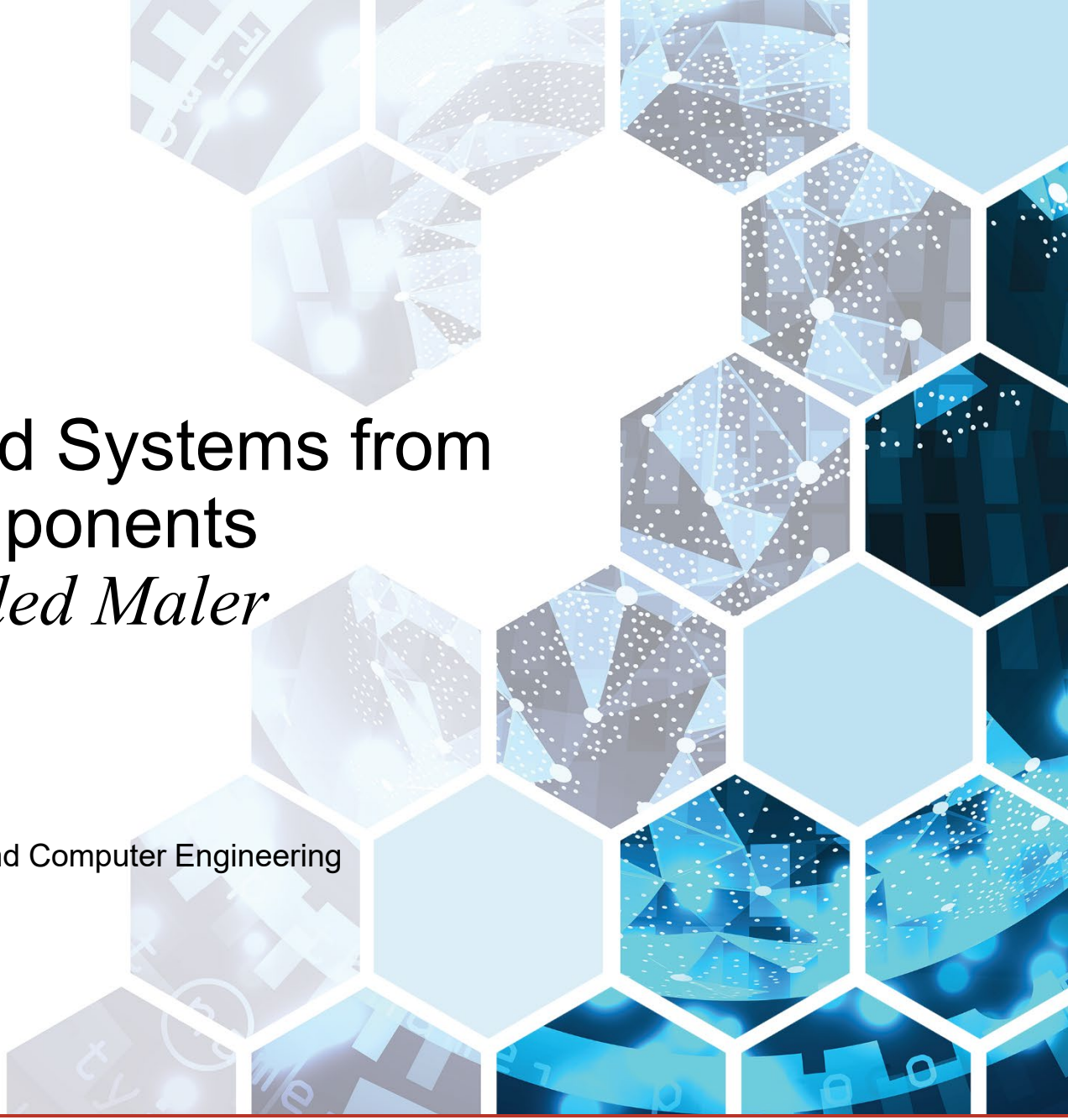


Building Trusted Systems from Untrusted Components

in memory of Oded Maler

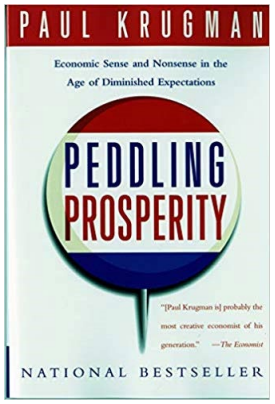
Bruce Krogh
Professor Emeritus of Electrical and Computer Engineering
SEI Research Staff

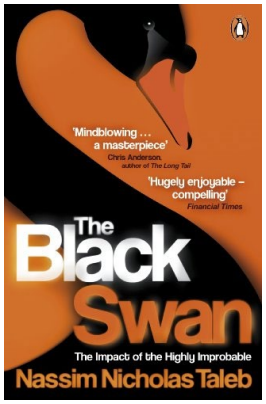
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

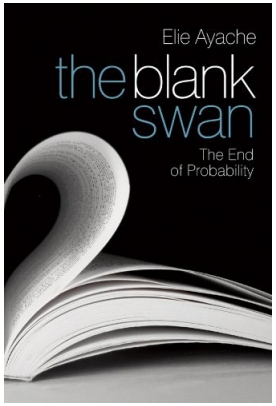
Document Markings

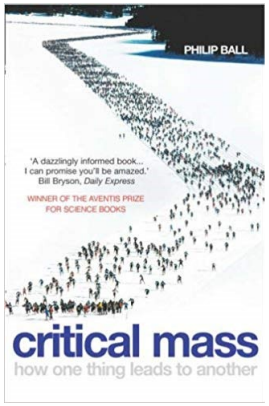
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

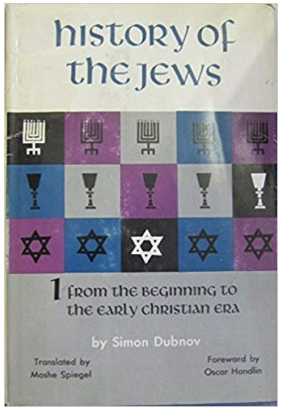
DM19-0392

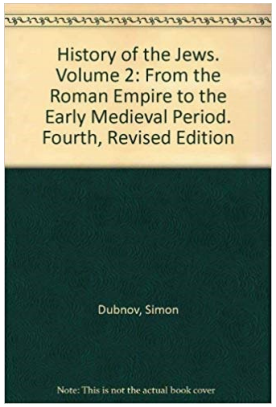


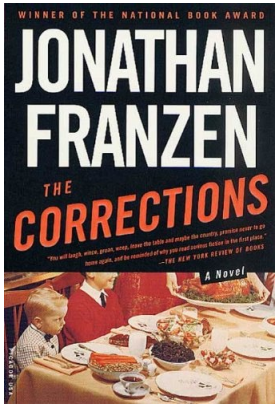


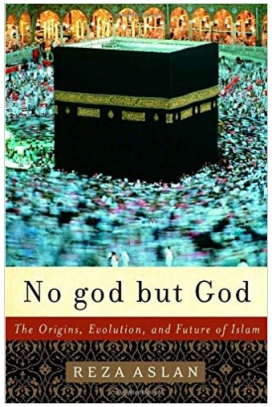


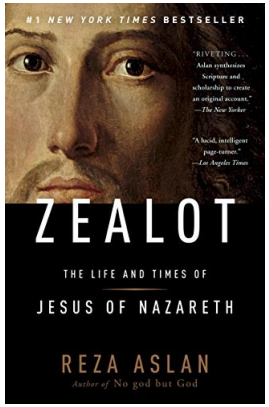


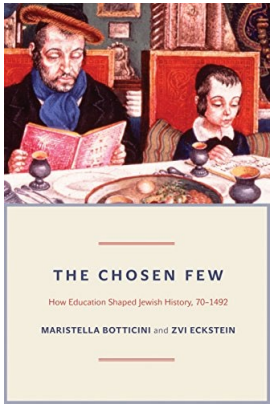


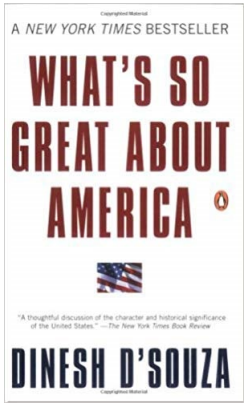


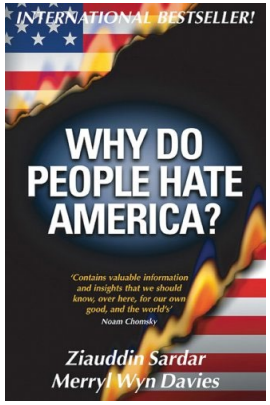


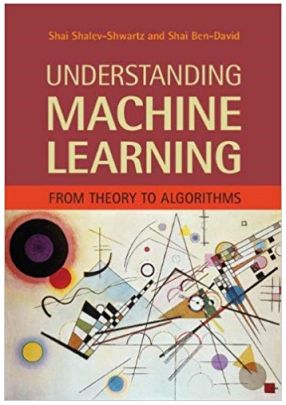


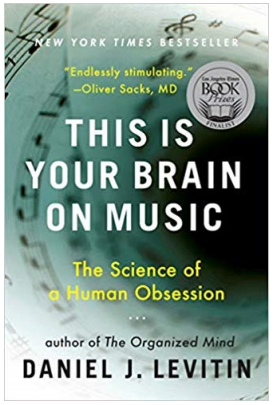




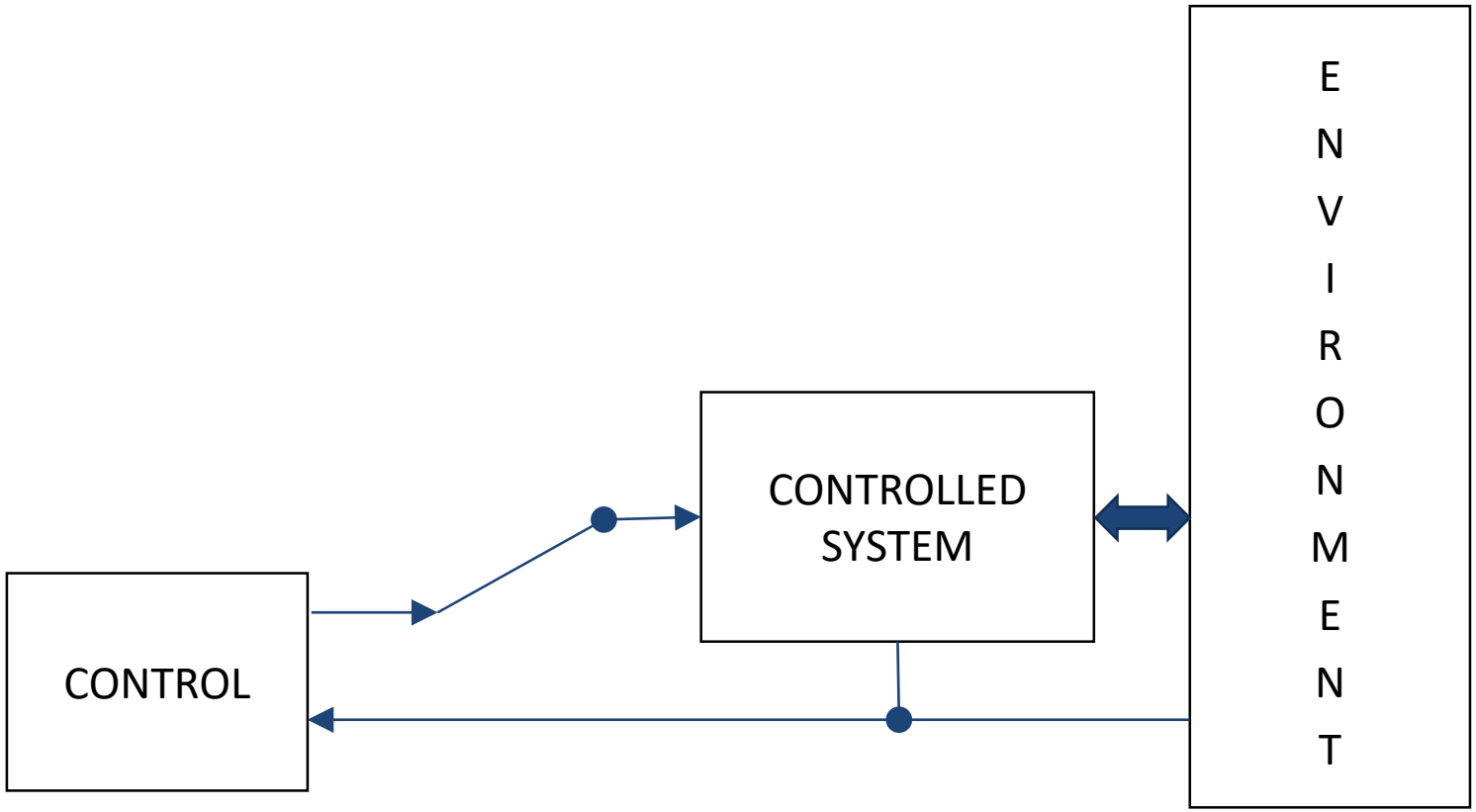








Building Trusted Systems



Building Trusted Systems: Oded's Contributions

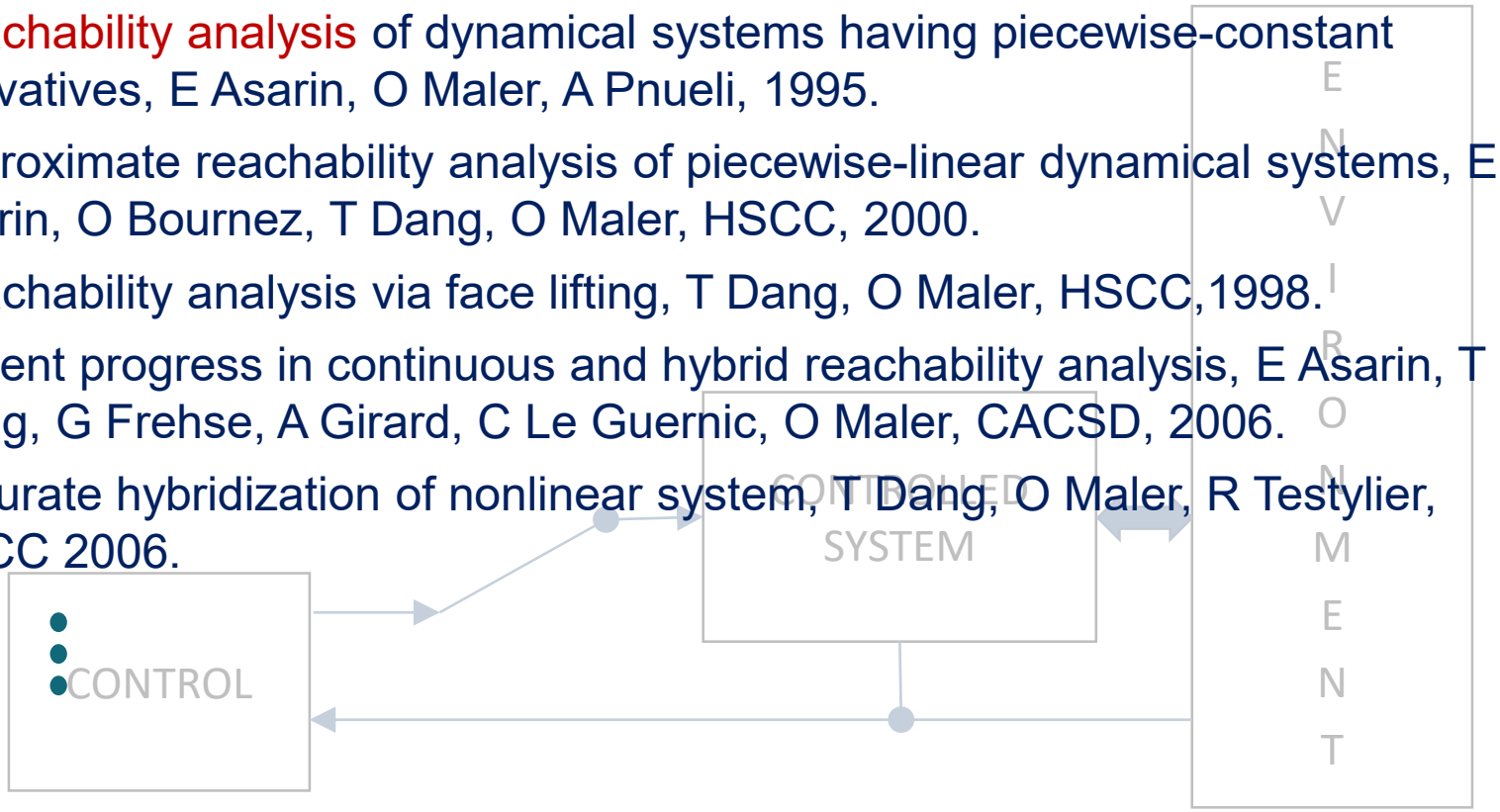
Reachability analysis of dynamical systems having piecewise-constant derivatives, E Asarin, O Maler, A Pnueli, 1995.

Approximate reachability analysis of piecewise-linear dynamical systems, E Asarin, O Bournez, T Dang, O Maler, HSCC, 2000.

Reachability analysis via face lifting, T Dang, O Maler, HSCC,1998.

Recent progress in continuous and hybrid reachability analysis, E Asarin, T Dang, G Frehse, A Girard, C Le Guernic, O Maler, CACSD, 2006.

Accurate hybridization of nonlinear system, T Dang, O Maler, R Testylier, HSCC 2006.



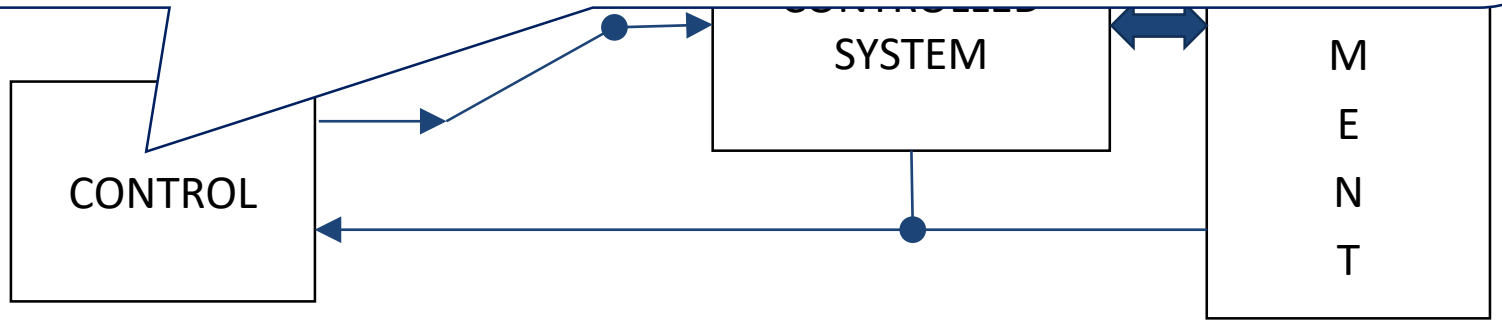
Building Trusted Systems: Oded's Contributions

Controller synthesis for timed automata, E Asarin, O Maler, A Pnueli, J Sifakis, IFAC Proceedings, 1998.

Effective synthesis of switching controllers for linear systems, E Asarin, O Bournez, T Dang, O Maler, A Pnueli, Proceedings of the IEEE, 2000.

Control from computer science, O Maler, Annual Reviews in Control, 2002.

From control loops to real-time programs, P Caspi, O Maler, Handbook of networked and embedded control systems, 2005.



Building Trusted Systems: Oded's Contributions

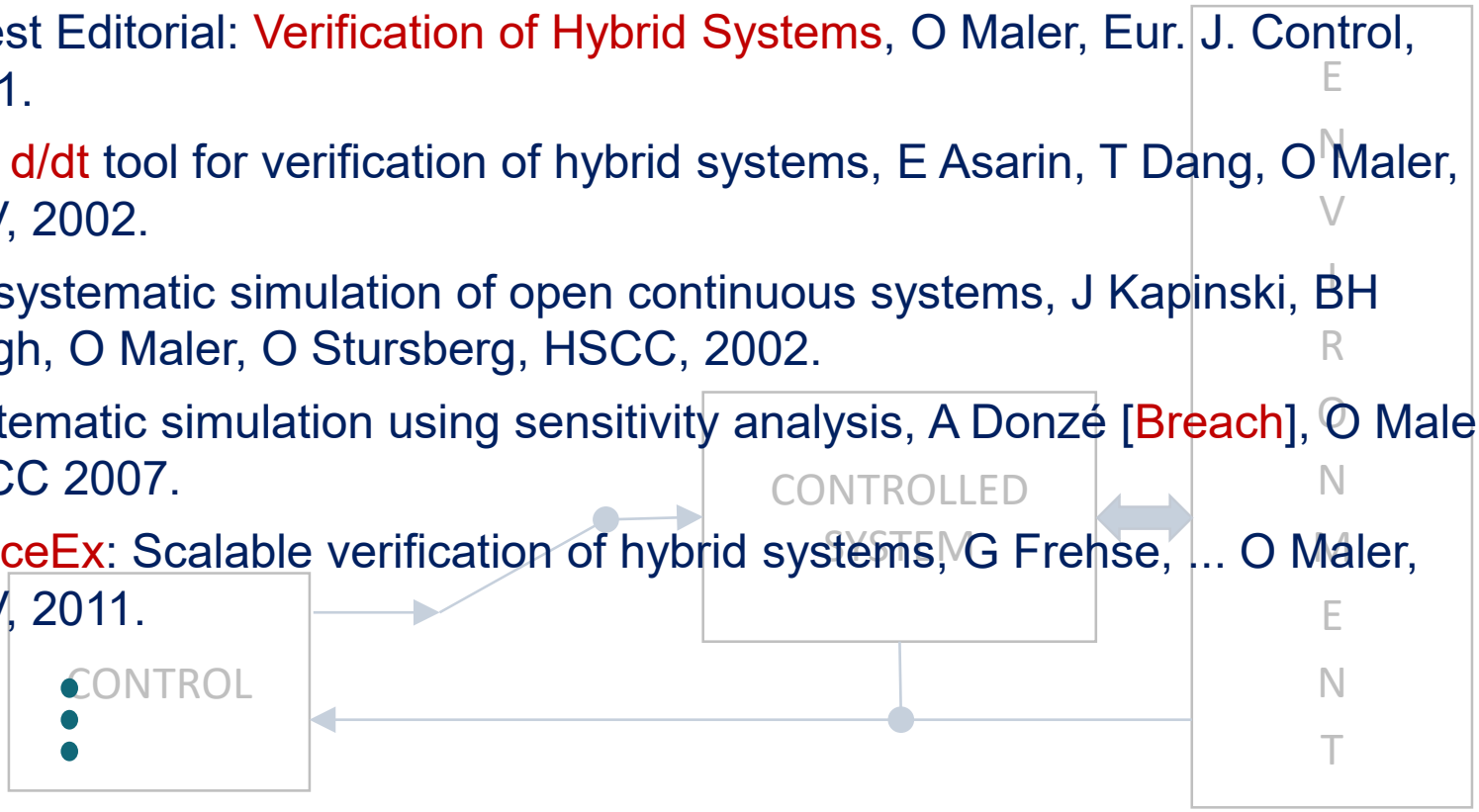
Guest Editorial: Verification of Hybrid Systems, O Maler, Eur. J. Control, 2001.

The d/dt tool for verification of hybrid systems, E Asarin, T Dang, O Maler, CAV, 2002.

On systematic simulation of open continuous systems, J Kapinski, BH Krogh, O Maler, O Stursberg, HSCC, 2002.

Systematic simulation using sensitivity analysis, A Donzé [Breach], O Maler, HSCC 2007.

SpaceEx: Scalable verification of hybrid systems, G Frehse, ... O Maler, CAV, 2011.



Buildi

Gues
2001.

The c
CAV,

On sy
Krogh

Syste
HSC

Spac
CAV,

From: Oded Maler <Oded.Maler@univ-grenoble-alpes.fr>
Sent: Monday, May 14, 2018 6:12 AM
To: Bruce H. Krogh <krogh@ece.cmu.edu>
Subject: Your retirement

Hi Bruce,

I really regret not being able to come but at least I sent a kind of a representative.. let me thank you again for the great five years of summer post-doc … including the paper on systematic simulation … By the way, when I presented the paper in a project meeting, in my way, Manfred was very unimpressed and the paper was accepted to HSCC only because I was the PC chair. You presented it in Prague in your own way and Manfred came to you and said it was very interesting.

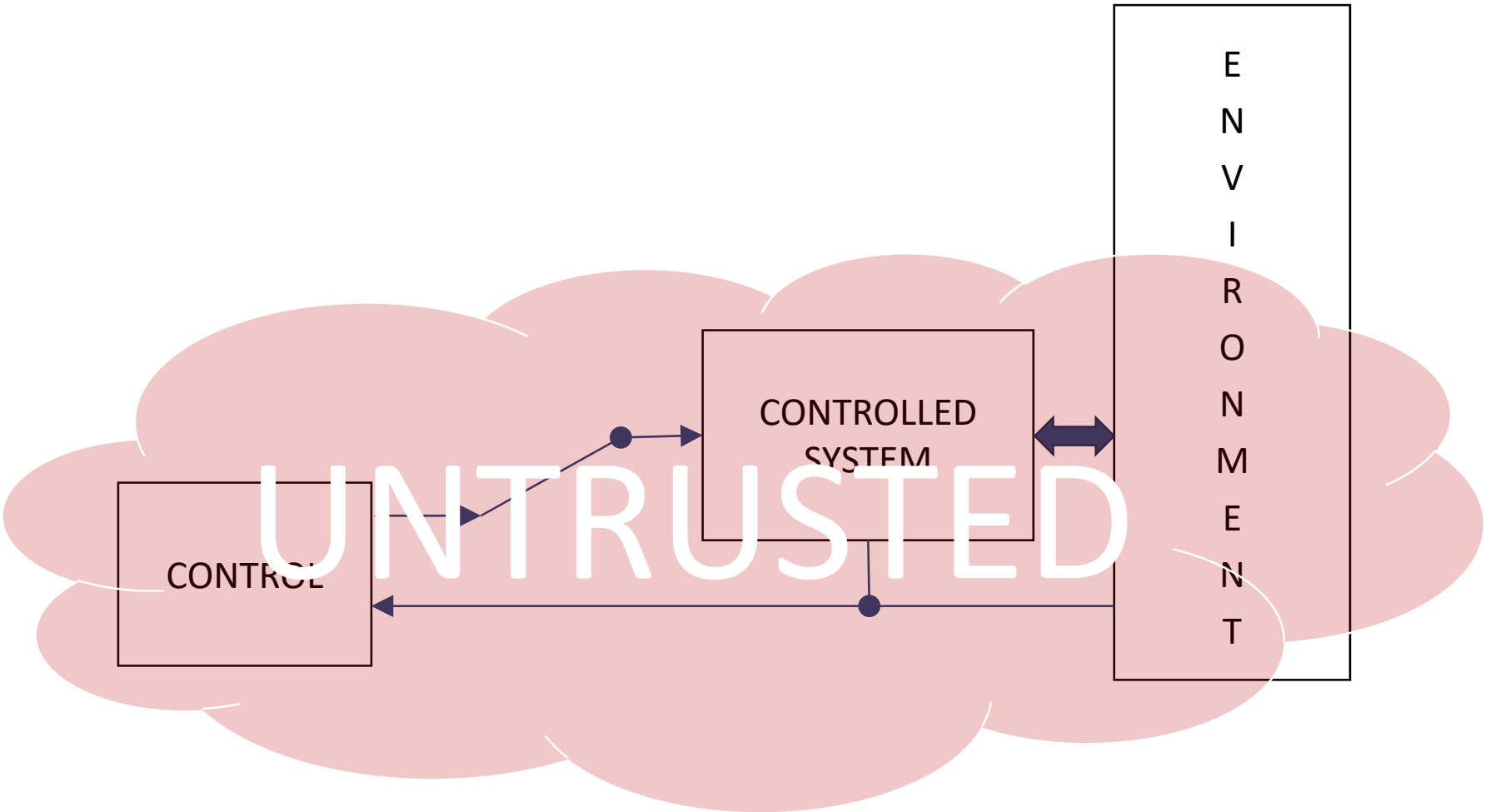
I can go endlessly in remembering anecdotes about our first encounters … but I'll stop here and wish you and Margie a good continuation.

--Oded

er,

aler,

But despite our best efforts …

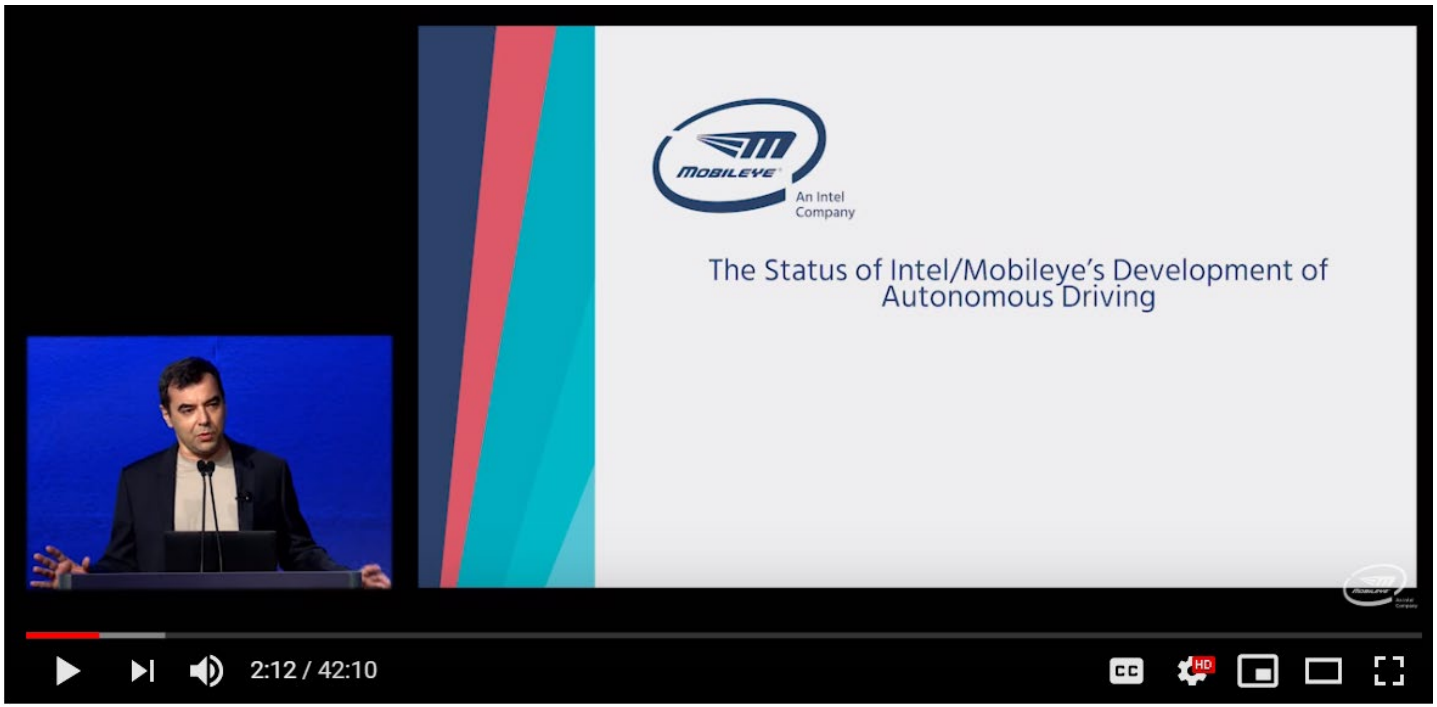


Challenge of autonomous driving

From: Oded Maler <Oded.Maler@univ-grenoble-alpes.fr>
Sent: Thursday, August 30, 2018 1:10 PM
To: Oded.Maler@univ-grenoble-alpes.fr
Subject: Fwd: video on autonomous driving

https://www.youtube.com/watch?v=yOJXA3Cs6hY

Oded (mobile)



Prof. Amnon Shashua at 2018 Intel Capital Global Summit

The other video from August 30 …

From: Oded Maler <Oded.Maler@univ-grenoble-alpes.fr>
Sent: Thursday, August 30, 2018 3:58 AM
To: Bruce H. Krogh <krogh@ece.cmu.edu>
Subject: YouTube from the Vietnam times

https://www.youtube.com/watch?v=ZY_nq4tfi24

Vidal vs Buckley - Crypto-Nazi Debate (Best Quality)

What are the new challenges for system design? [Sifakis]*

- Increasing complexity of
  - enabling technologies (components)
  - environments
  - missions
  - systems (architectures)
- run-time uncertainty/unpredictability
- push for autonomy

*J. Sifakis, System Design in the Era of IoT — Meeting the Autonomy Challenge, invited paper, *Proceedings of the 1st International Workshop on Methods and Tools for Rigorous System Design* (MeTRiD 2018), Thessaloniki, Greece, April 2018, pp. 1–22. Received 27/05/2018 after Oded wrote: "Joseph, I think Bruce might also be interested in your paper."

Why new system design methods are needed [Sifakis]

Traditional Systems	Emerging Autonomous Systems
• programmed behavior	• evolvable behavior
• controlled environments	• non-predictable, changing environments
• structured interactions (protocols)	• complex interactions
• correctness at design time	• correctness ensured through adaptation
• human backup	• no human backup

Prevailing attitudes about the lack of rigorous methods [Sifakis]

Resigned realism. Charge ahead and accept the risks because the benefits will be so great.

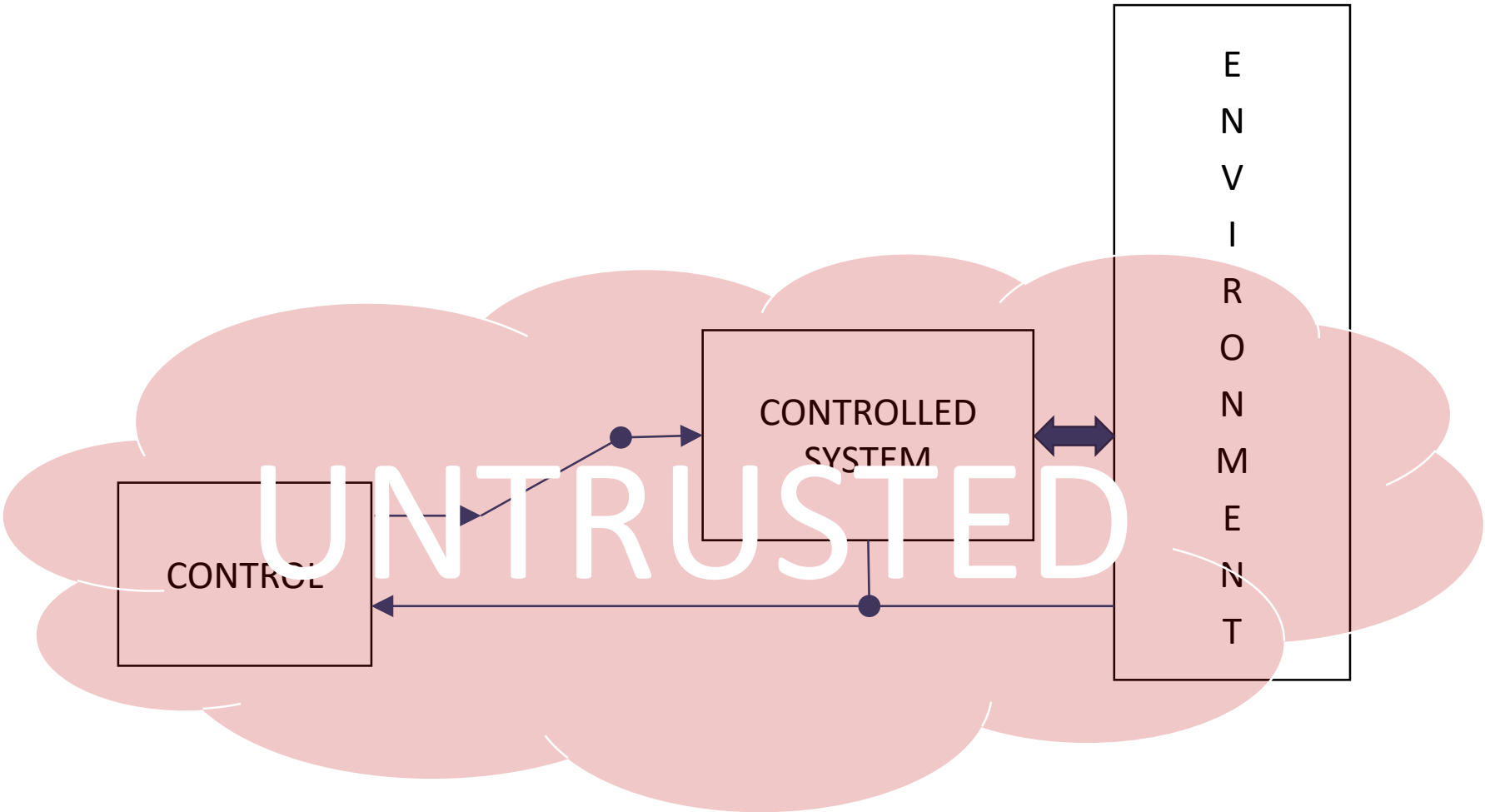
Unbridled optimism. We have the right tools, it's just a matter of time.*

Blind faith in empirical methods. Rigorous approaches are inherently inadequate; complex problems can be solved only by empirical methods.

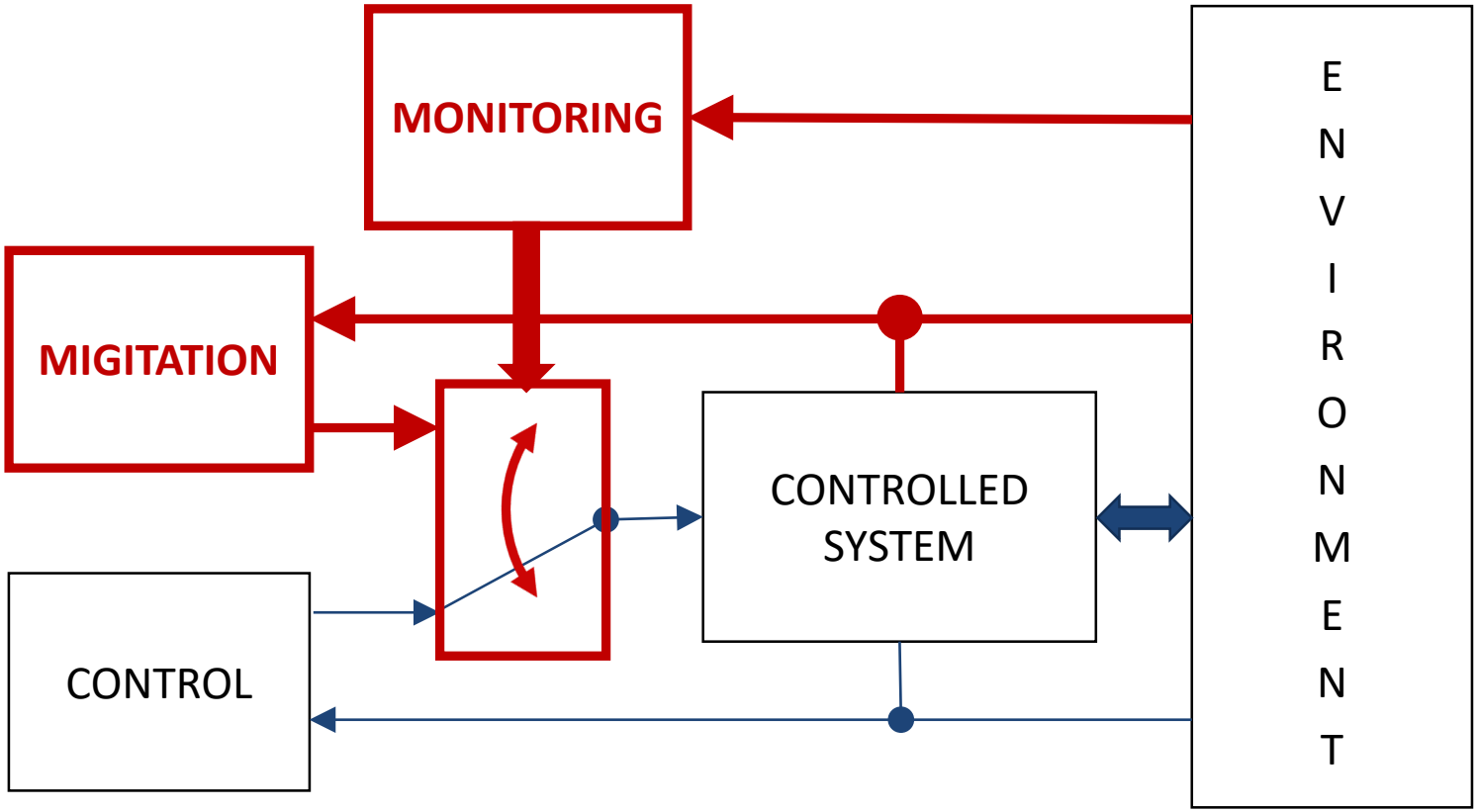
*"I almost view [autonomous cars] as a solved problem. We know what to do, and we'll be there in a few years."

Elon Musk, Nvidia GPU Technology Conference
March 17, 2015.

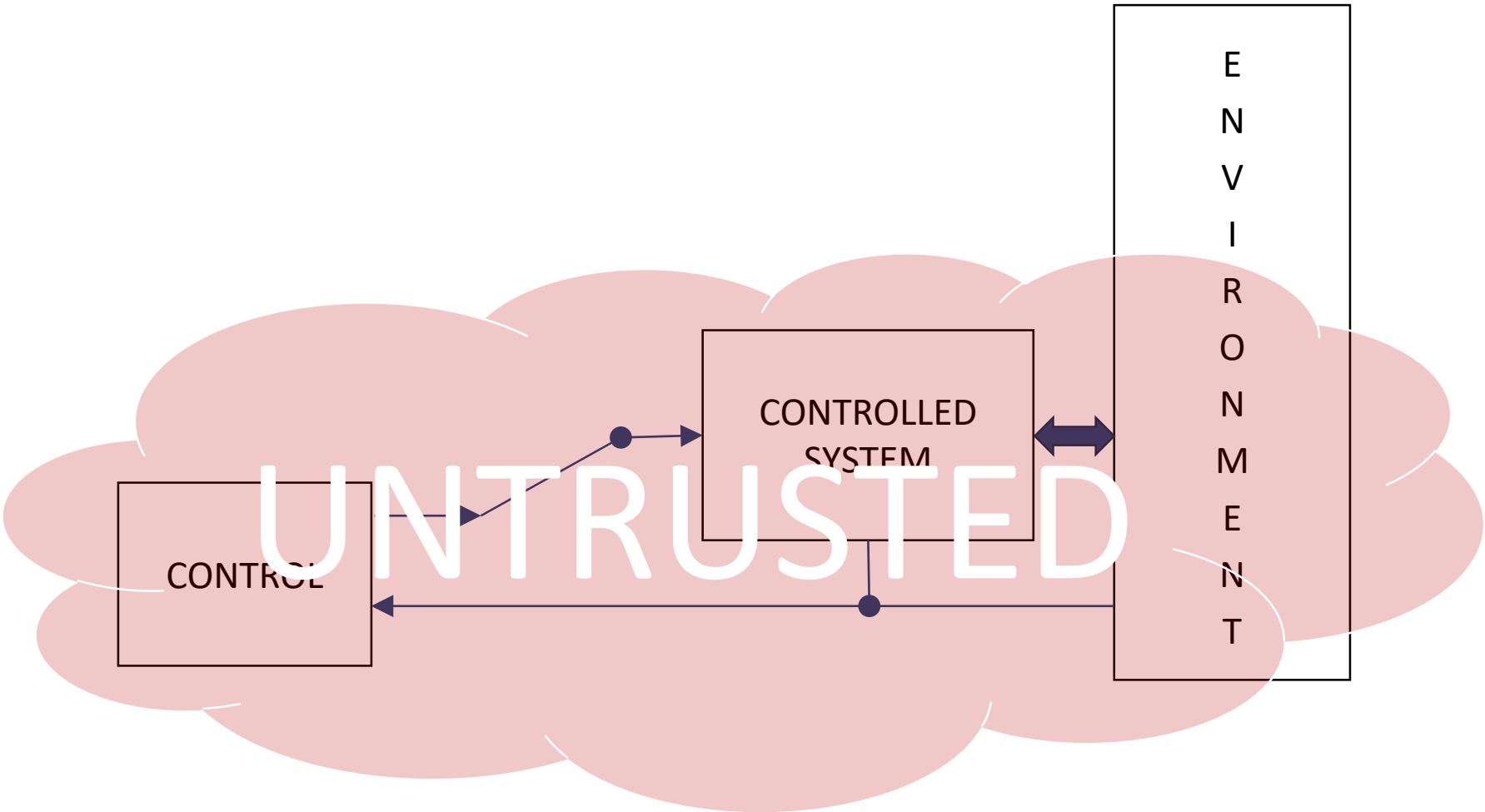
Building Trusted Systems from Untrusted Components



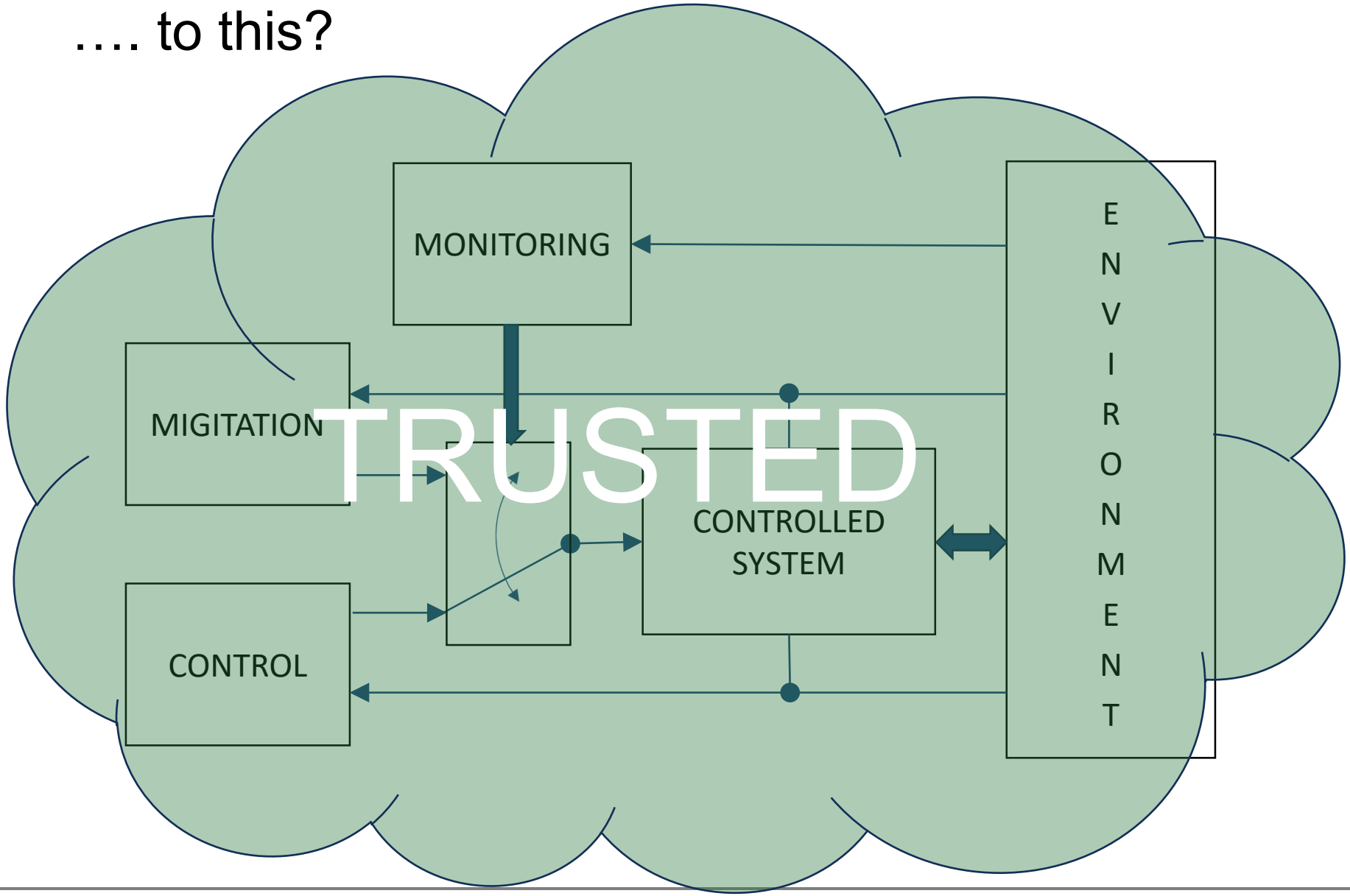
Building Trust through Monitoring and Mitigation



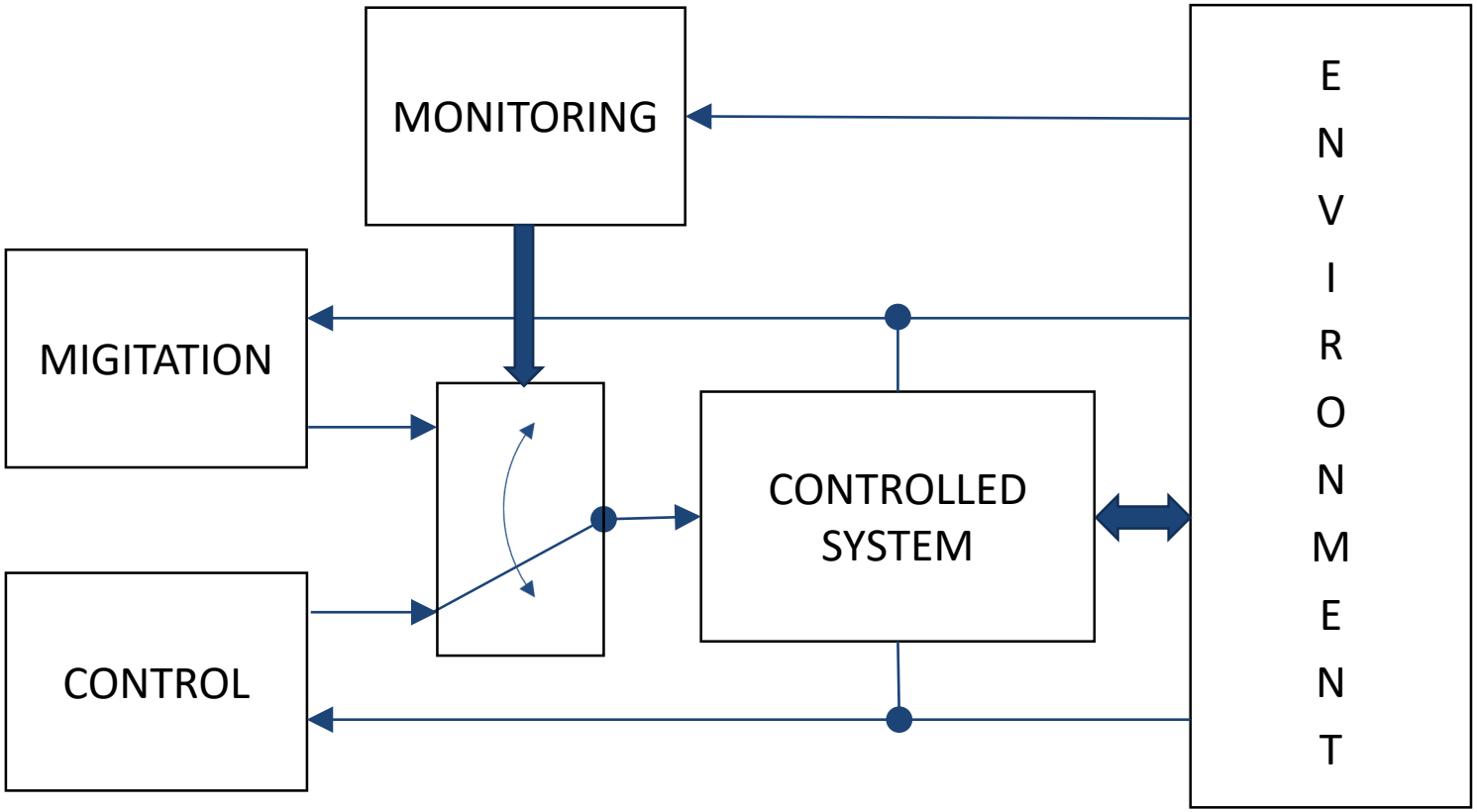
How can we go from this …



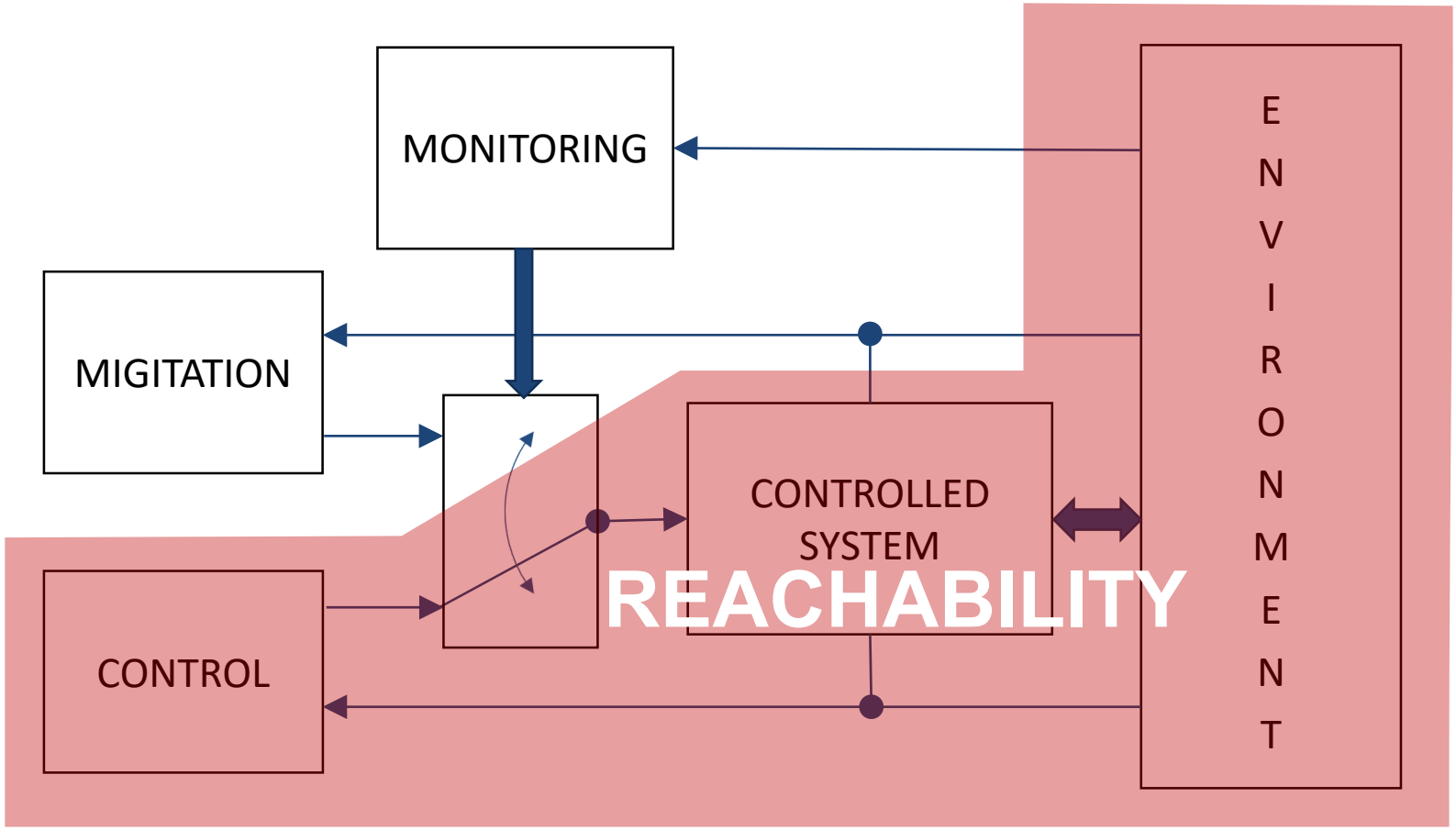
…. to this?



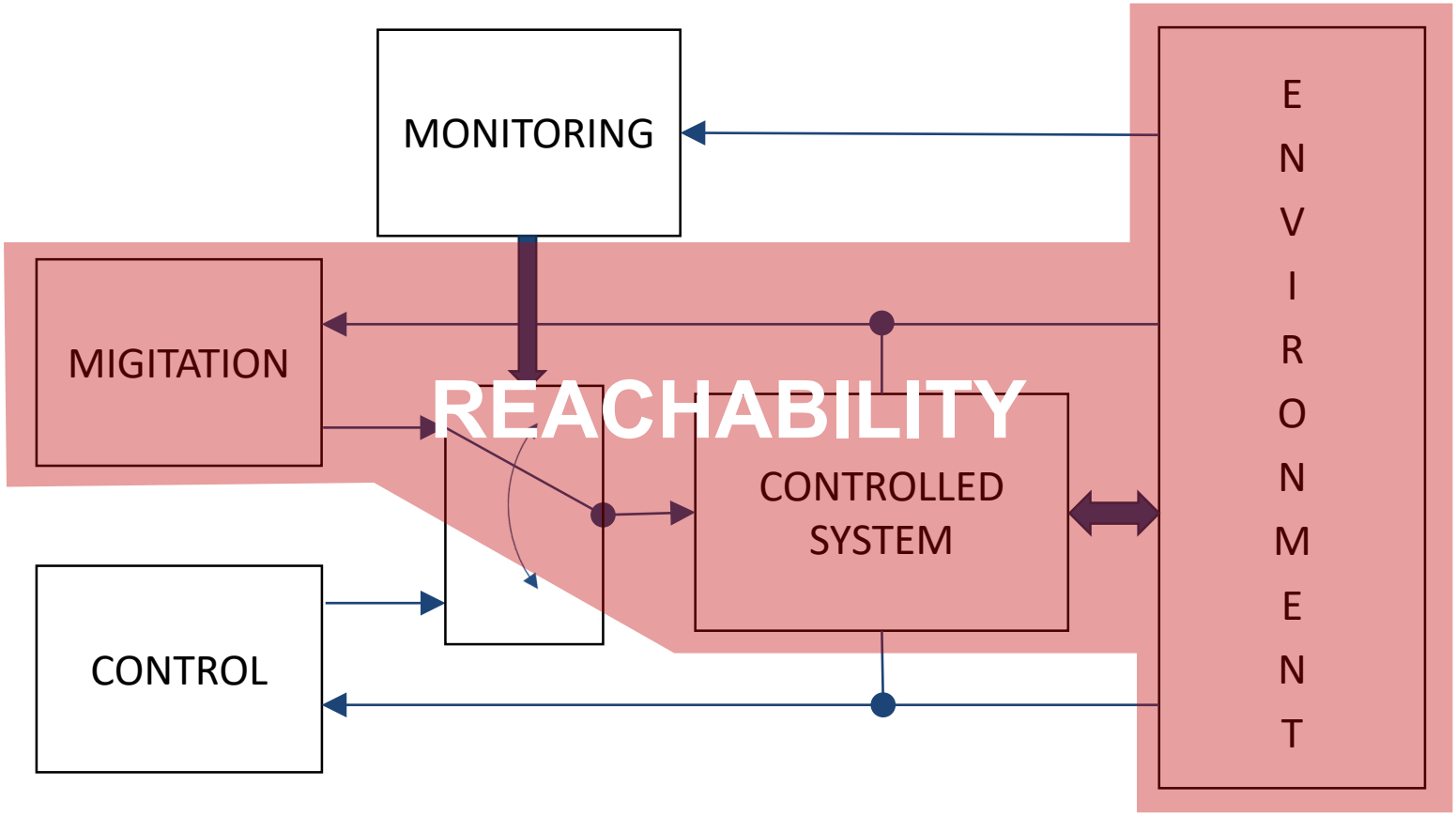
Building Trusted Systems: Oded's Contributions



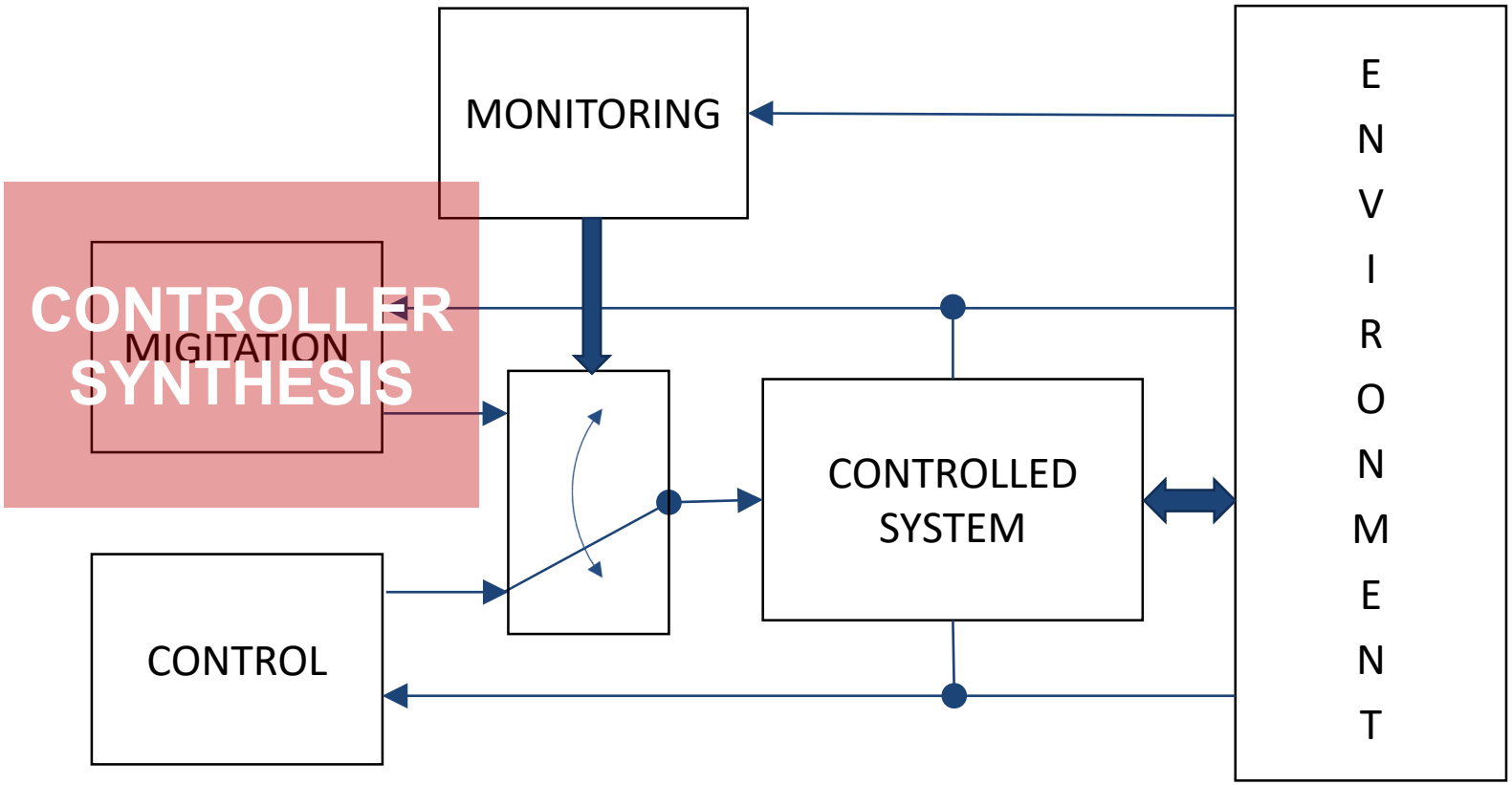
Building Trusted Systems: Oded's Contributions



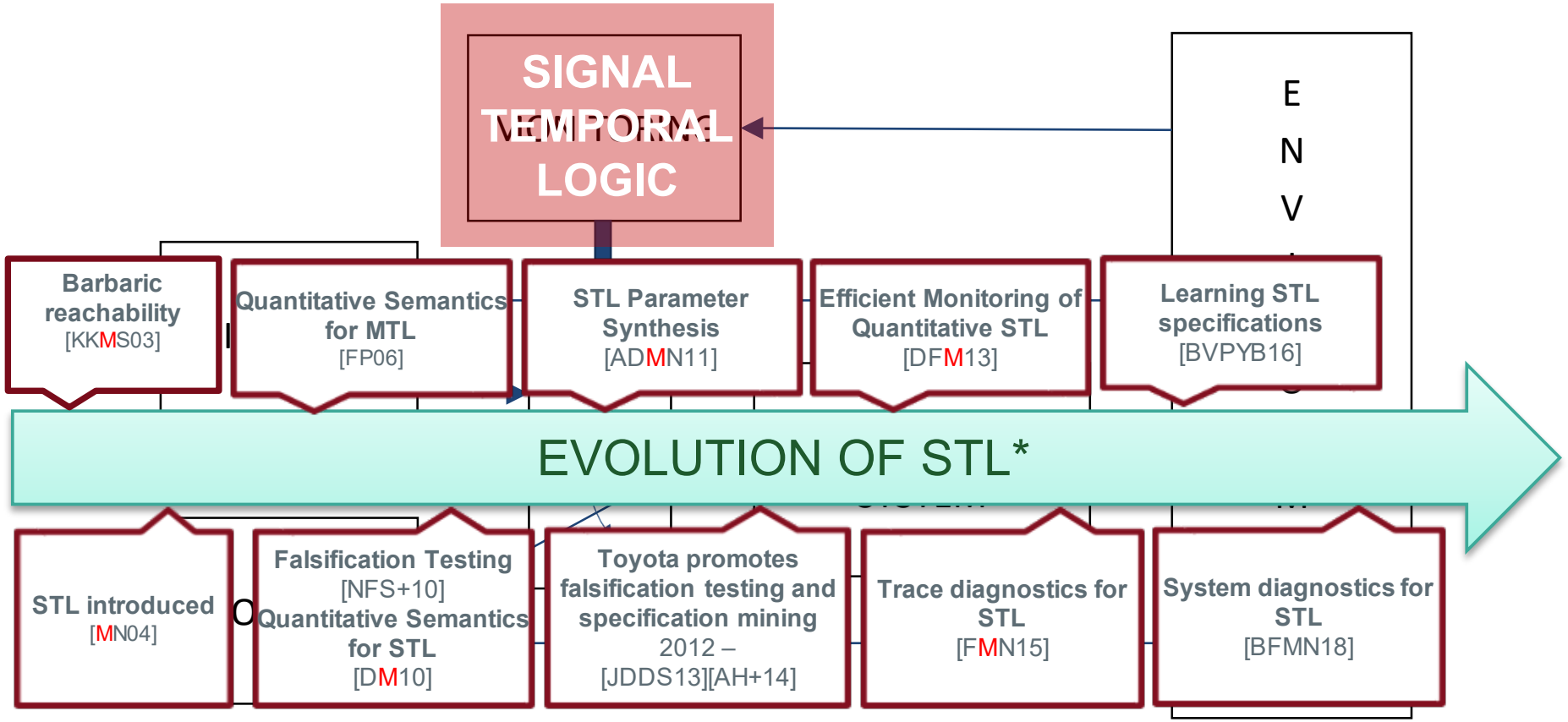
Building Trusted Systems: Oded's Contributions



Building Trusted Systems: Oded's Contributions

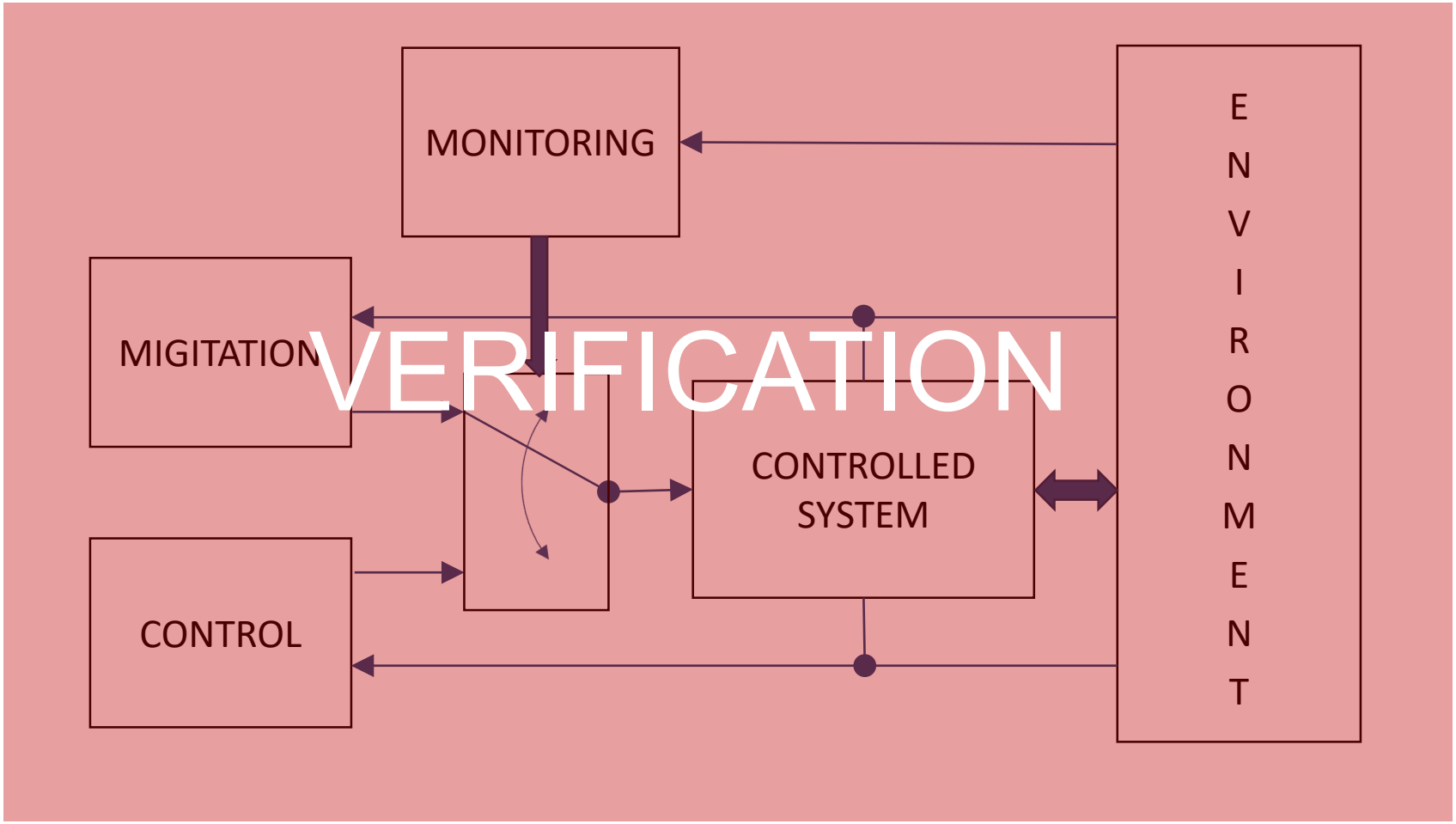


Building Trusted Systems: Oded's Contributions

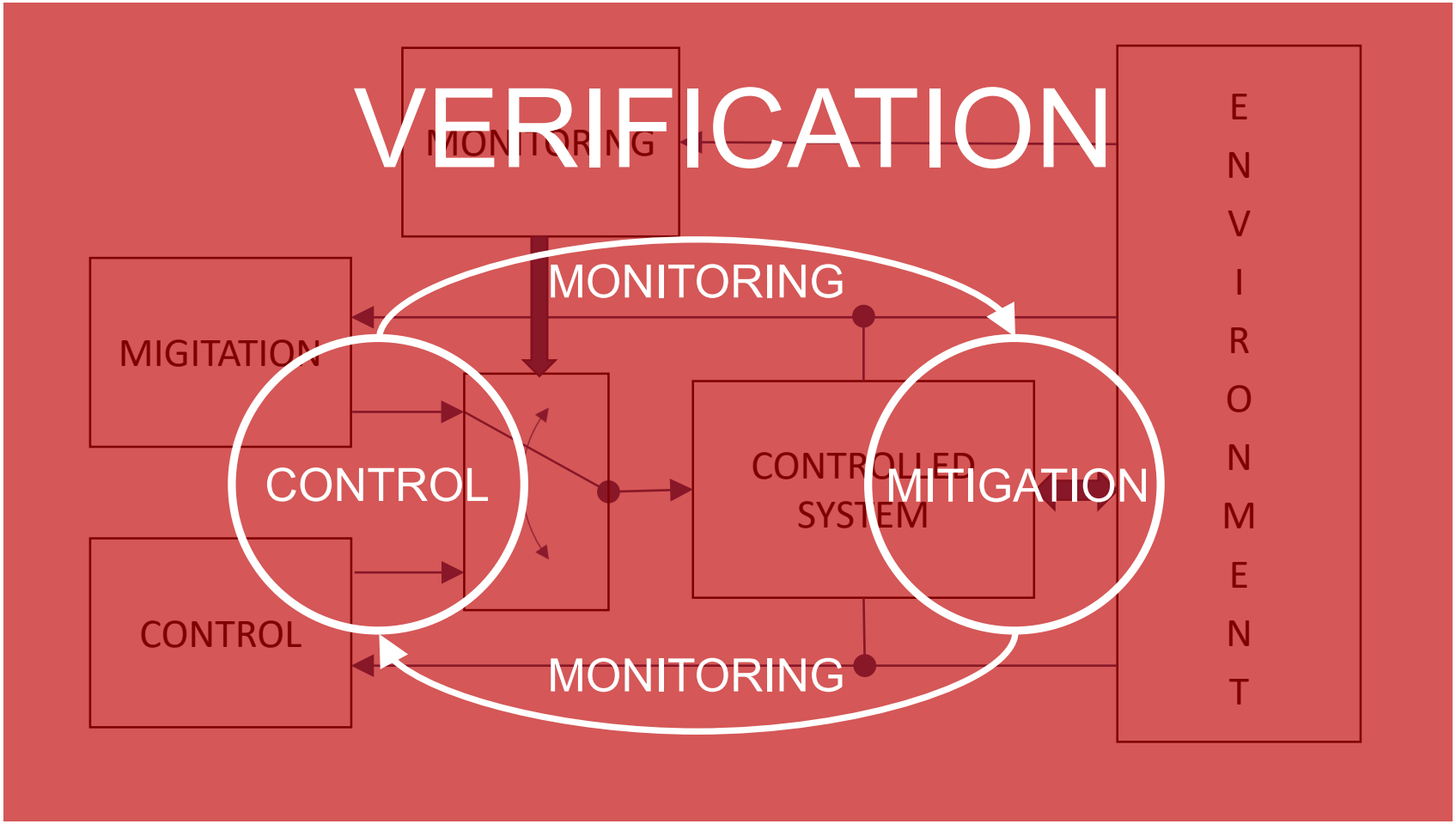


* Dejan Ničković, Oded Maler: A memory box full of diamonds, MT-CPS 2019.

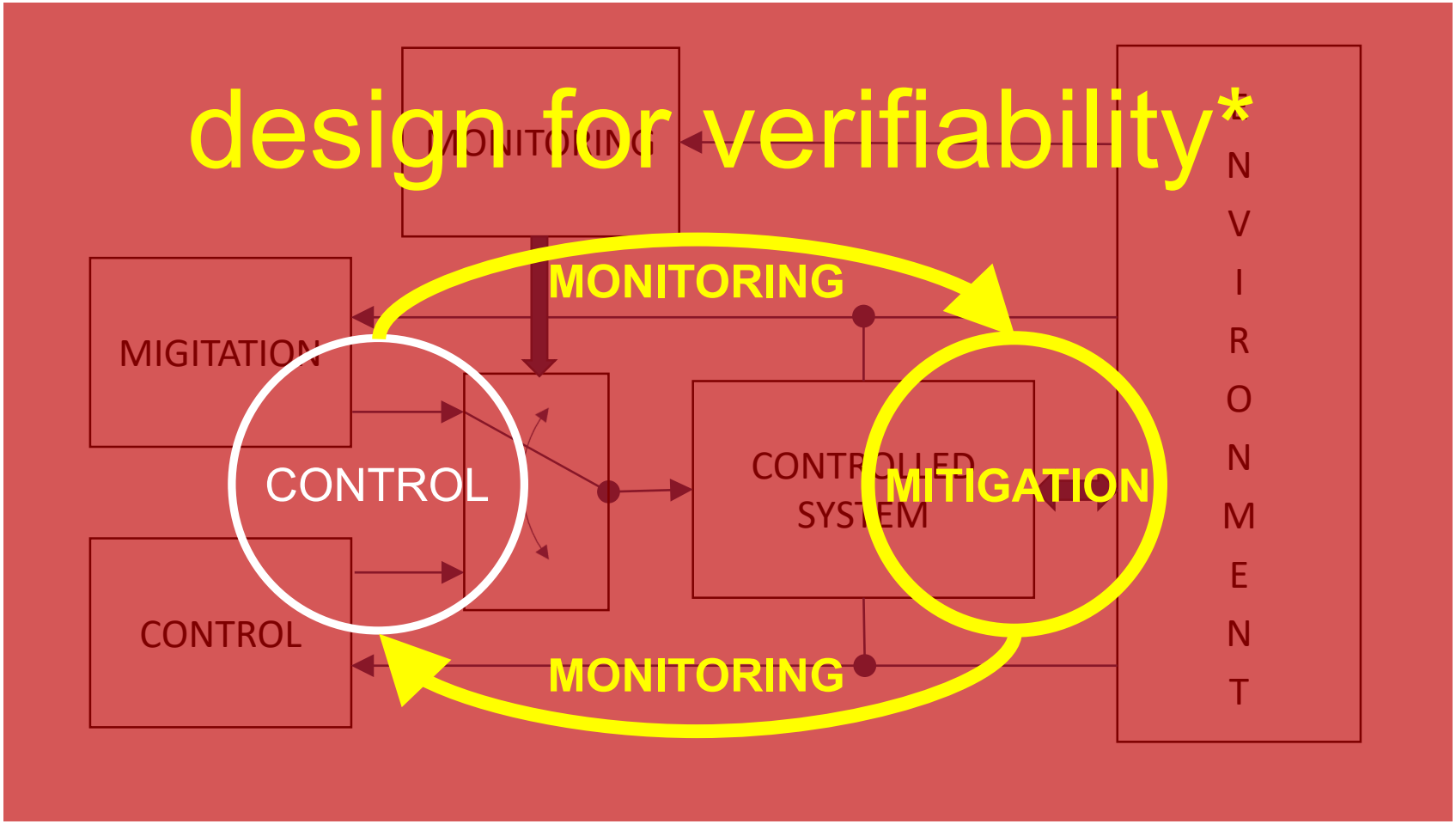
Building Trusted Systems: Oded's Contributions



Building Trusted Systems: Oded's Contributions



Building Trusted Systems from Untrusted Components



* L. Sha, Using simplicity to control complexity, IEEE Software, July/Aug 2001, 20-28.

Building Trusted Systems from Untrusted Components

in memory of Oded Maler