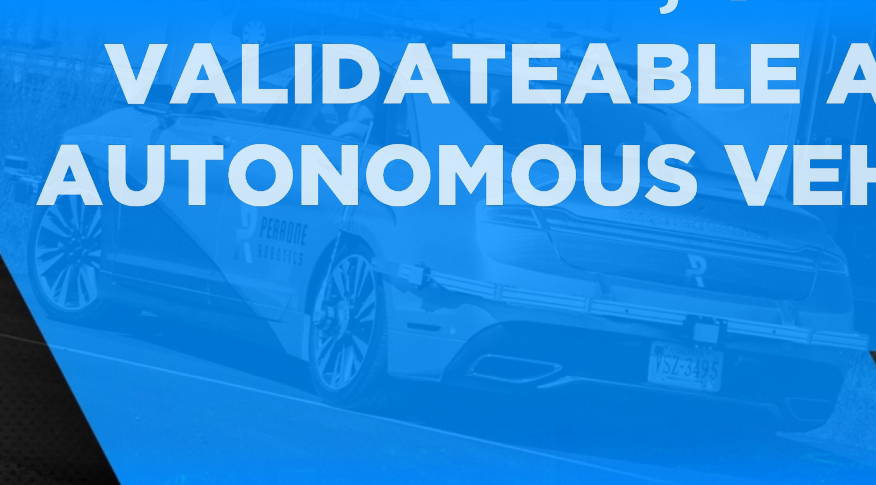
A FLEXIBLE, VERIFIABLE, AND VALIDATEABLE APPROACH TO AUTONOMOUS VEHICLE SAFETY



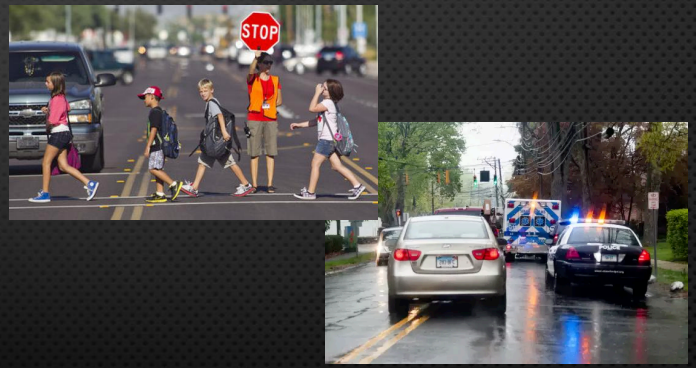
PAUL J. PERRONE

PERRONE ROBOTICS

JANUARY 30, 2021

SAFETY VS CERTIFICATION AXIOMS

SAFETY



SOMETHING CERTIFIED MAY NOT BE SAFER

CERTIFICATION

SOMETHING SAFER MAY NOT BE CERTIFIED

ESPECIALLY TRUE WITH SOFTWARE SYSTEMS

CERTIFICATION HARD TO KEEP UP WITH EXPONENTIAL TECHNOLOGY GROWTH

PERRONE ROBOTICS

COMPLEXITY INCREASE WITH AUTONOMY

A.I.

FULL AUTONOMY

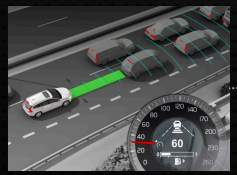
DISTRIBUTED PROCESSING

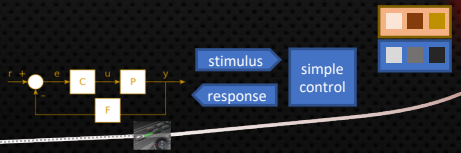
COMPONENTS INCREASE

COMPLEXITY

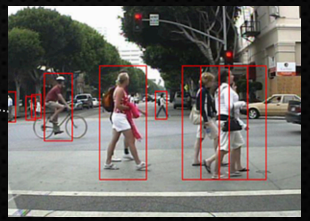
CHASM!

ADAPTIVE CRUISE CONTROL





PEDESTRIAN PERCEPTION, FUSION, & MANEUVERS



0 1 2 3 4 5

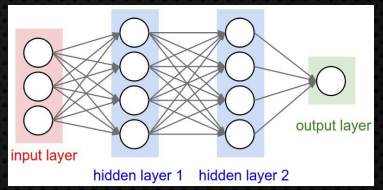
AUTONOMY LEVELS

WORLDS COLLIDING

AUTOMOTIVE CONTROLS

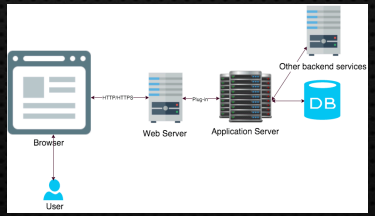
LOW-LEVEL
SIMPLER
EASIER TO V&V

ARTIFICIAL INTELLIGENCE



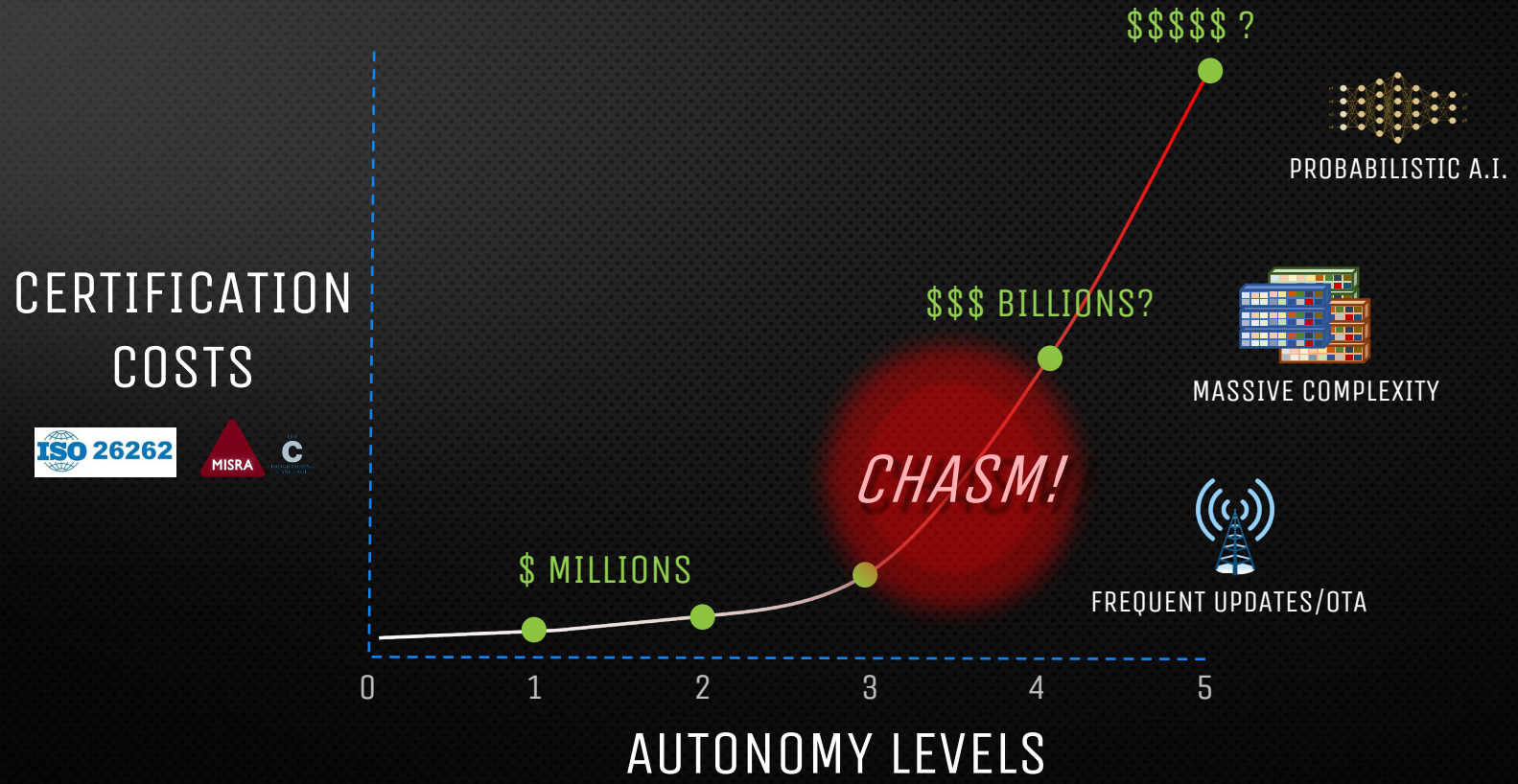
ABSTRACT/PROBABILISTIC-LEVEL
HIGHEST COMPLEXITY
IMPOSSIBLE TO V&V

LARGE SCALEABLE IT SOFTWARE



HIGHER-LEVEL
SCALABLE COMPLEXITY
DIFFICULT TO V&V

NON-SCALING LEGACY CERTIFICATION



SCALING FOR FULL AUTONOMY

ARTIFICIAL INTELLIGENCE

MACHINE LEARNING METHODS
(NEURAL NETWORKS, MARKOV MODELS, RULES)

LARGE SCALEABLE IT SOFTWARE

HIGHER LEVEL PROGRAMMING LANGUAGES
(JAVA, C#, PYTHON, RUBY)

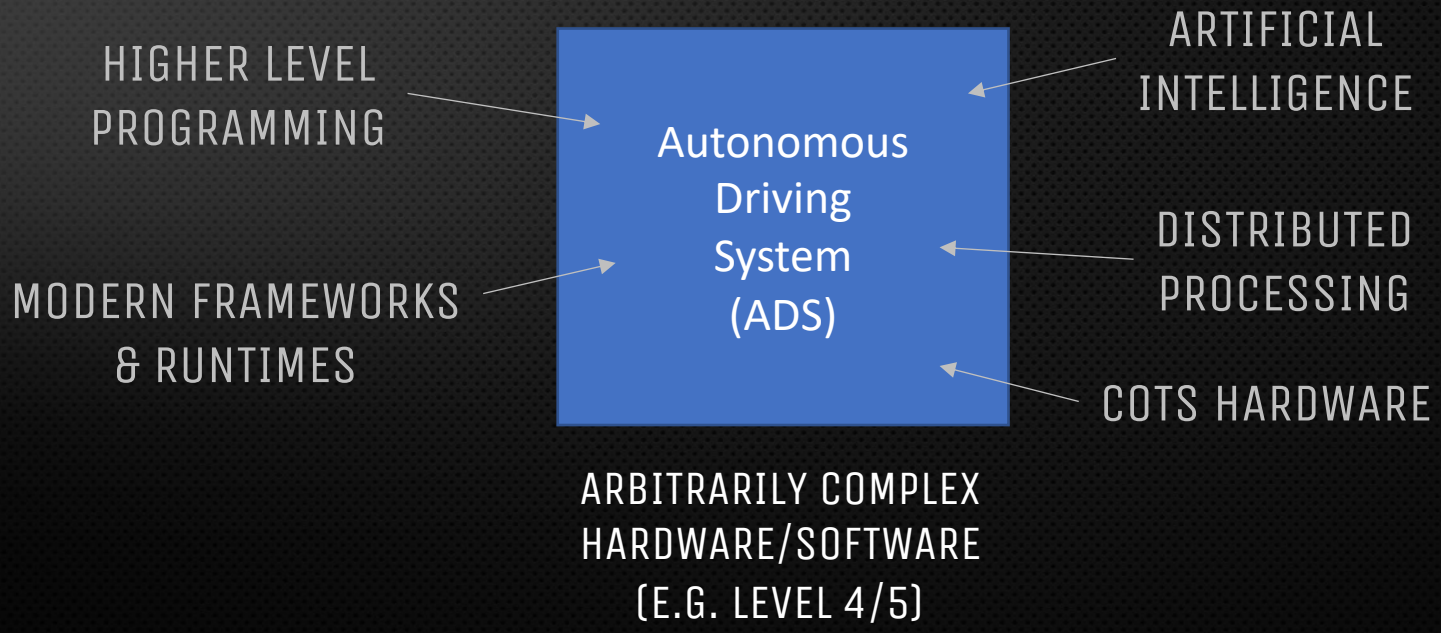
HIGHER LEVEL PROGRAMMING METHODS
(OBJECT-ORIENTED, FRAMEWORKS, MANAGED RUNTIMES)

EMBEDDED-IT INTERSECTIONS

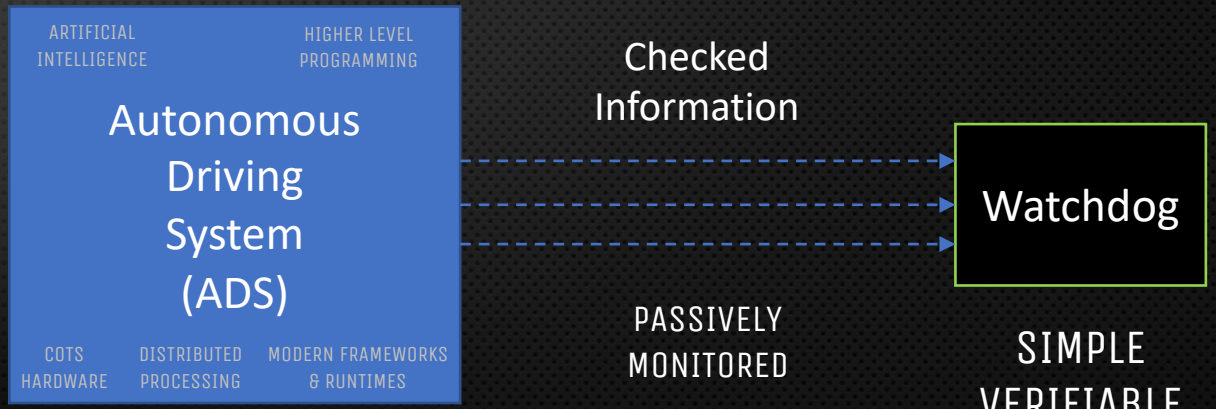
HIGH-LEVEL REAL-TIME PROGRAMMING
(REAL-TIME OS, REAL-TIME JAVA)

PERRONE ROBOTICS

HOW DO WE MAKE THIS SAFE?

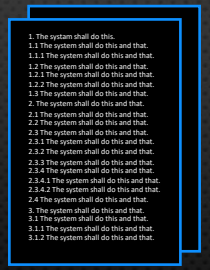


SAFETY WATCHDOG



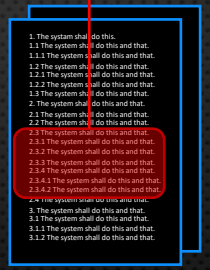
WATCHDOG SPECIFICATION PROCESS

SYSTEM SPECIFICATION



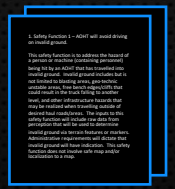
SAFETY ANALYSIS

SAFETY-CRITICAL SPEC SUBSET



SAFETY ANALYSIS

SAFETY FUNCTIONS

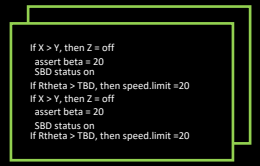


HAZARD ANALYSES, FORMAL METHODS, OR V&V'D METHODS

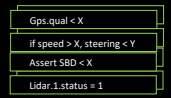
DERIVATION PROCESS

MAPPED V&V'D SAFETY CHECKING FUNCTIONS

MAPPED V&V'D WATCHDOG RULES



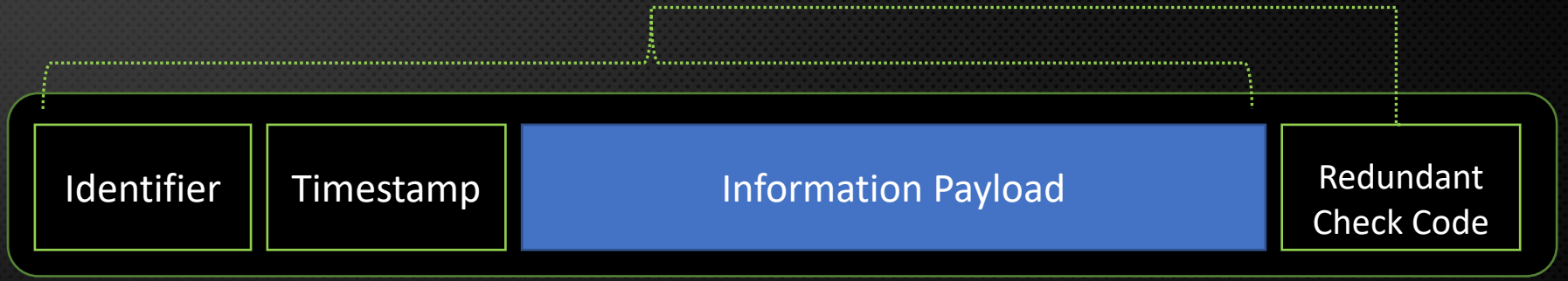
DERIVATION PROCESS



VERIFIABLE & VALIDATEABLE PROCESS

PERRONE ROBOTICS

CODED INFORMATION

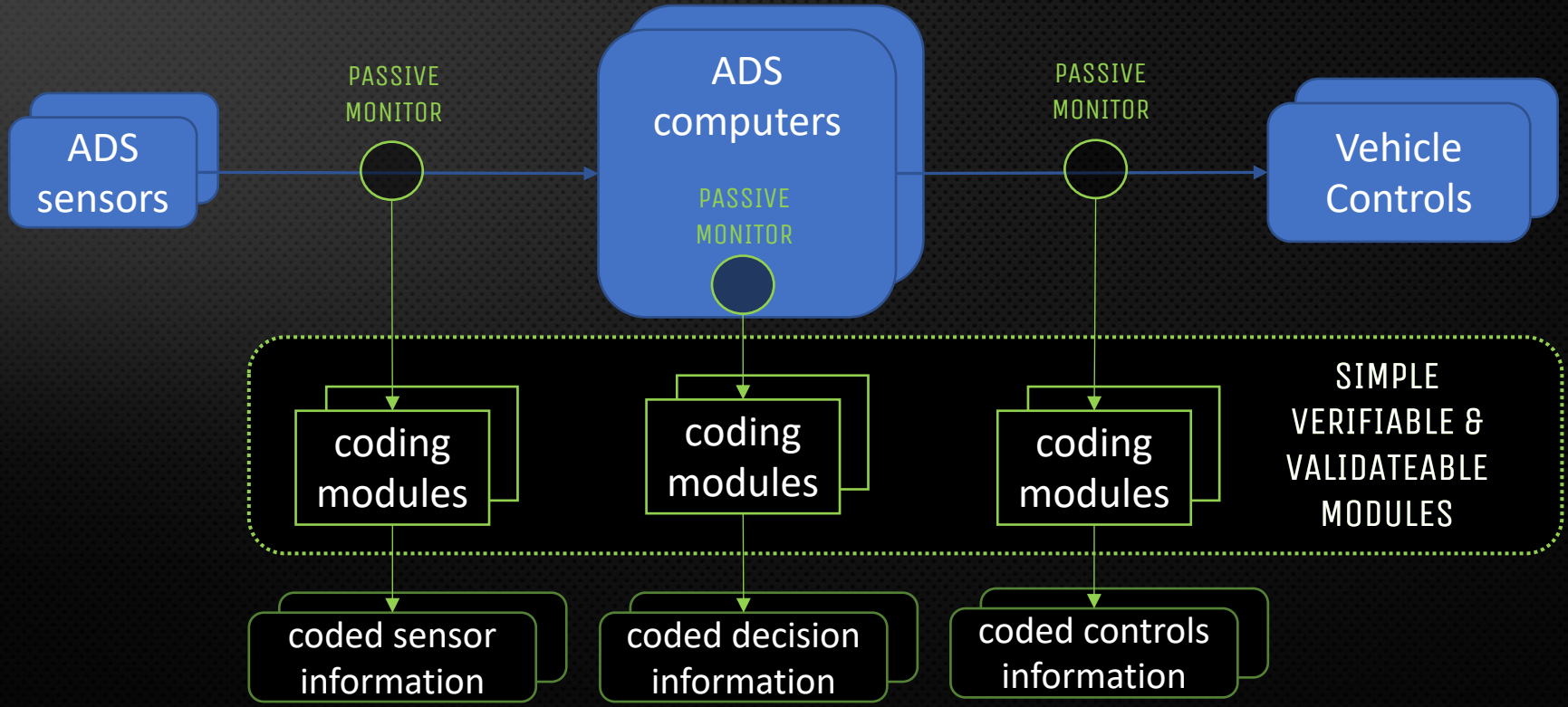


UNIQUELY IDENTIFY INFO

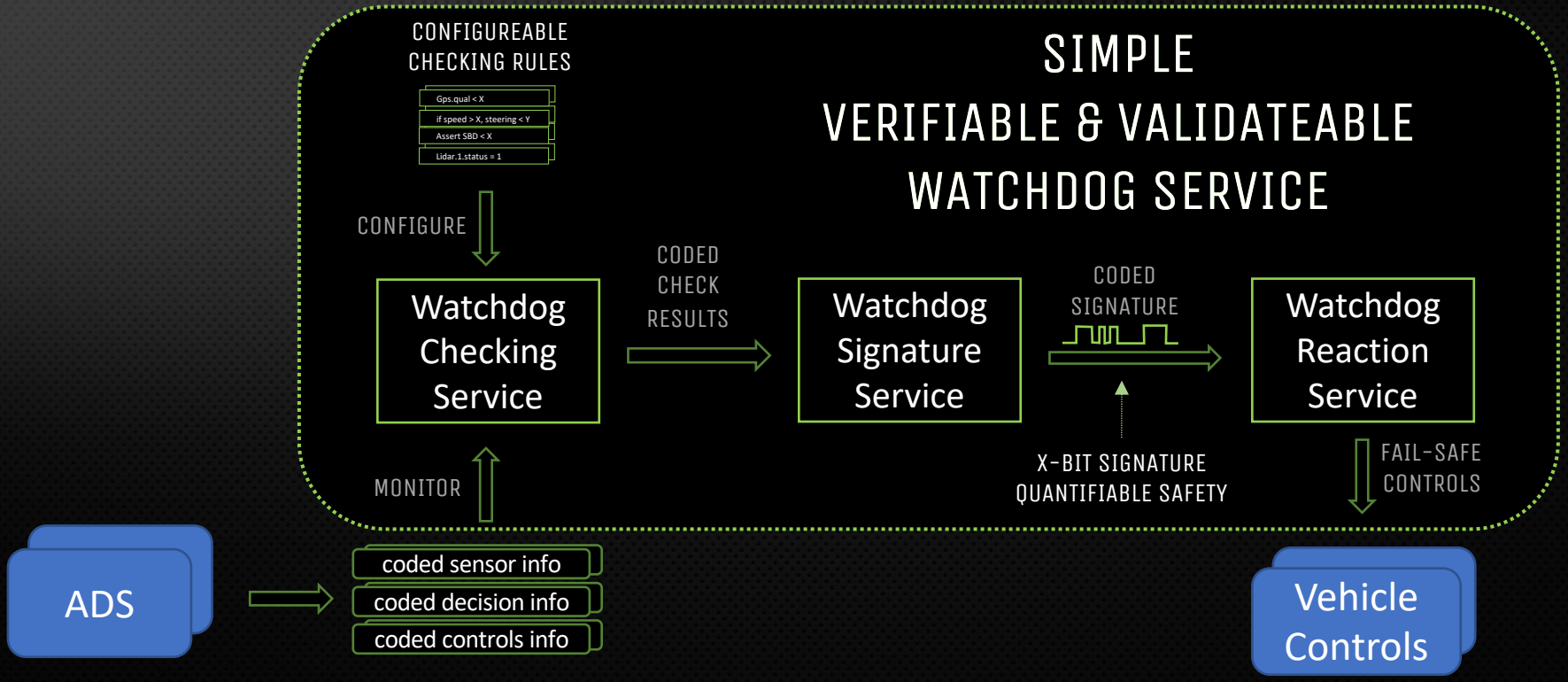
ENSURE INFO "FRESHNESS"

PROTECT AGAINST CORRUPTION

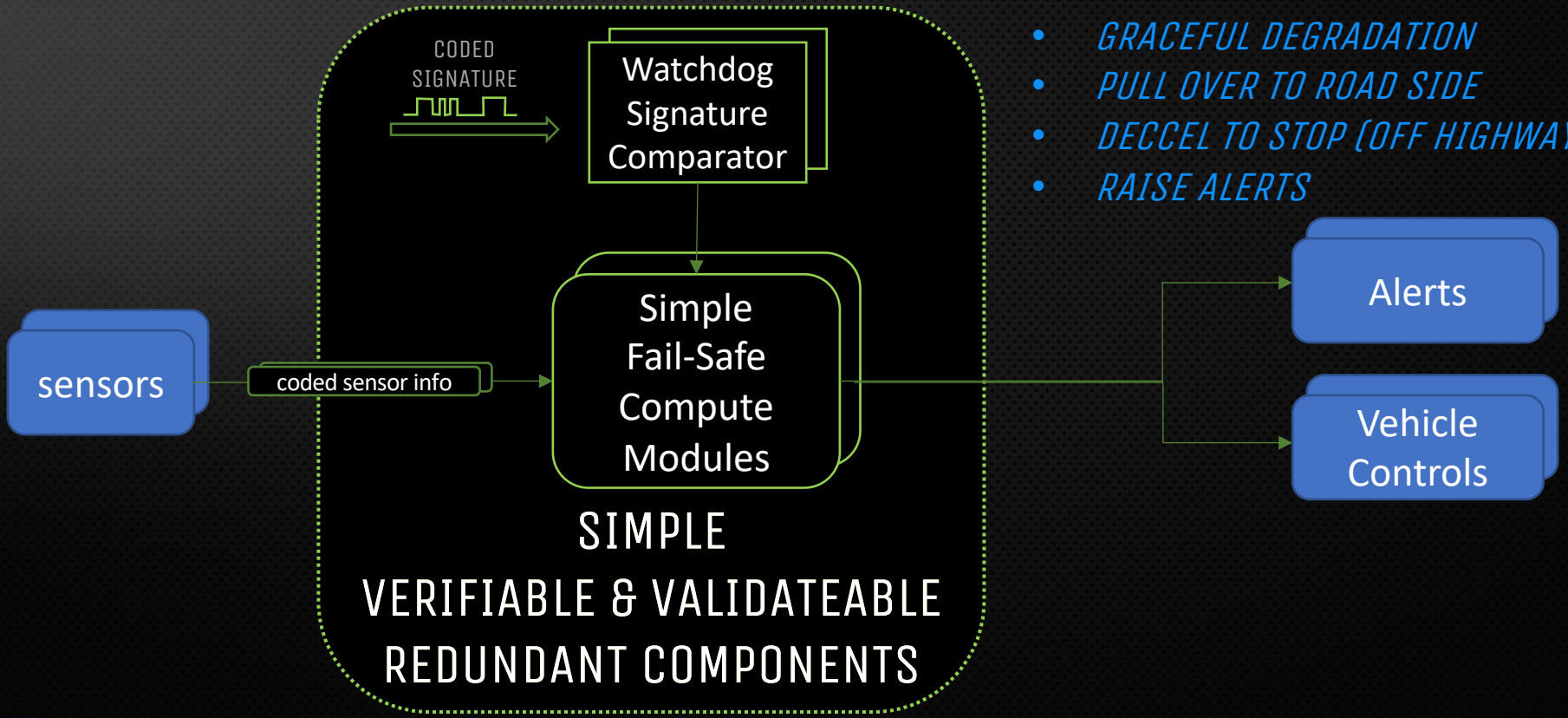
CODING SAFETY-CRITICAL INFORMATION



WATCHDOG SERVICE APPROACH



FAIL-SAFE WATCHDOG REACTION SERVICE



- *GRACEFUL DEGRADATION*
- *PULL OVER TO ROAD SIDE*
- *DECCEL TO STOP (OFF HIGHWAY)*
- *RAISE ALERTS*

SUMMARY

- CURRENT CERTIFICATION METHODS "DATED" TO DEAL WITH FULL AUTONOMY COMPLEXITY
- HIGHER LEVEL PROGRAMMING LANGUAGES/METHODS (FROM IT) + MODERN FRAMEWORKS/RUNTIMES + AI/ML REQUIRED TO ADDRESS FULL AUTONOMY COMPLEXITY
- NEW APPROACHES NEEDED FOR SAFETY WITH FULL AUTONOMY
- SIMPLE VERIFIABLE/VALIDATEABLE WATCHDOG APPROACH
  - Provable and quantifable safety
  - Bonus: Same approach to safety applies to security

PERRONE ROBOTICS