Advances on Core Technologies and Applications:
Building with and around AI, ML, IOT, 5G, Mobility and Cognition

AI-Centric Cyber Laboratory Services: Operationalizing Specific White Box Architectures for Fuzzers

Steve Chan, IARIA Fellow & Decision Engineering Analysis Laboratory

DECISION engineering Analysis Laboratory

IARIA

CORETA 2021 | November 14-18, 2021
Athens, Greece

TABLE OF CONTENTS

DECISION engineering Analysis Laboratory

IARIA

I. INTRODUCTION

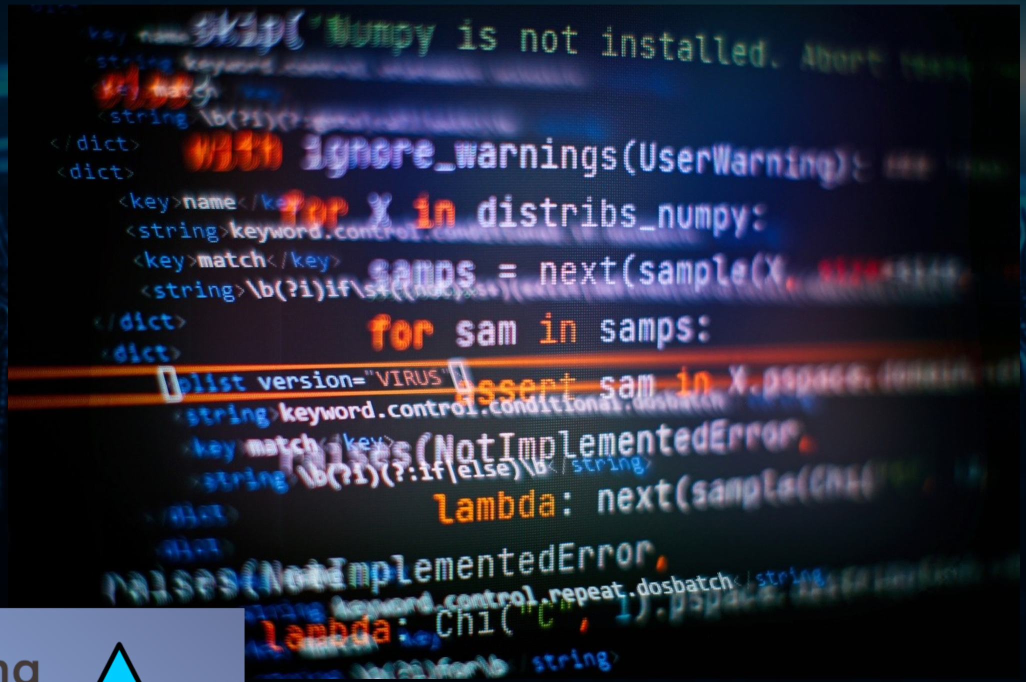
Lab services must contend with cyber issues, and in some cases, the use of black-box architectural tools, such as certain fuzzers, may lead to cyber blindspots.

II. BACKGROUND

- Simplistically, a fuzzer is a software program that injects pseudo-random data into a target application for the purpose of detecting bugs.

- Fuzzing or Fuzz testing is the technique by which a fuzzer is utilized.

DECISION engineering Analysis Laboratory IARIA



Benefits of Fuzzing

- The benefits of fuzzing have been well documented, such as when researchers found dozens of vulnerabilities in wireless networks.

Prototypical Fuzzers have Coverage Issues

- Prototypical fuzzers have coverage issues (i.e., they only fuzz certain lines of code or certain sections of the software program).

DECISION engineering Analysis Laboratory

IARIA

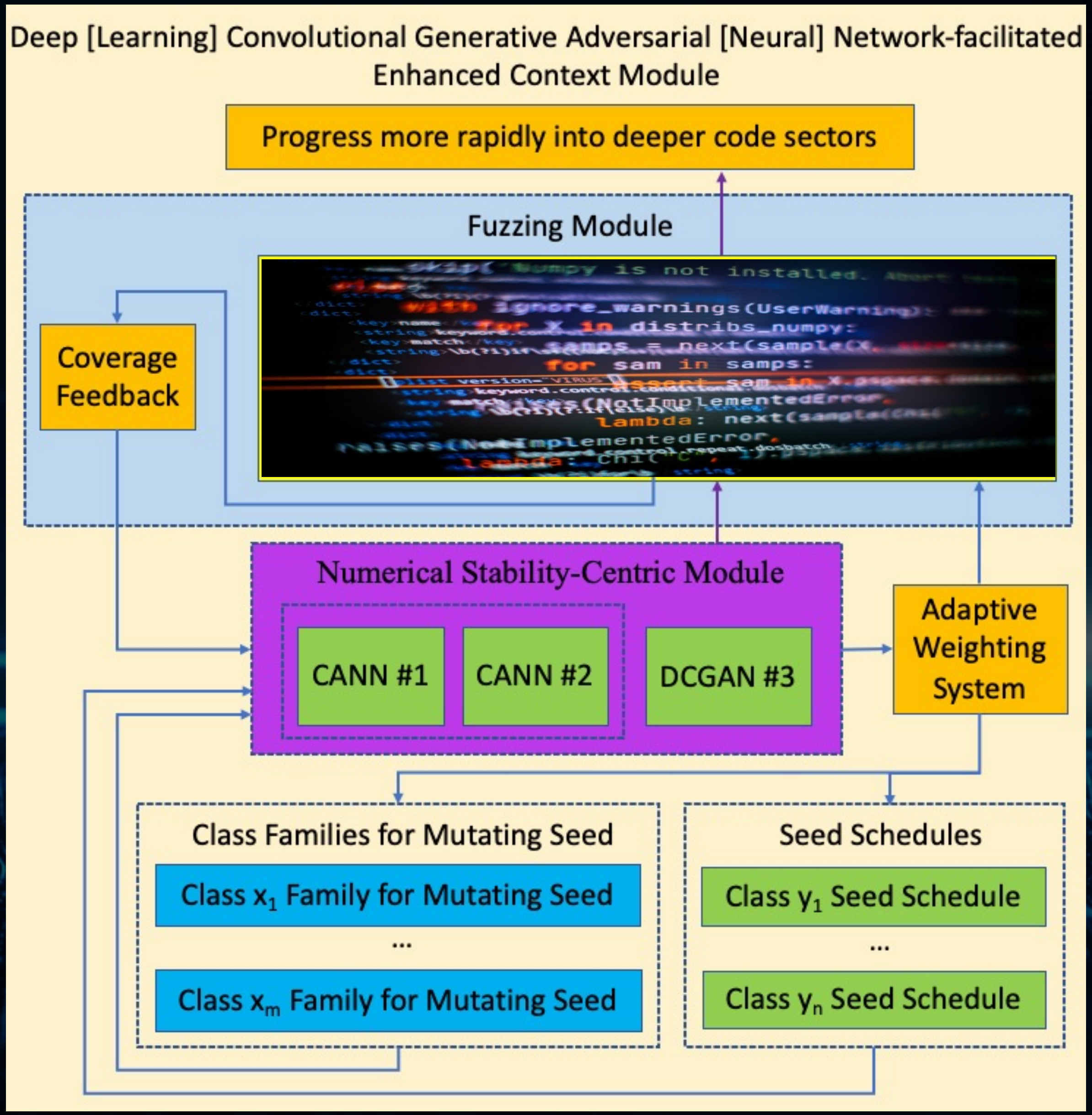
Fuzzers can be divided into Black-box and White-box

- In general, black-box fuzzers tend to have better computational performance, but we tend to be unsure of the coverage, and white-box fuzzers tend to have worse computational performance, but we tend to be more sure of the coverage.

We will not be discussing grey-box fuzzers today

- There are also grey-box fuzzers, but for the purposes of our discussion today, we shall focus on black-box and white-box.

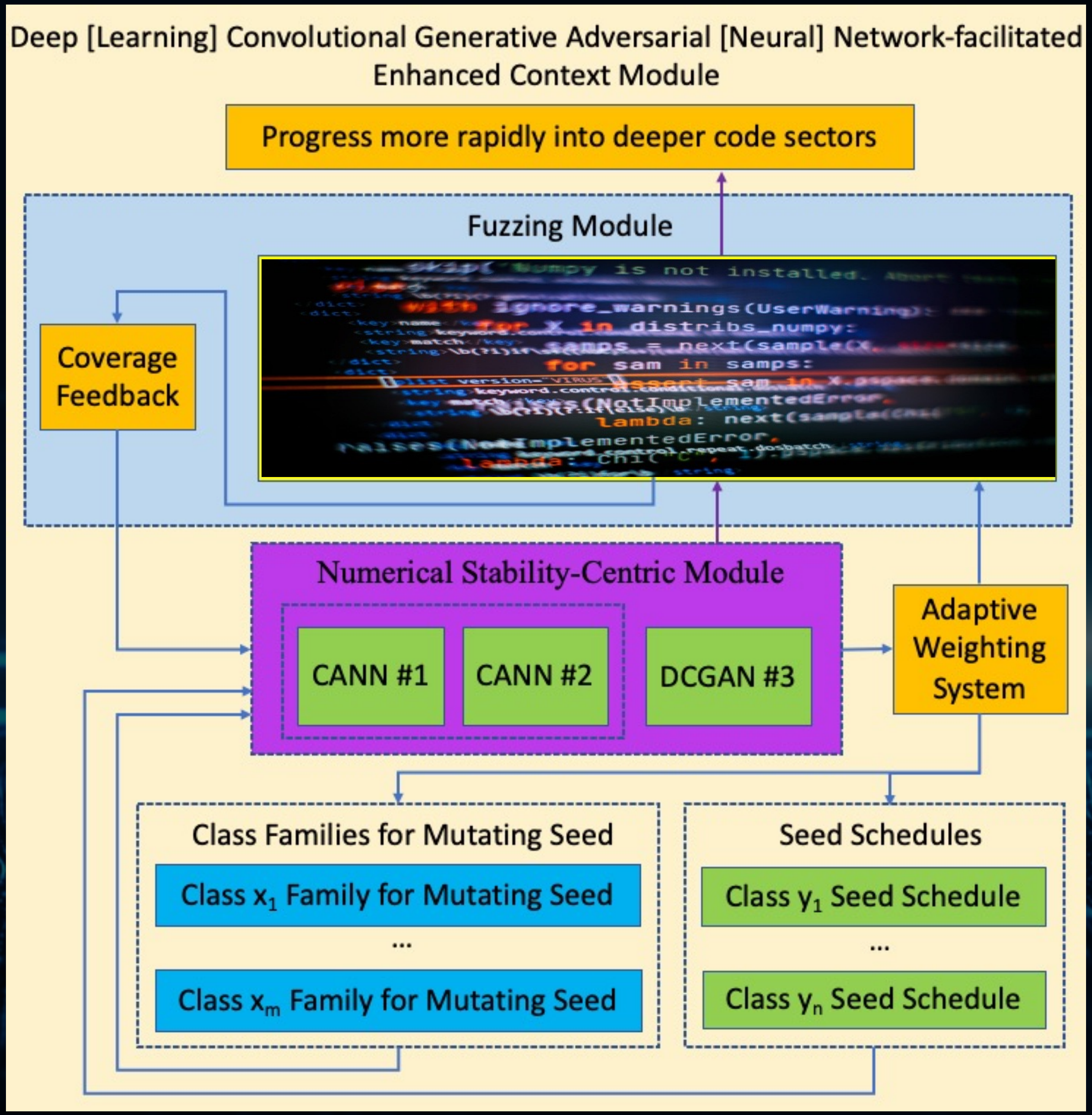
White-box Fuzzers:



- For many cases, the more white-box the fuzzer, the better we are able to discern which parts of a software program it visits and how consistent it is in doing so.

- Specifically, the more white-box the fuzzer, the more insight we have into the utilized seed schedules (i.e., varying distributions of the fuzzing time spent among the seeds) for coverage.

- The significance of this resides in the fact that the fuzzer's Enhanced Context Module or ECM selects a seed, mutates it, and serves it as input to the test target. If the input causes a crash, it will be added to the ECM's crash set. Alternatively, if the input segues to new coverage, it will be added to the search seed pool.



White-box Fuzzers

- This coverage feedback serves as input to the Numerical Stability-Centric Module or NSCM, which processes the information and informs the Adaptive Weighting System, which dynamically weights the Class Families for Mutating Seed and Seed Schedules. This should segue to a more optimal Seed Schedules for decreasing Time-to-Exposure or TTE (i.e., speed at which bugs are found) as well as a more optimal Relative Standard Deviation or RSD (i.e., number of unique bugs found for the fuzzing iterations).

DECISION engineering Analysis Laboratory

IARIA

Spawned Nonconvex Problems

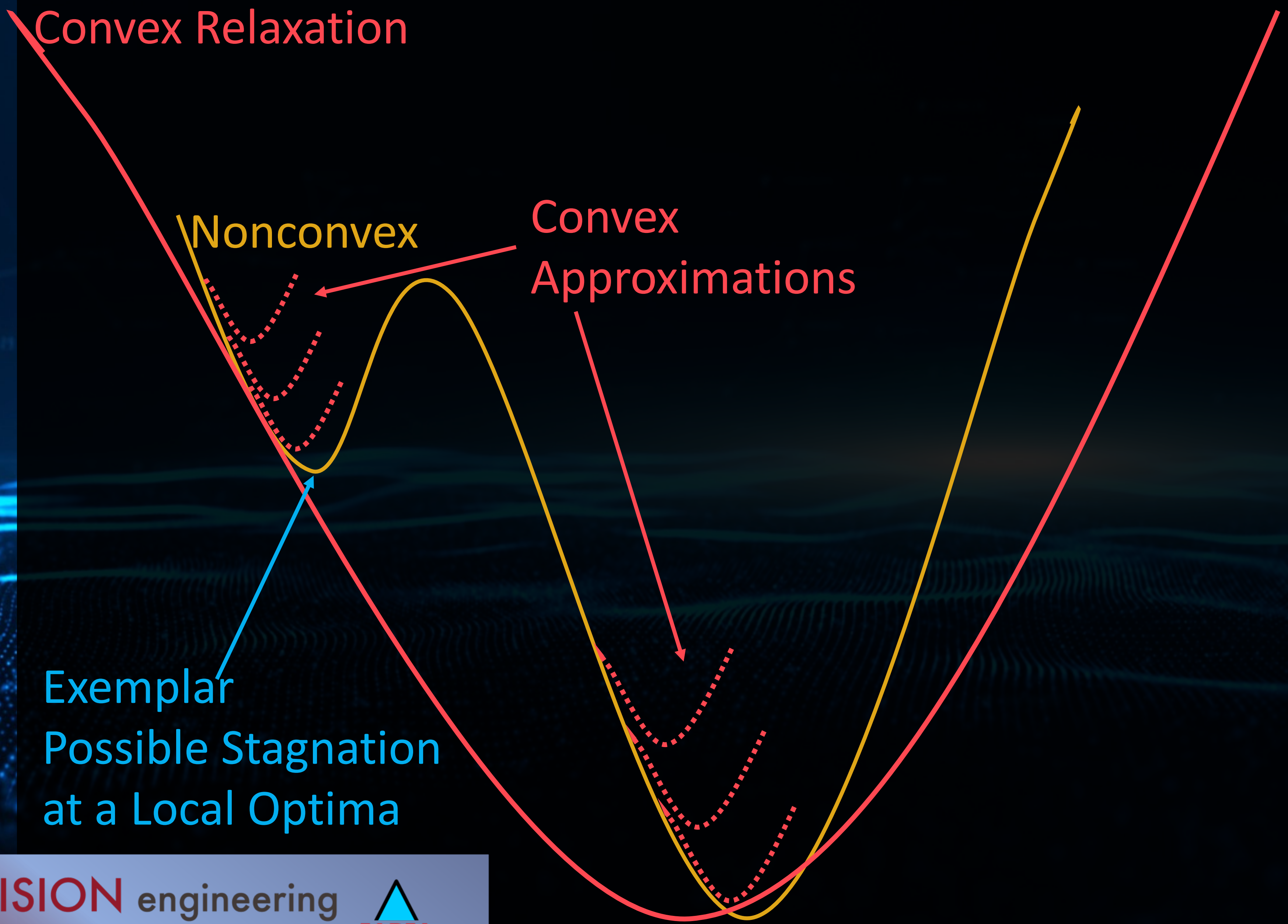
- It should be noted that even when the input set is specifically designed/architected to segue to a convex paradigm, the resultant output set may still turn out to be nonconvex, thereby necessitating a transformation to a convex optimization problem via certain relaxation techniques. This transformation in itself may spawn yet other nonconvex optimization problems, thereby highlighting the need/opportunity to utilize a Robust Convex Relaxation (RCR) paradigm.

- This seems prudent not only for solving the involved convex optimization problems, but also leveraging the same RCR mechanism for tuning its own hyperparameters.

DECISION engineering Analysis Laboratory IARIA

III. NUMERICAL CHALLENGES

- Given its advantages in terms of the reduced number of hyperparameters to tune, Particle Swarm Optimization (PSO) is often implemented. However, PSO presents its own technical challenges.

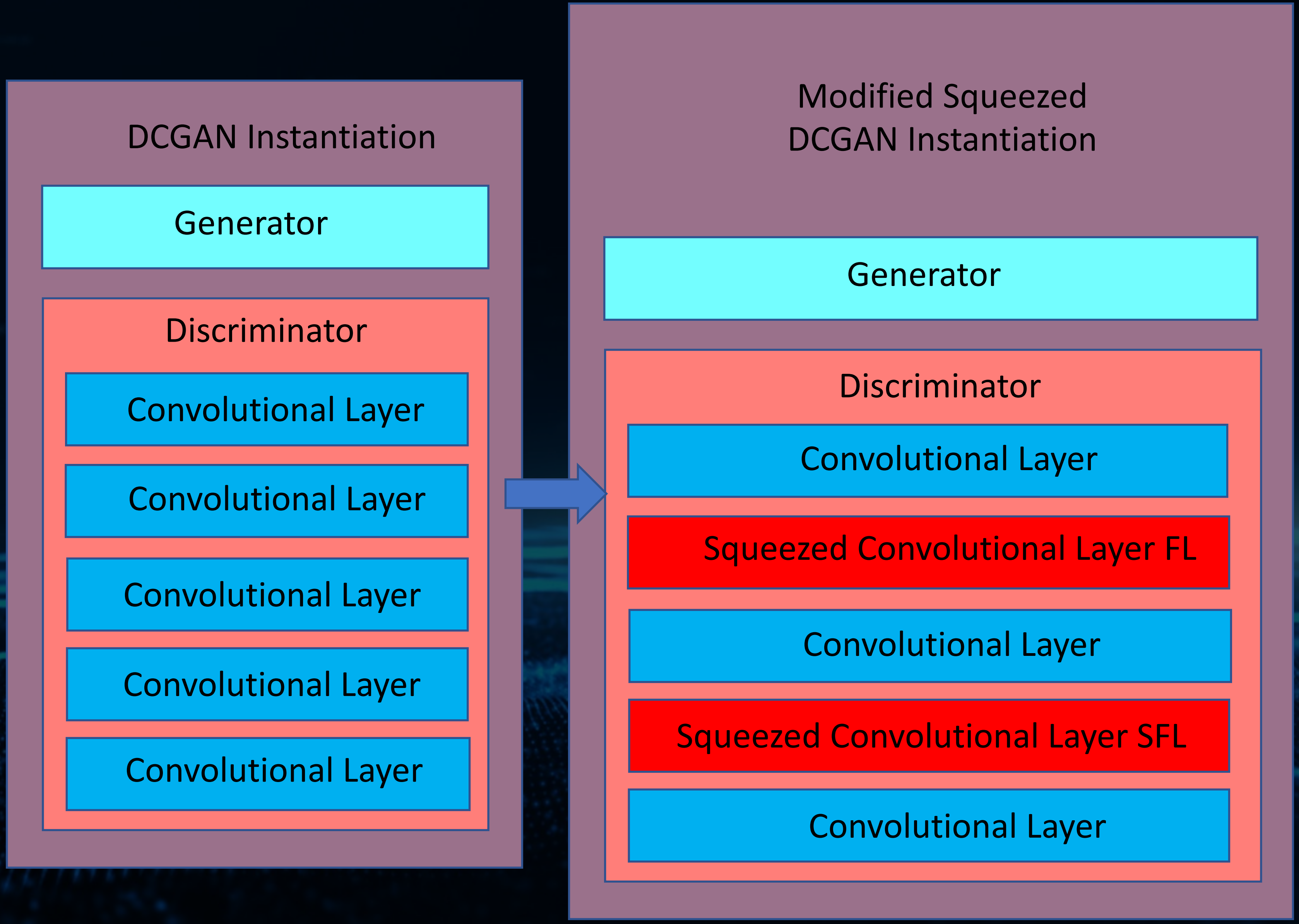


DECISION engineering Analysis Laboratory IARIA

Particle Swarm Optimization

- Given its advantages in terms of the reduced number of hyperparameters to tune, Particle Swarm Optimization (PSO) is often implemented.

- This approach gives rise to various technical challenges. When implemented on Deep Convolutional Generative Adversarial Networks (DCGANs), PSO requires converting continuous/discontinuous hyperparameters to discrete values (e.g., integers). Yet, rounding the calculated velocities to discrete integer values creates an artificial paradigm, wherein particles may stagnate prematurely. Certain techniques, such as increasing the inertia (thereby allowing particles to advance past their current local optimum) can address this issue.

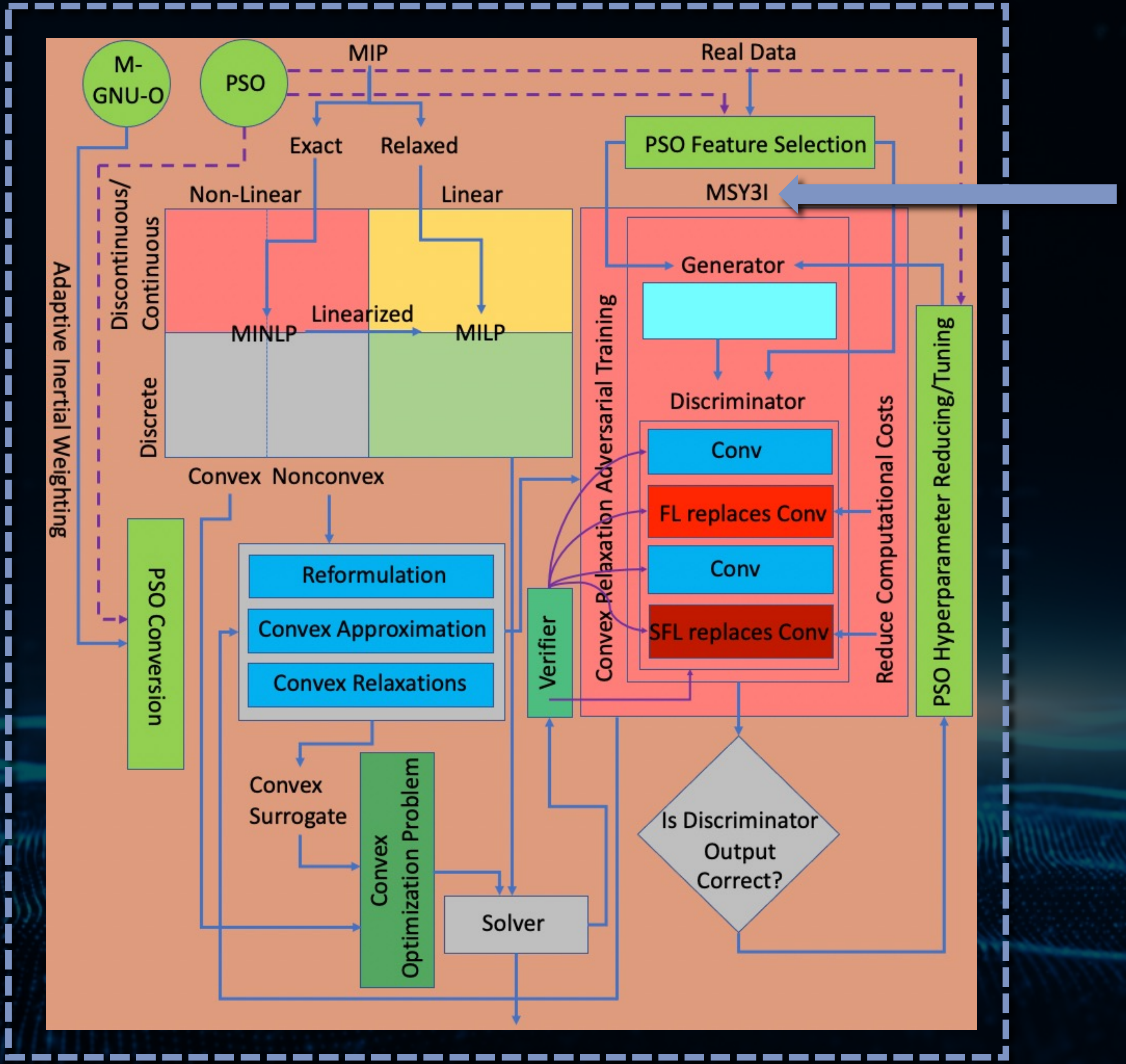


DECISION engineering Analysis Laboratory IARIA

Fire Layers

- To reduce the computational cost, the notion of fire modules/layers from SqueezeNet (a deep neural network) was utilized to replace convolution layers (a.k.a. Conv) with Fire Layers (FL), and a SqueezeDet adaptation was incorporated for the replacement of certain Conv with Special Fire Layers (SFL).

- The combination of FL/SFL with convex relaxation adversarial training can improve the bound tightening for each successive neural network layer to better facilitate the resolution of the various involved optimization formulations which are, in essence, Mixed Integer Non-Linear Programming (MINLP) problems that need to be optimally solved (e.g., the global optimum).



RCR Paradigm

DCGAN PSO Benefit:

- Facilitates valid bounds for near-optimal convex optimization solutions.

Achieving the DCGAN PSO Benefit, via an RCR Paradigm

- Squeezed Convolutional Layers, Fire Layer (FL) or Special Fire Layer (SFL), with a specific implementation (Modified Squeezed YOLO version 3 Implementation or MSY3I, in this case).

- Convex Relaxation Adversarial Training.

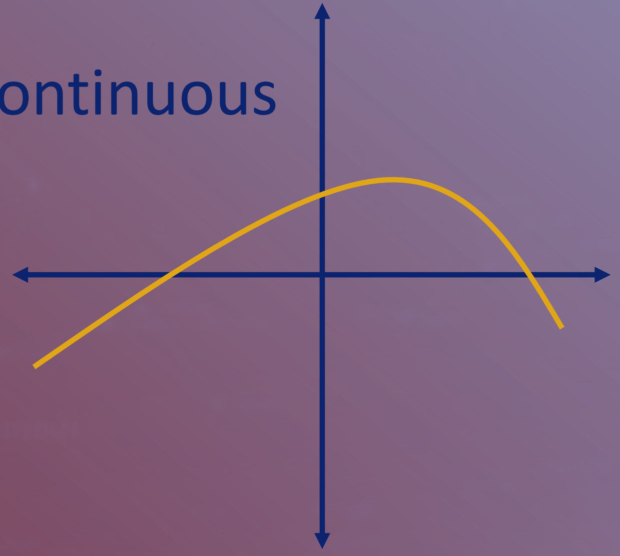
- Facilitated Robust Convex Relaxations (RCR).

DECISION engineering
Analysis Laboratory
IARIA

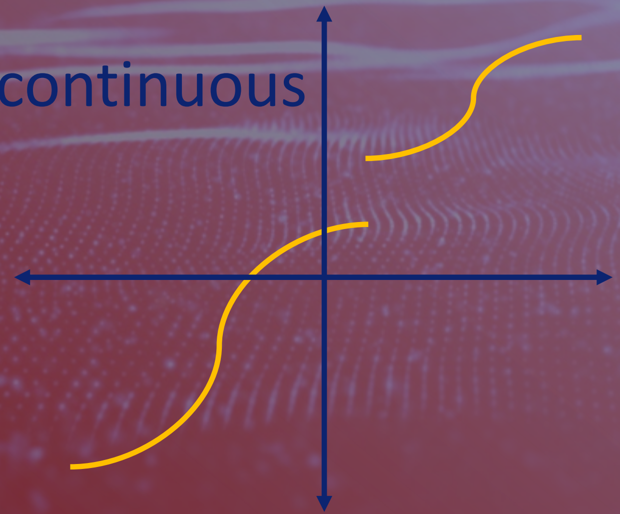
MIP PROBLEMS

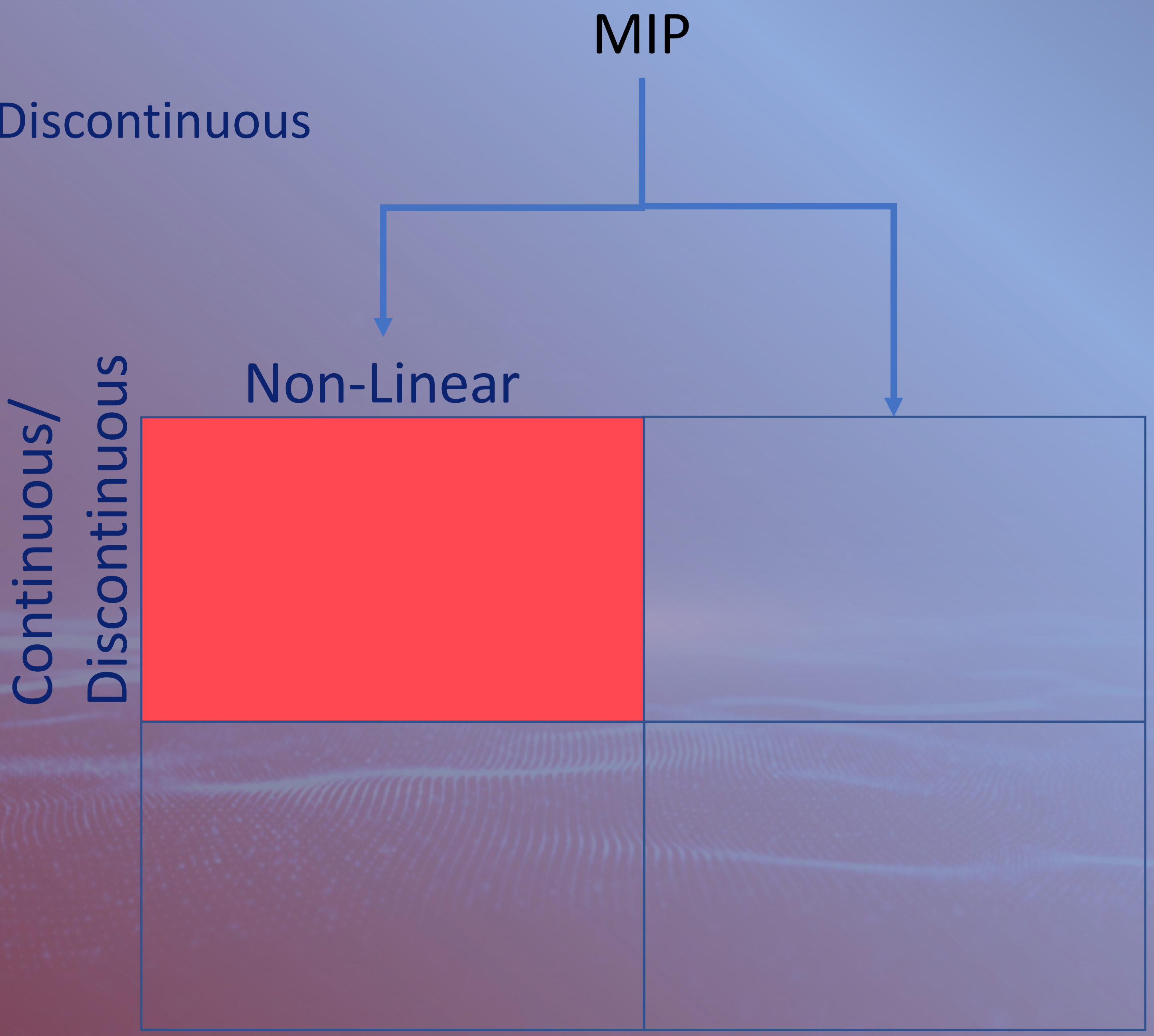
Non-Linear, Continuous/Discontinuous

Continuous



Discontinuous

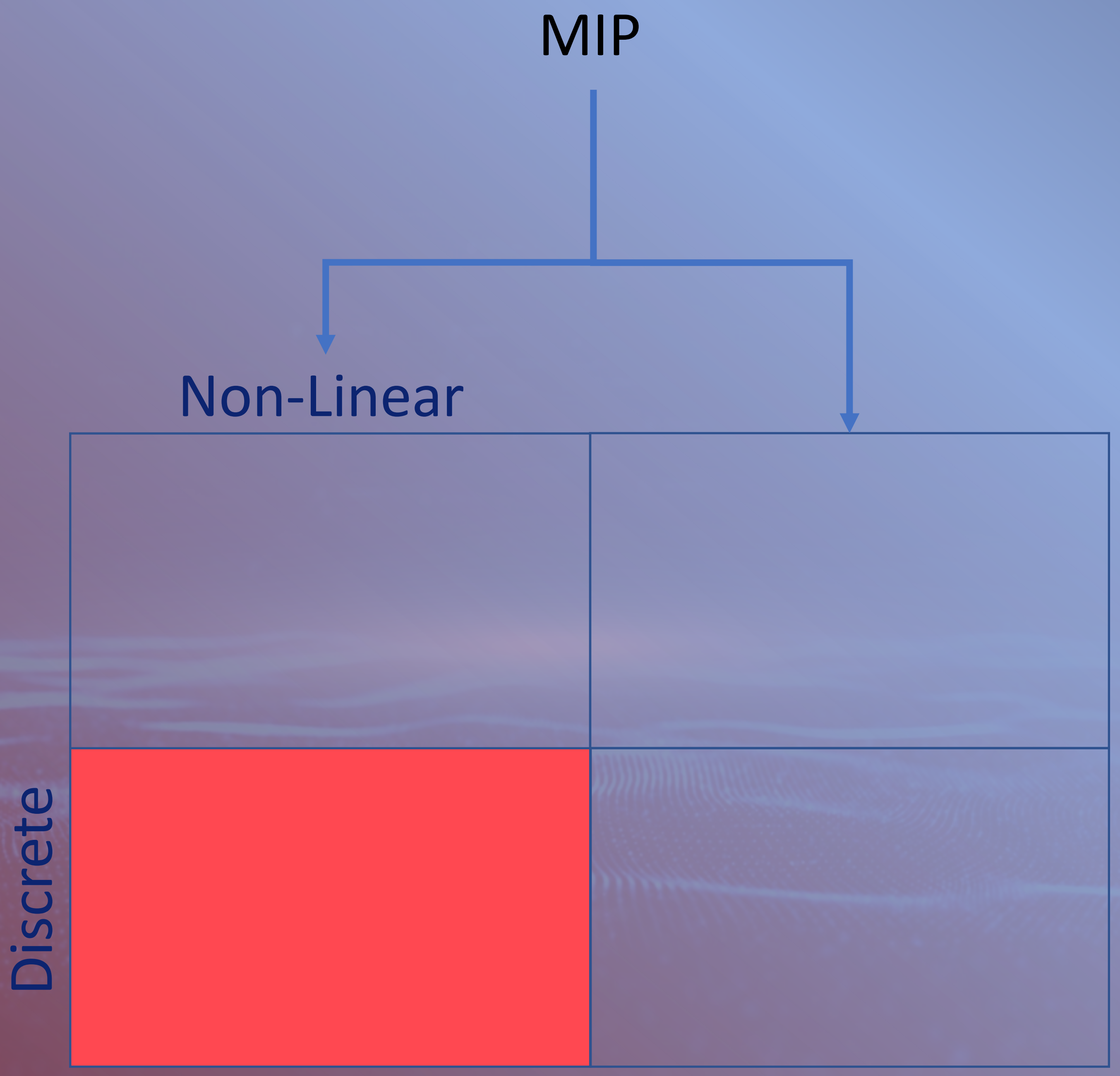


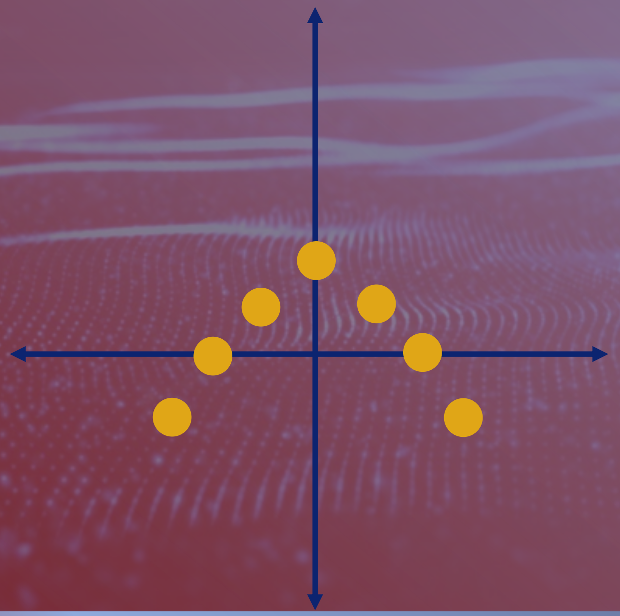


DECISION engineering
Analysis Laboratory
IARIA

MIP PROBLEMS

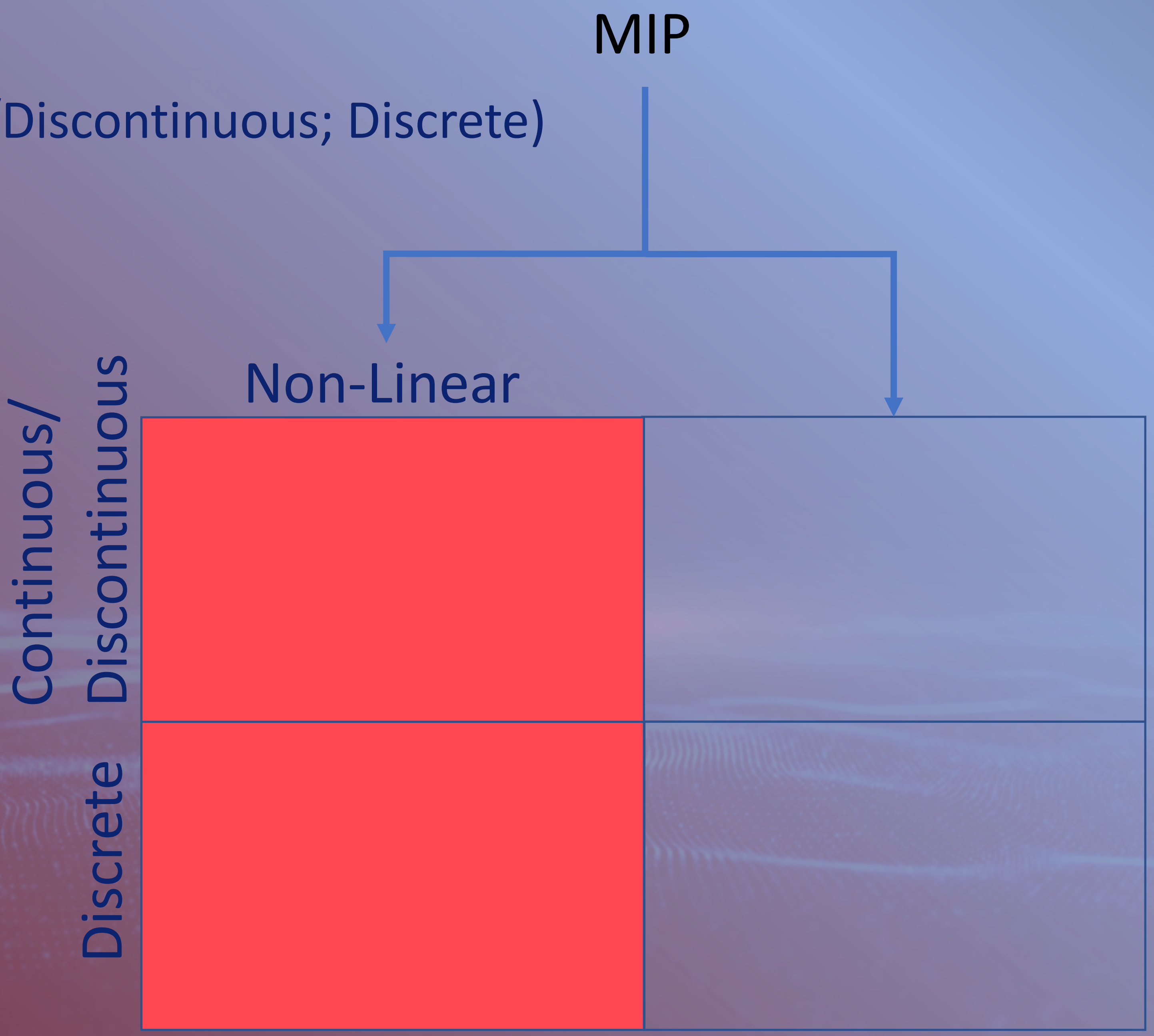
Non-Linear, Discrete





MIP PROBLEMS

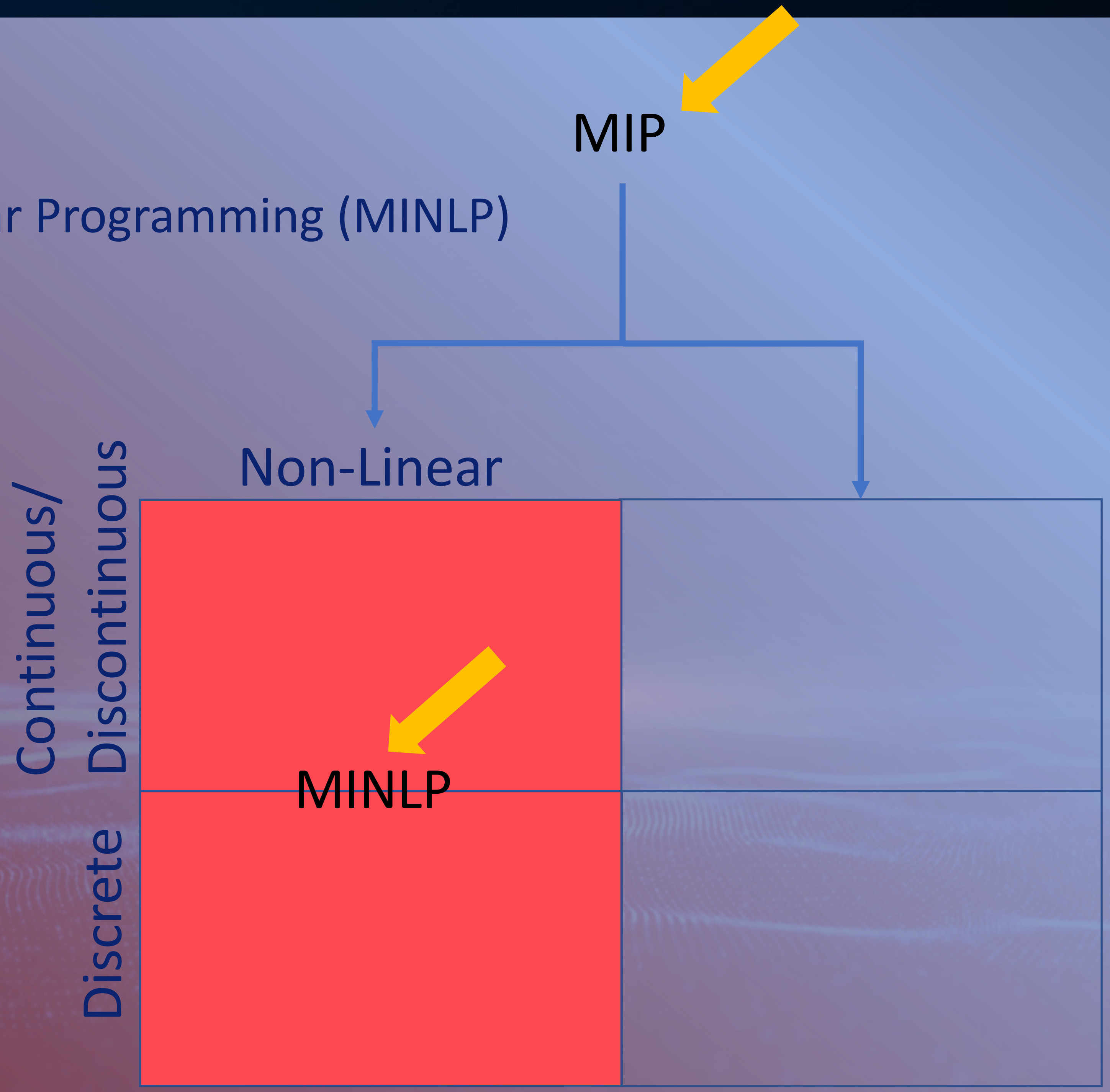
Non-Linear (Continuous/Discontinuous; Discrete)



DECISION engineering
Analysis Laboratory
IARIA

MIP PROBLEMS

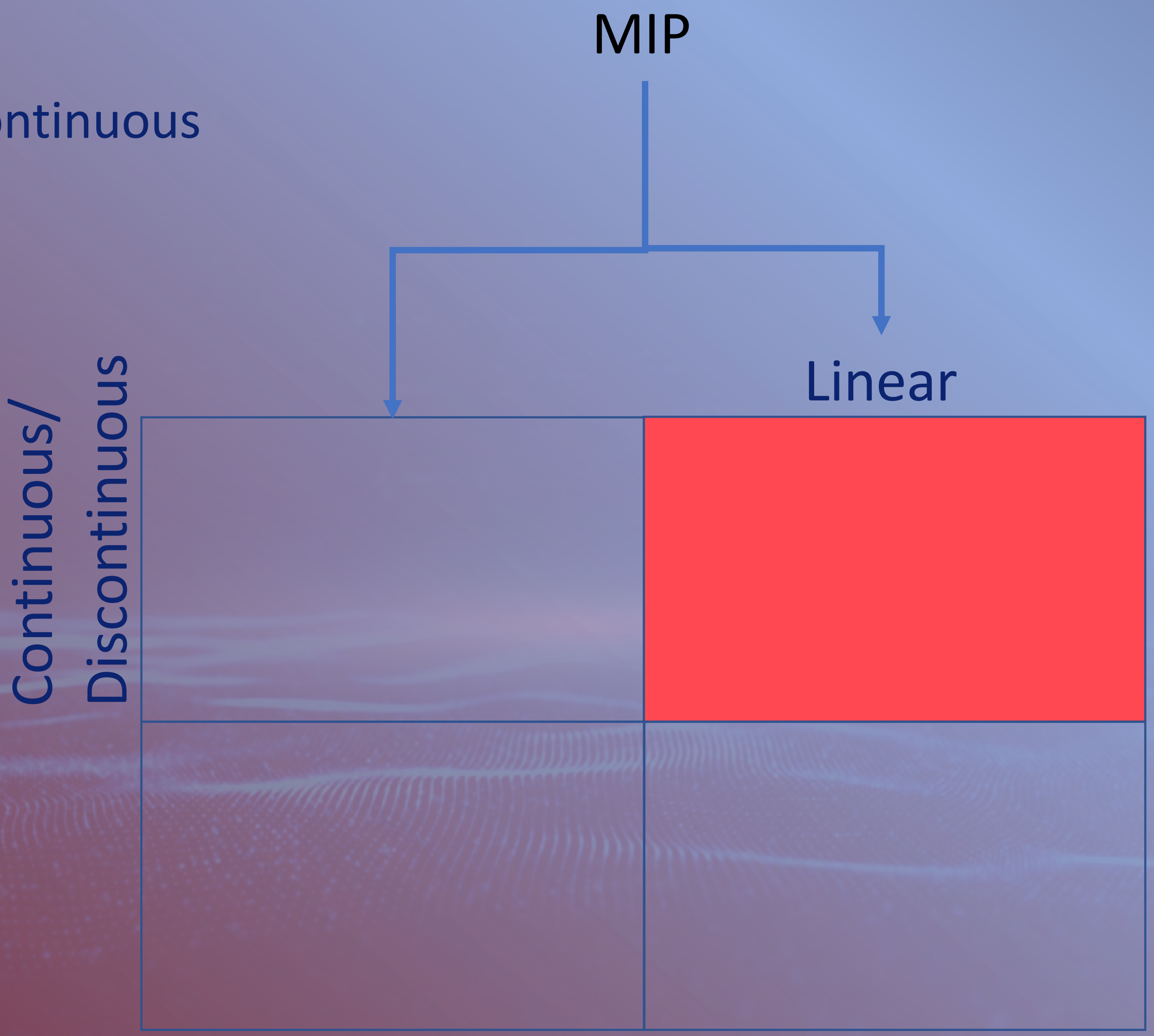
Mixed Integer Non-Linear Programming (MINLP) Problems



DECISION engineering Analysis Laboratory

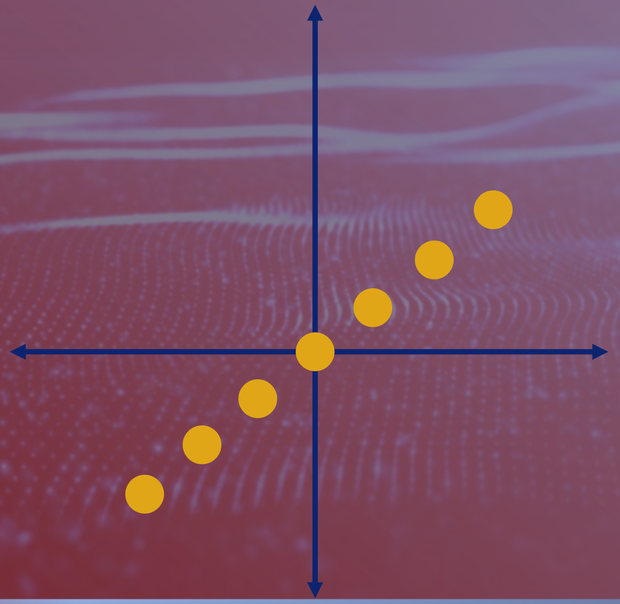
MIP PROBLEMS

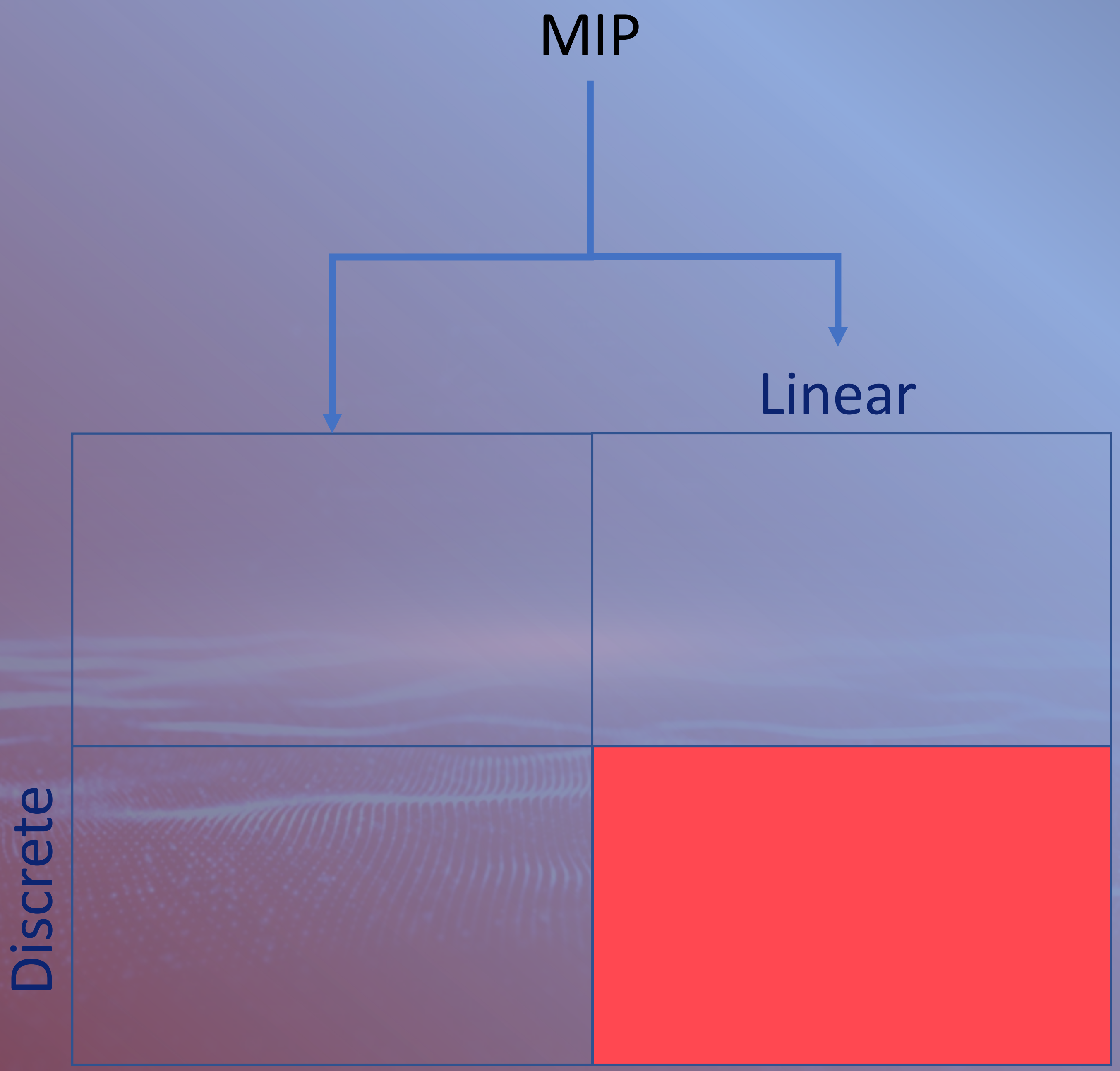
Linear, Continuous/Discontinuous



DECISION engineering
Analysis Laboratory
IARIA

MIP PROBLEMS
Linear, Discrete

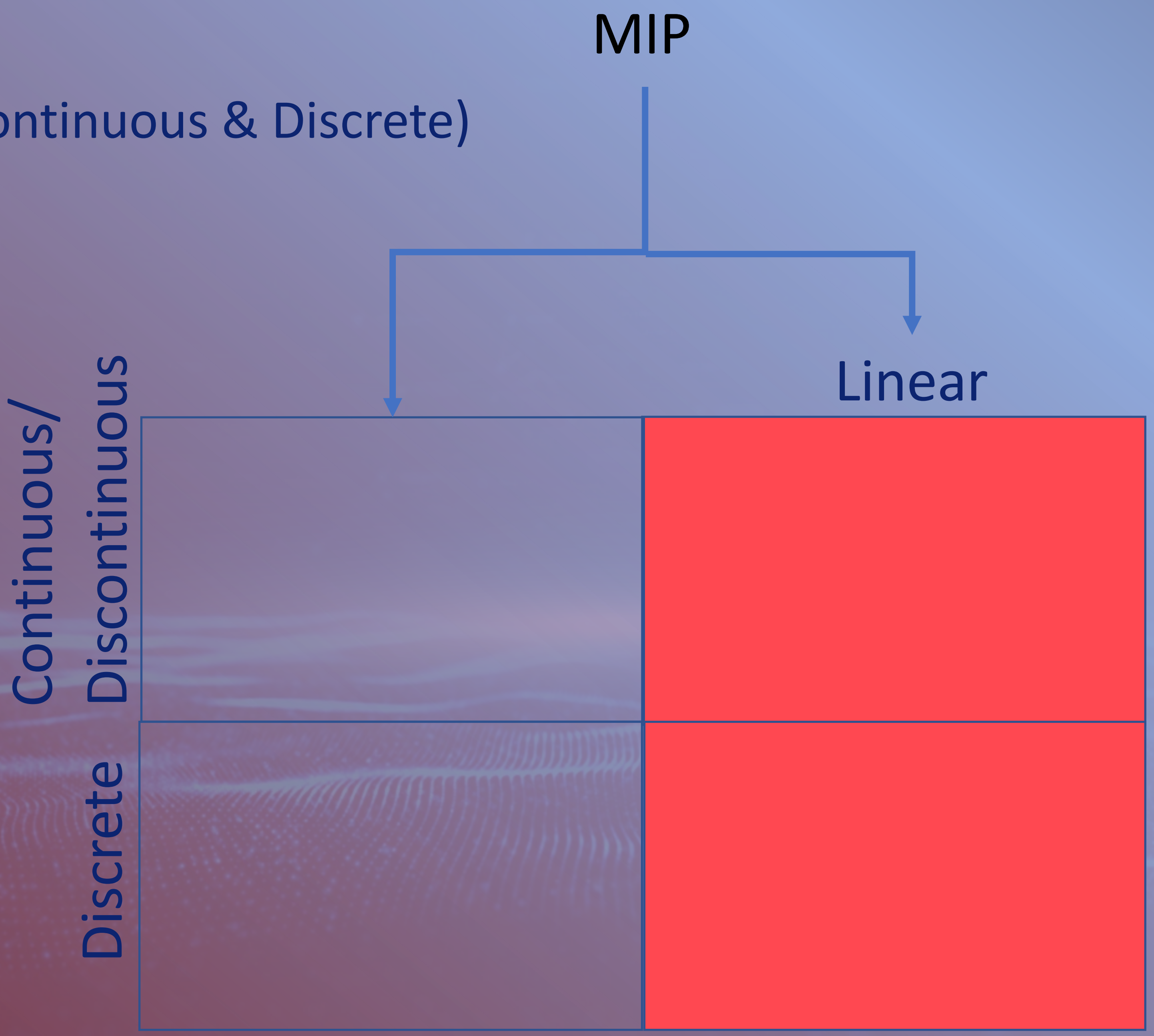




DECISION engineering Analysis Laboratory IARIA

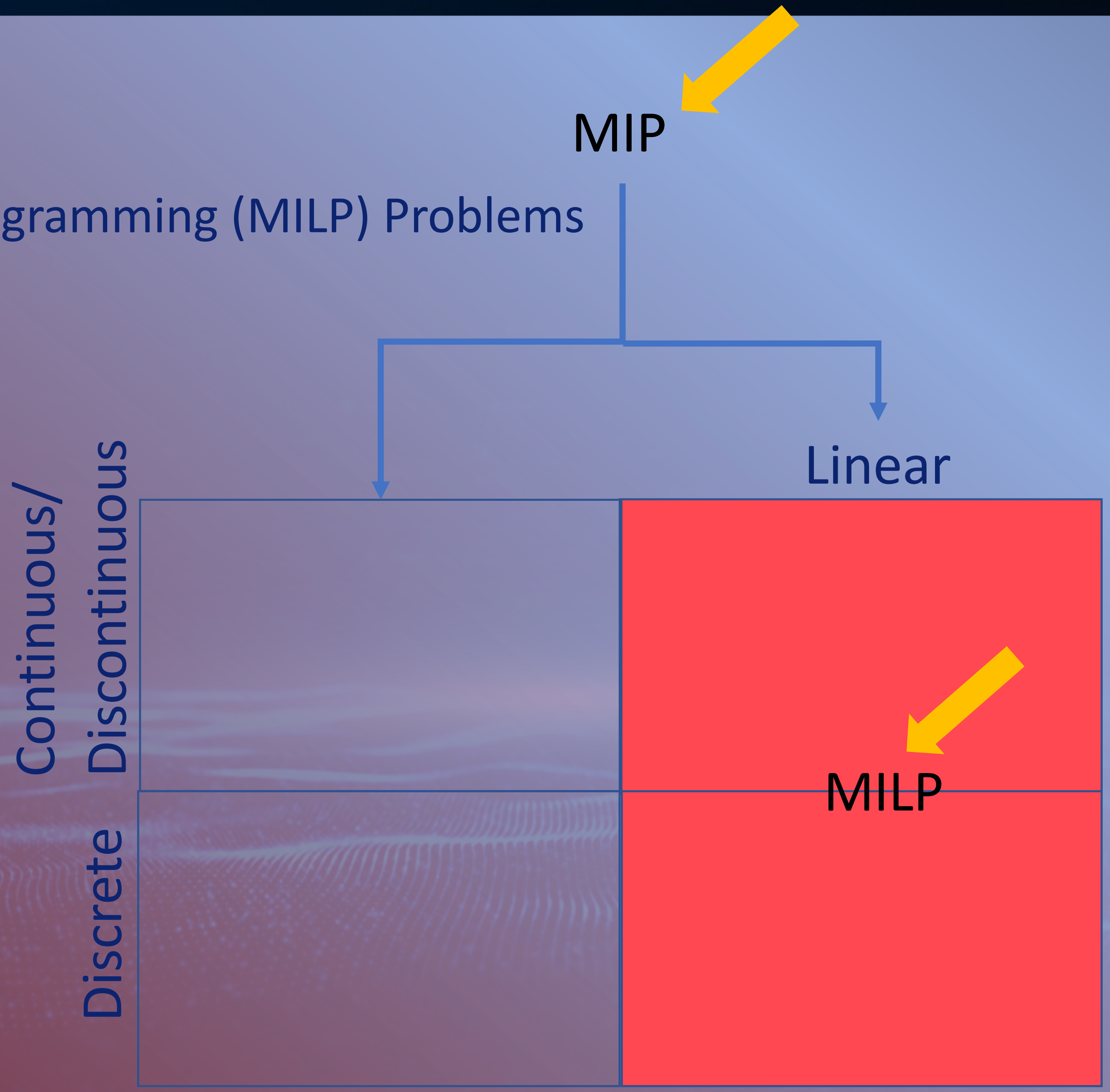
MIP PROBLEMS

Linear (Continuous/Discontinuous & Discrete)



MIP PROBLEMS

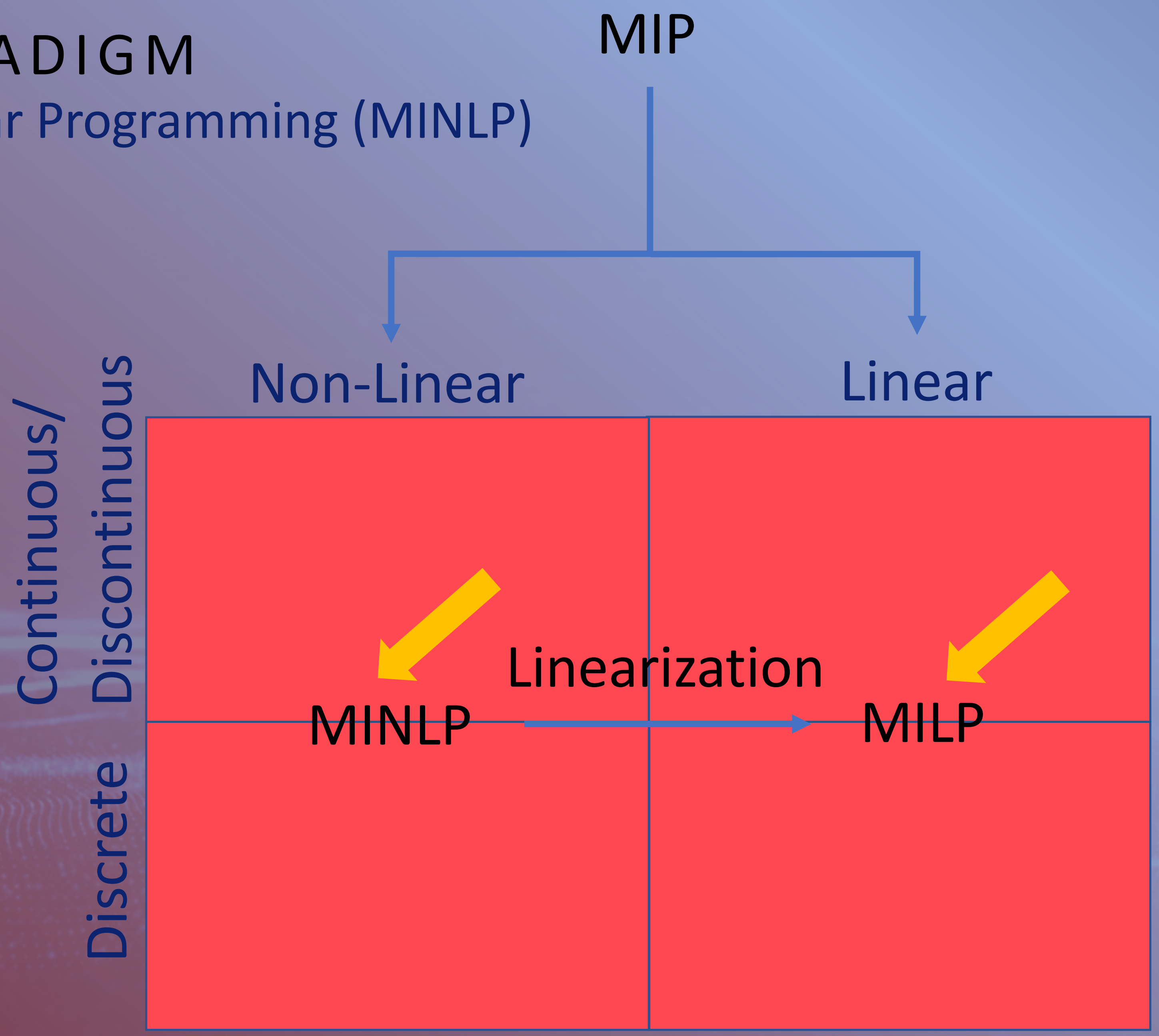
Mixed Integer Linear Programming (MILP) Problems



DECISION engineering
Analysis Laboratory
IARIA

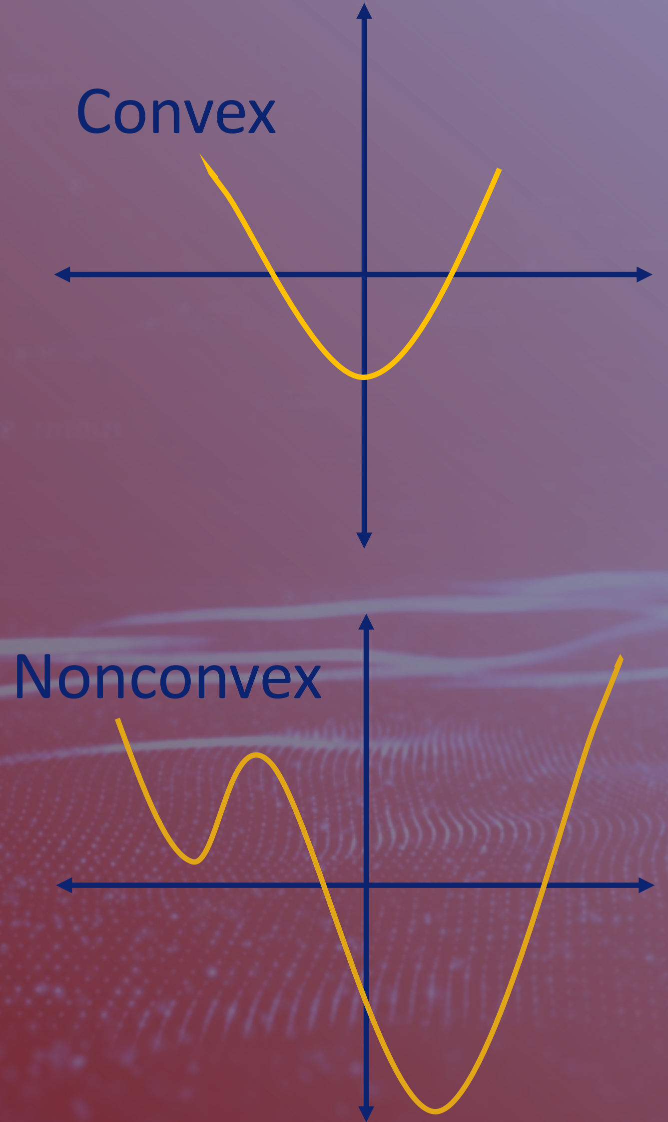
NONCONVEX PARADIGM

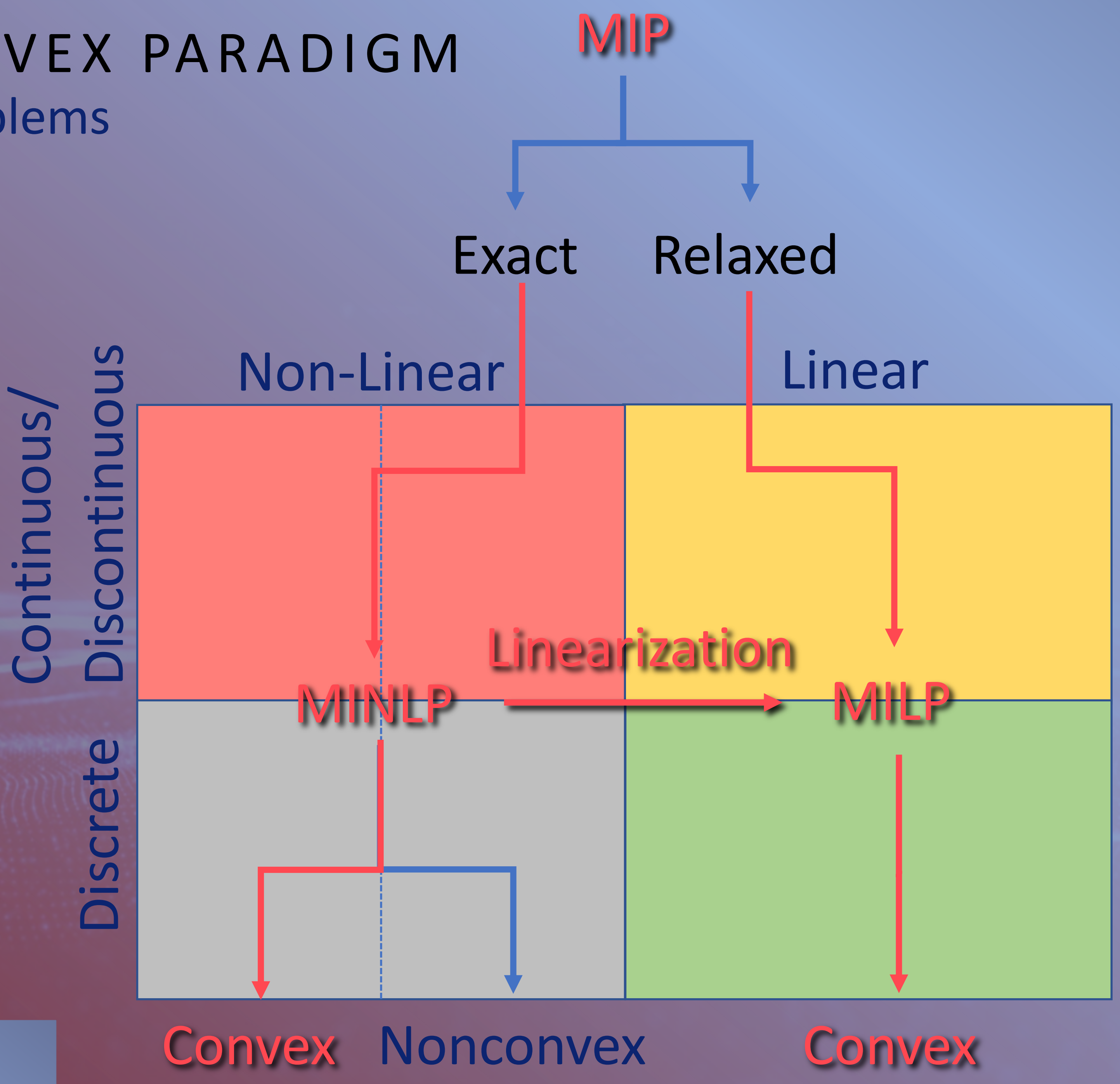
Mixed Integer Non-Linear Programming (MINLP) Problems



ATTAINING A CONVEX PARADIGM

Pathways to Convex Problems



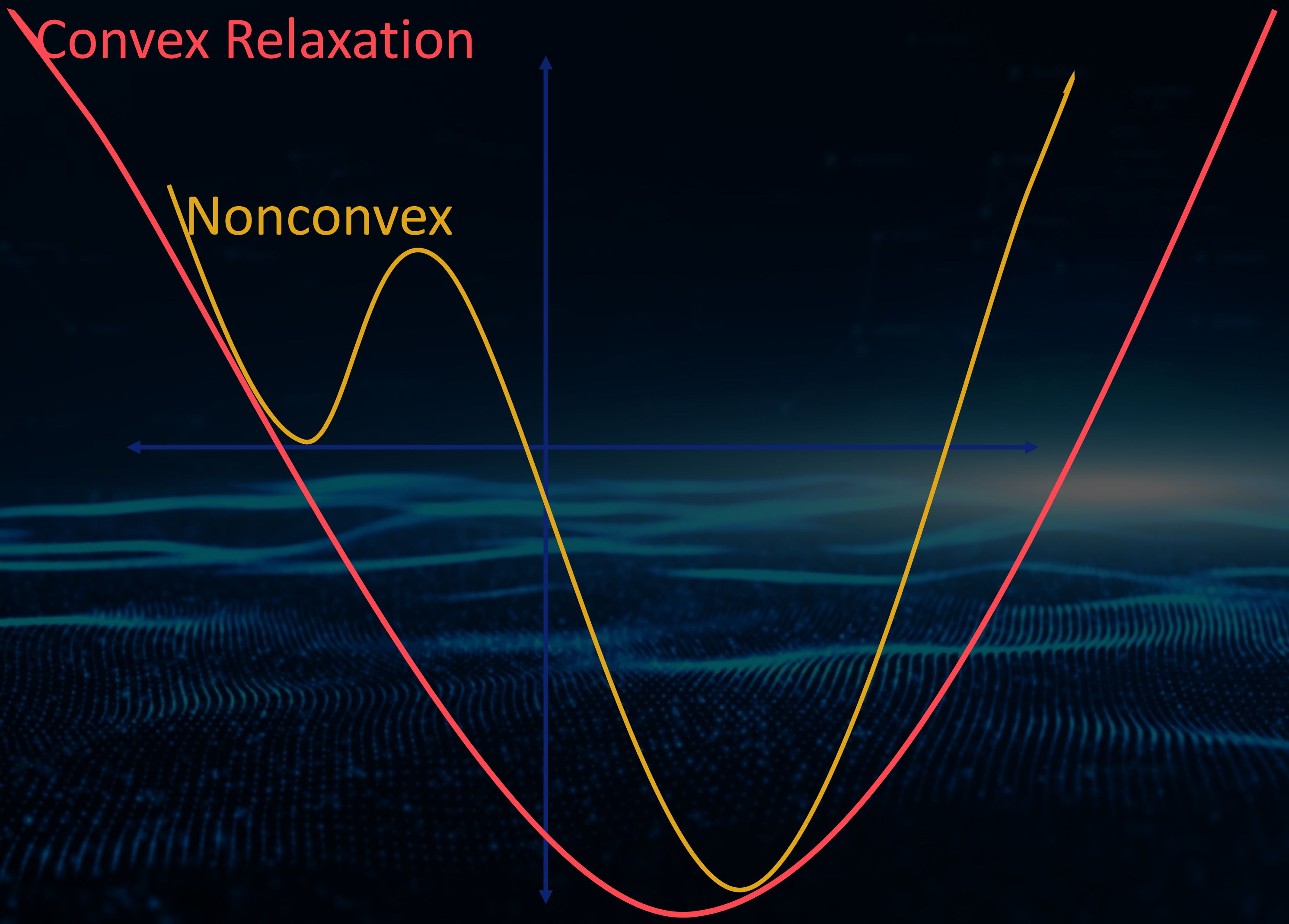


IV. POSITED APPROACH

- A Series of Robust Convex Relaxations (RCR), via PSO, Represents a Viable Posited Approach.

DECISION engineering
Analysis Laboratory
IARIA

Convex Relaxations

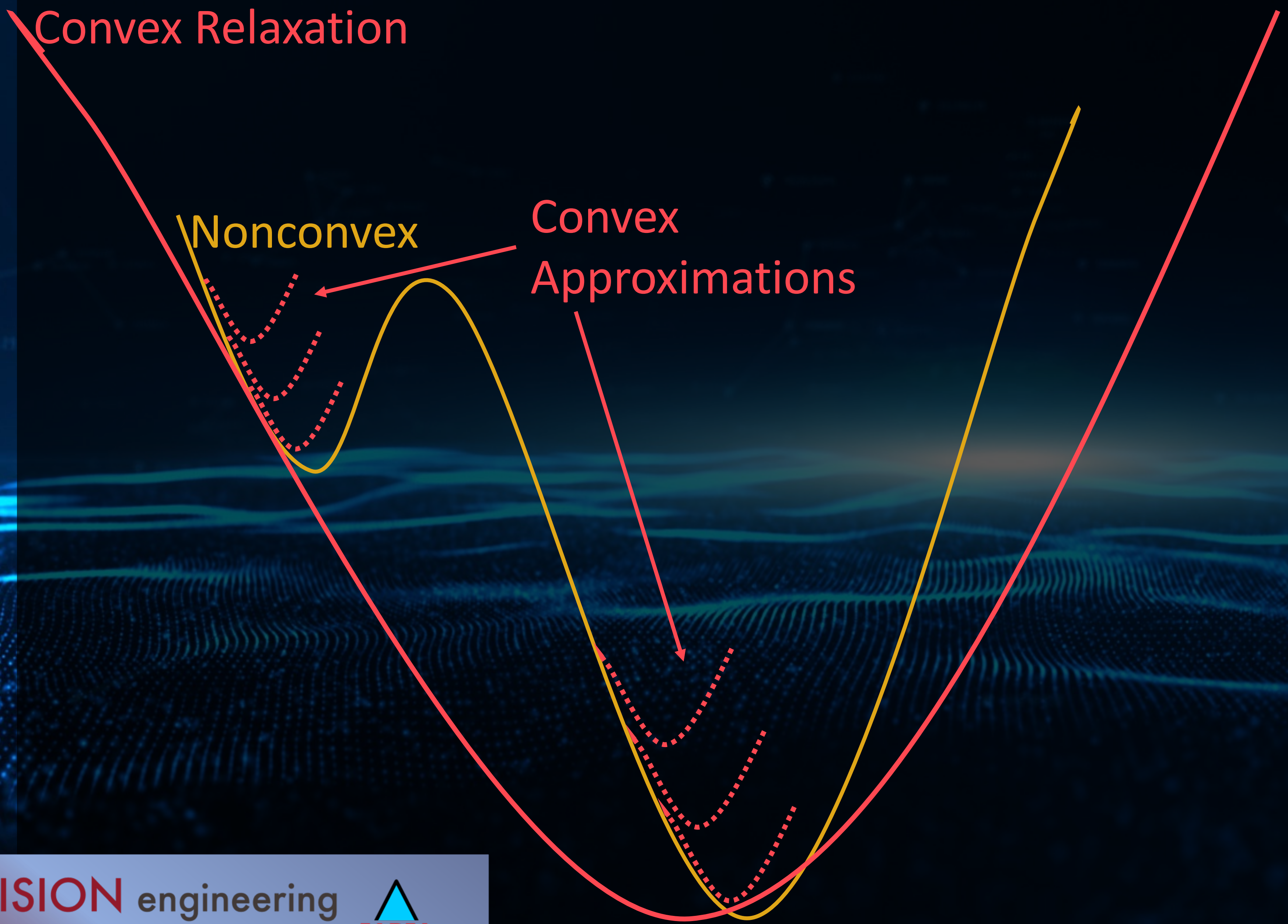


Advantages of this Approach

- Deep Generative Convolutional Adversarial Network (DCGAN) with particular attention paid at each neural network layer.
- Increased transparency at each neural network layer.

DECISION engineering Analysis Laboratory IARIA

Convex Surrogate



DECISION engineering Analysis Laboratory

IARIA

Our Utilized Approach:

- Convex Surrogates.
- Convex Approximations.
- Convex Relaxations.
- Series of Robust Convex Relaxations (RCR), via PSO.

The Promise of PSO:

- Facilitates valid bounds for near-optimal convex optimization solutions.
- Reduced number of hyperparameters to tune, via a specific implementation of PSO.

V. CONCLUDING REMARKS

- The posited RCR architecture, as an Enhanced White-box Architecture for certain fuzzers, demonstrates promise for better Insight into coverage.

DECISION engineering Analysis Laboratory IARIA

Advances on Core Technologies and Applications:
Building with and around AI, ML, IOT, 5G, Mobility and Cognition

AI-Centric Cyber Laboratory Services: Operationalizing Specific White Box Architectures for Fuzzers

Thank you!

Steve Chan, IARIA Fellow & Decision Engineering Analysis Laboratory