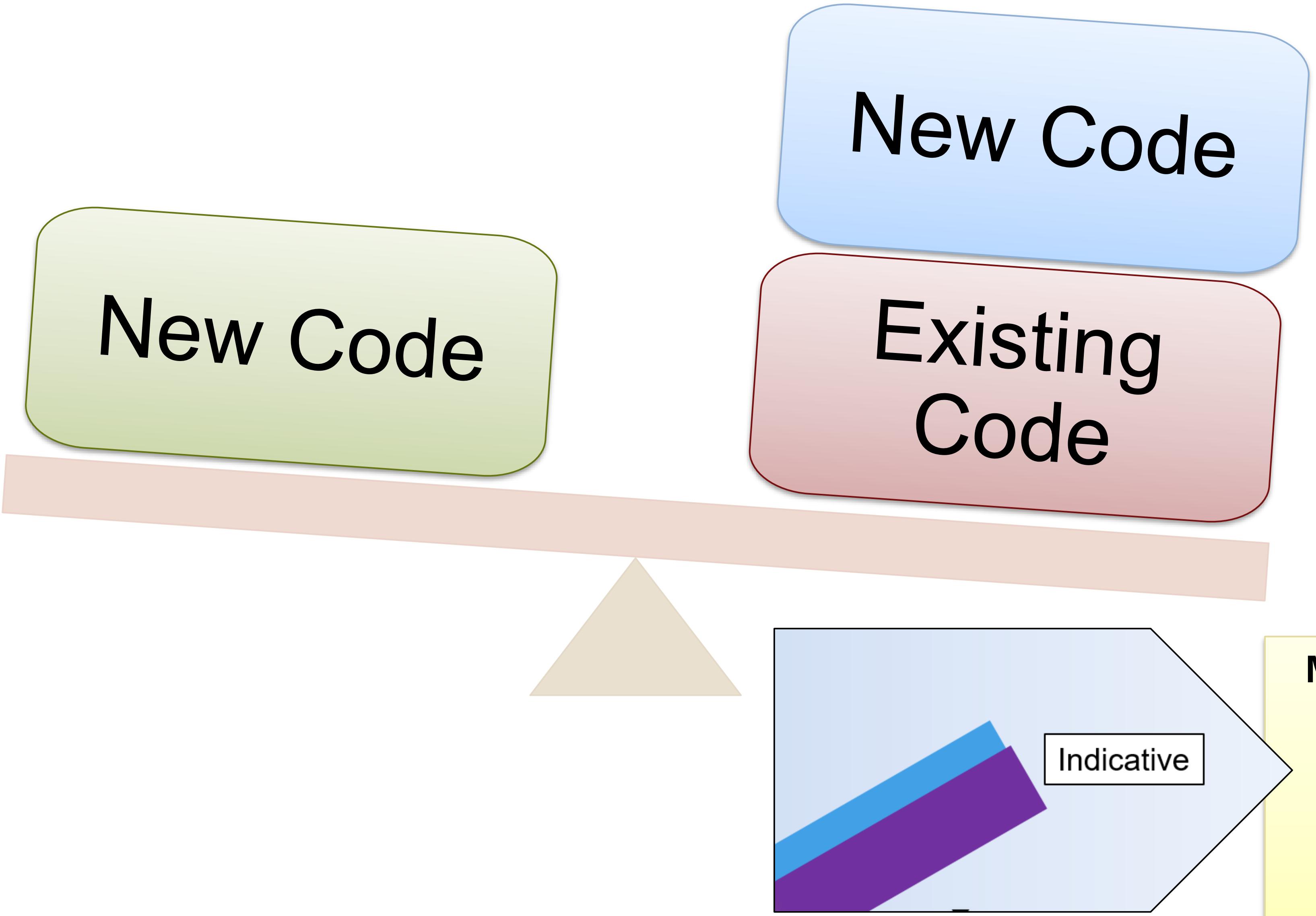
Screenshot captured 18 Sep 2019, from kef.com (url in screenshot)

[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

# Process Yin & Yang with SCA



# Starting points matter!



Most of our users find it easiest to start with the unsound tool on existing code

# Efficiency, IFF Speed + Confidence

**Speed and low false positives alone do not provide efficiency.**

**Lack of confidence is high risk gambling: losing is inefficient.**

{ INSERT YOUR OWN FAMOUS SOFTWARE ERROR HERE }

**Or increase your confidence so you don’t have to...**

# General Guidance: Tuning your process for efficiency

## Goal 1

- Achieve speed for the probable issues and necessary compliance

## Goal 2

- Minimize the noise (Its not just about False Positives )

## Goal 3

- Provide the means to achieve the confidence needed/desired

## Goal 4

- Leverage unsound results to inform the sound results

# Some specific synergy examples

## Sound tools can clean up after unsound tools

- In general: False Positives
- MISRA 10.x rules – essential type model

## Informing sound results with unsound

1. Sound tool provides finding of a potential buffer overflow
2. Unsound tool provides a tainted data finding, corroborating exploitability

# From a real user…

*“This is so complete I can get rid of my unit testing!”*