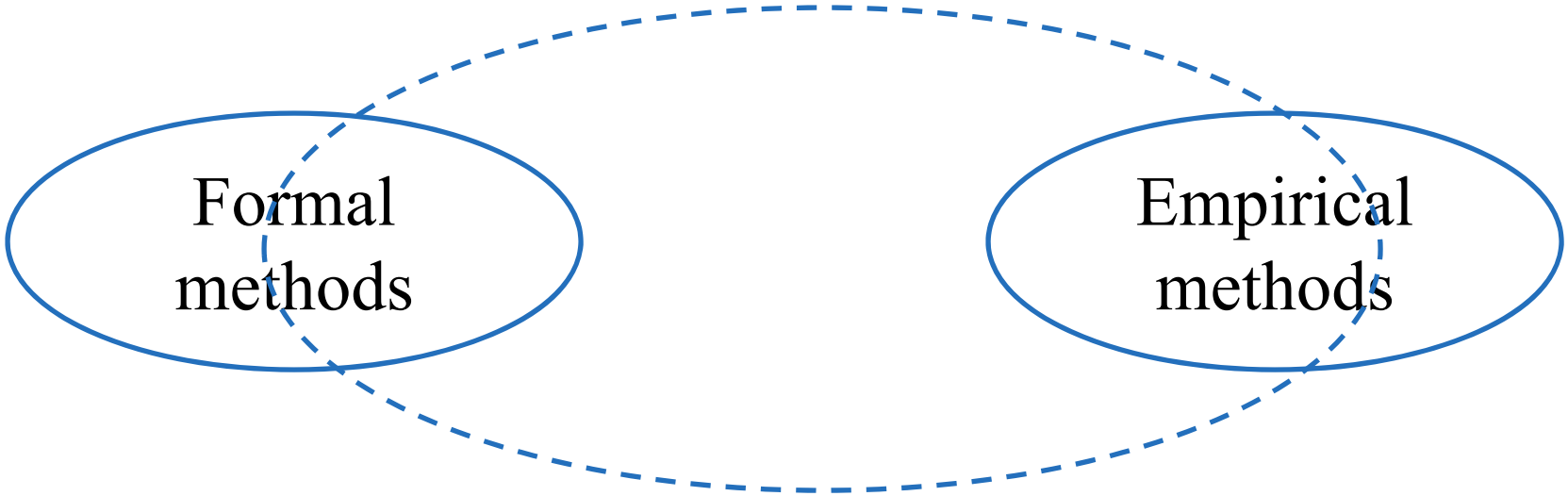
High assurance systems

Rami Melhem (U. of Pittsburgh)

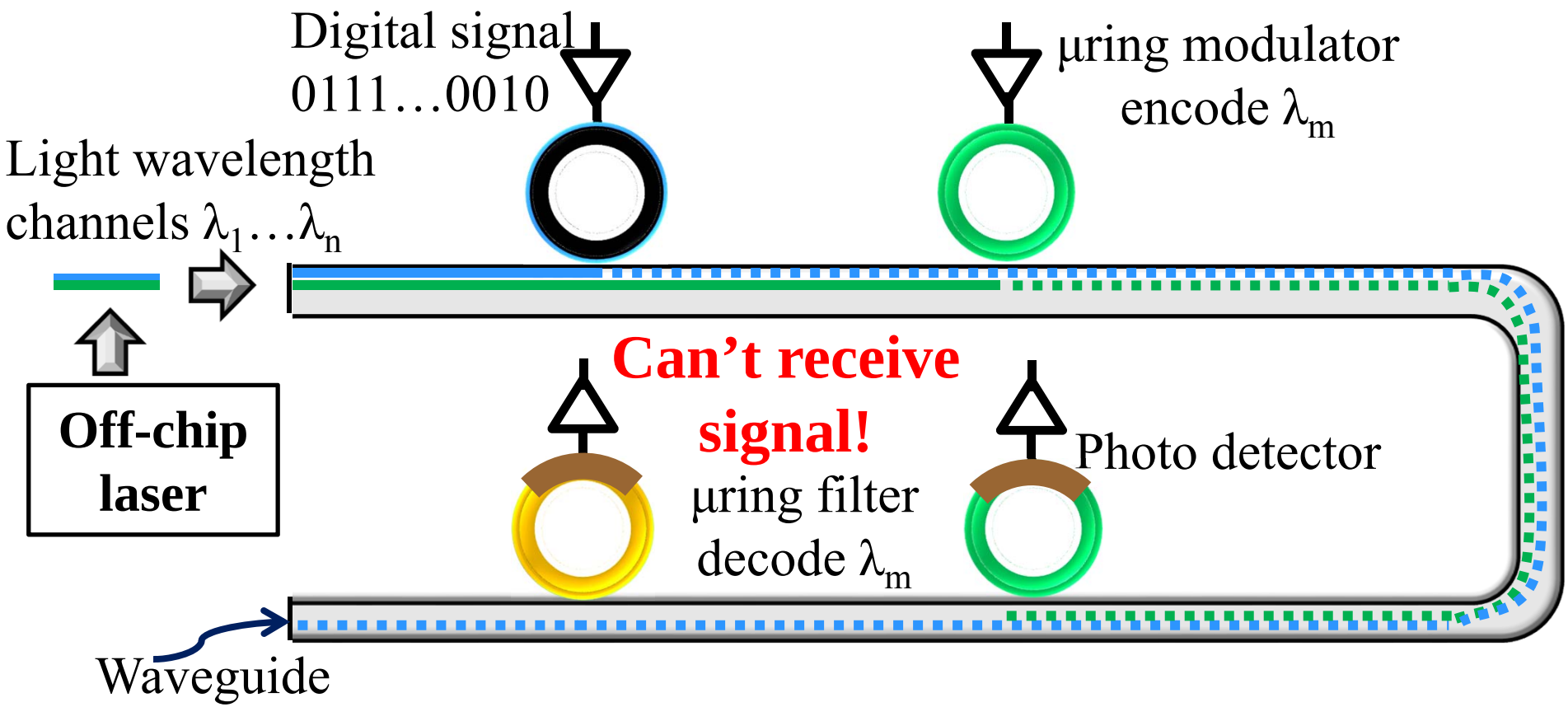
Ensures that computation completes correctly in time with optimal use of resources



Fault-tolerance | Timing guarantees | Power management | Security

Emerging technologies: nanophotonics & phase change memory

1. Tolerating Process Variations in Nanophotonic On-chip Networks



Challenge: Tolerance to process and temperature Variation (PV)

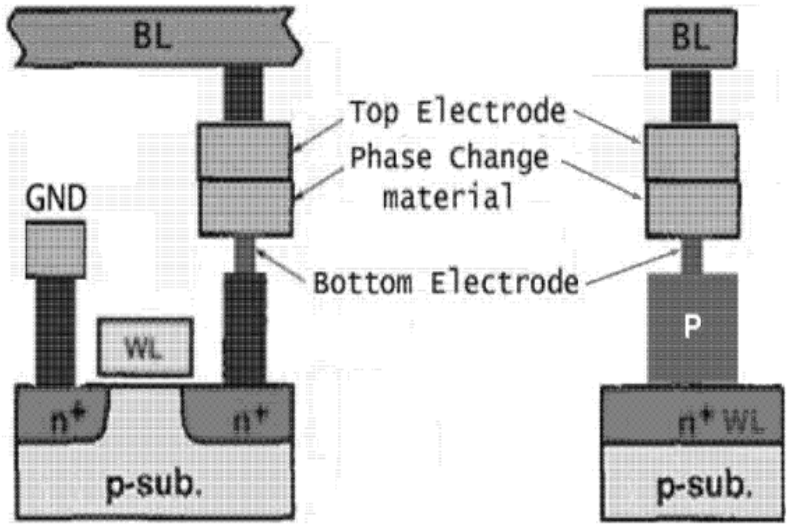
2. New error correction schemes for stuck at faults

Phase Change Memory (PCM)

A power saving memory technology

- Solid State memory made of germanium-antimony alloy
- Switching states is thermal based (not electrical based)

  - Samsung, Intel, Hitachi and IBM developed PCM prototypes (to replace Flash).



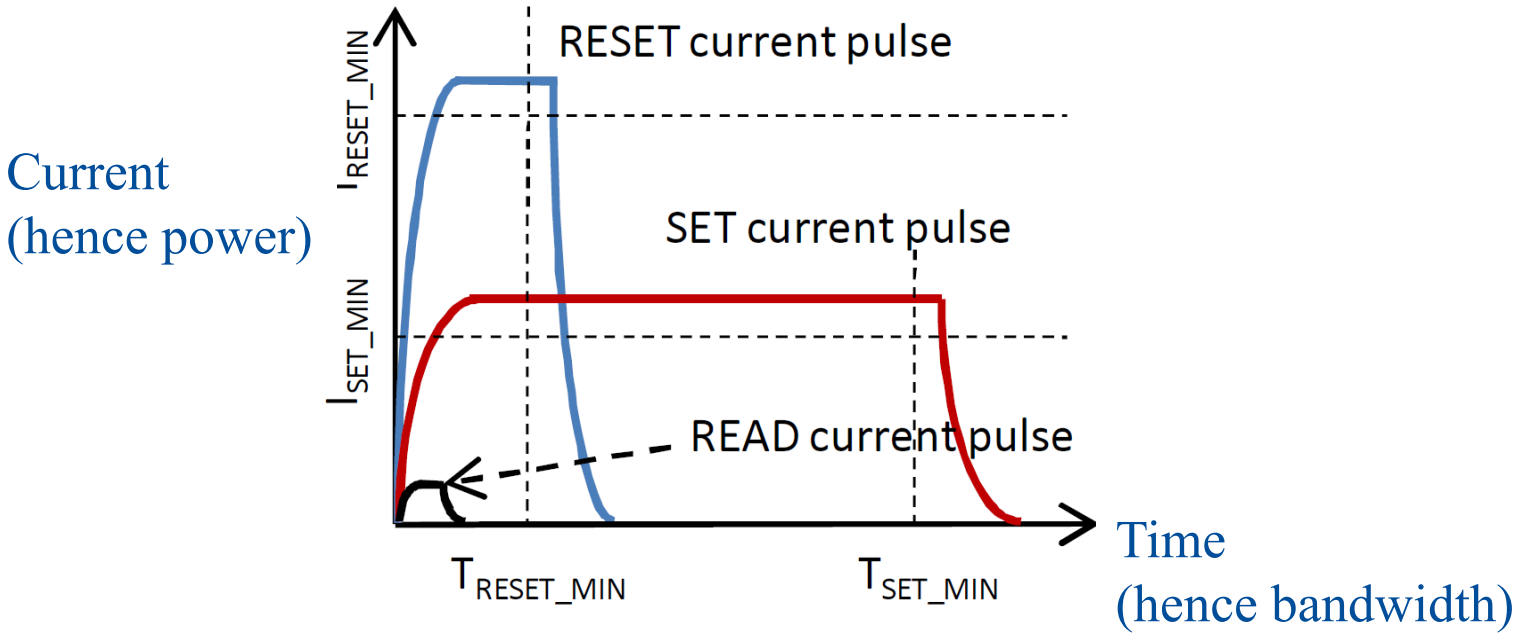
Properties of PCM

- Non-volatile but faster than Flash
- Byte addressable but denser and cheaper than DRAM
- Low power read and standby
- Not susceptible to single event upsets and hence do not need ECC
  - Errors may occur only during write (not read)
- Scalable: at least to 32nm and beyond (9nm)

Sounds wonderful – but where is the catch?

The Catch!!

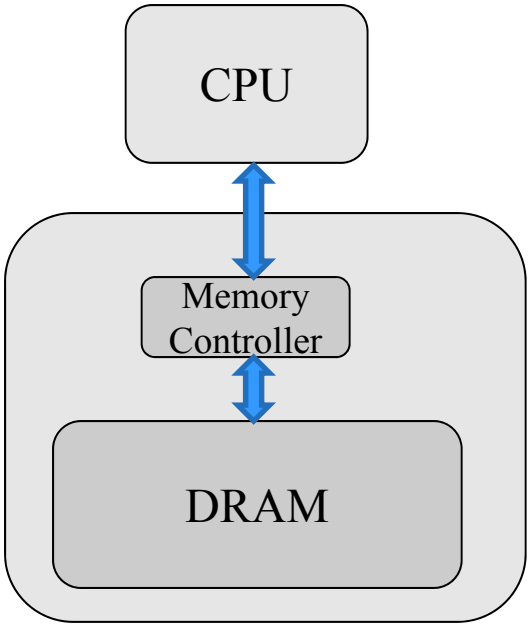
- Slower than DRAM, especially for write
- Low endurance: a cell fails after 10^7 writes (10^{15} for DRAM)
- Asymmetric Read/Write energy consumption
- Asymmetry of writing 0's and 1's



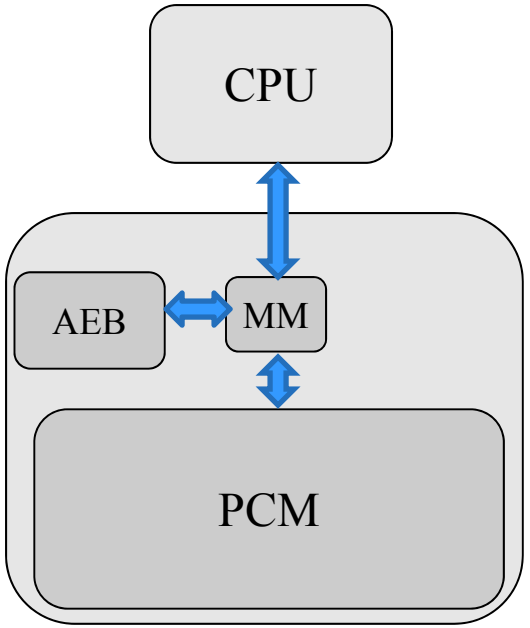
Ongoing work

- An error correction scheme for stuck-at fault models
  - Worn-out cells get stuck at 0/1 but can still be read
  - A worn-out cell can be classified as either stuck-at-right(SA-R) or stuck-at-wrong(SA-W) depending on the data pattern
- Identify a set containing the stuck-at-wrong cells
  - Some non-faulty(NF) cells could possibly be members of the set but none of the stuck-at-right cells
- At read time, invert the values read from the identified set

A Storage Class Memory Architecture for Energy Efficient Data Centers



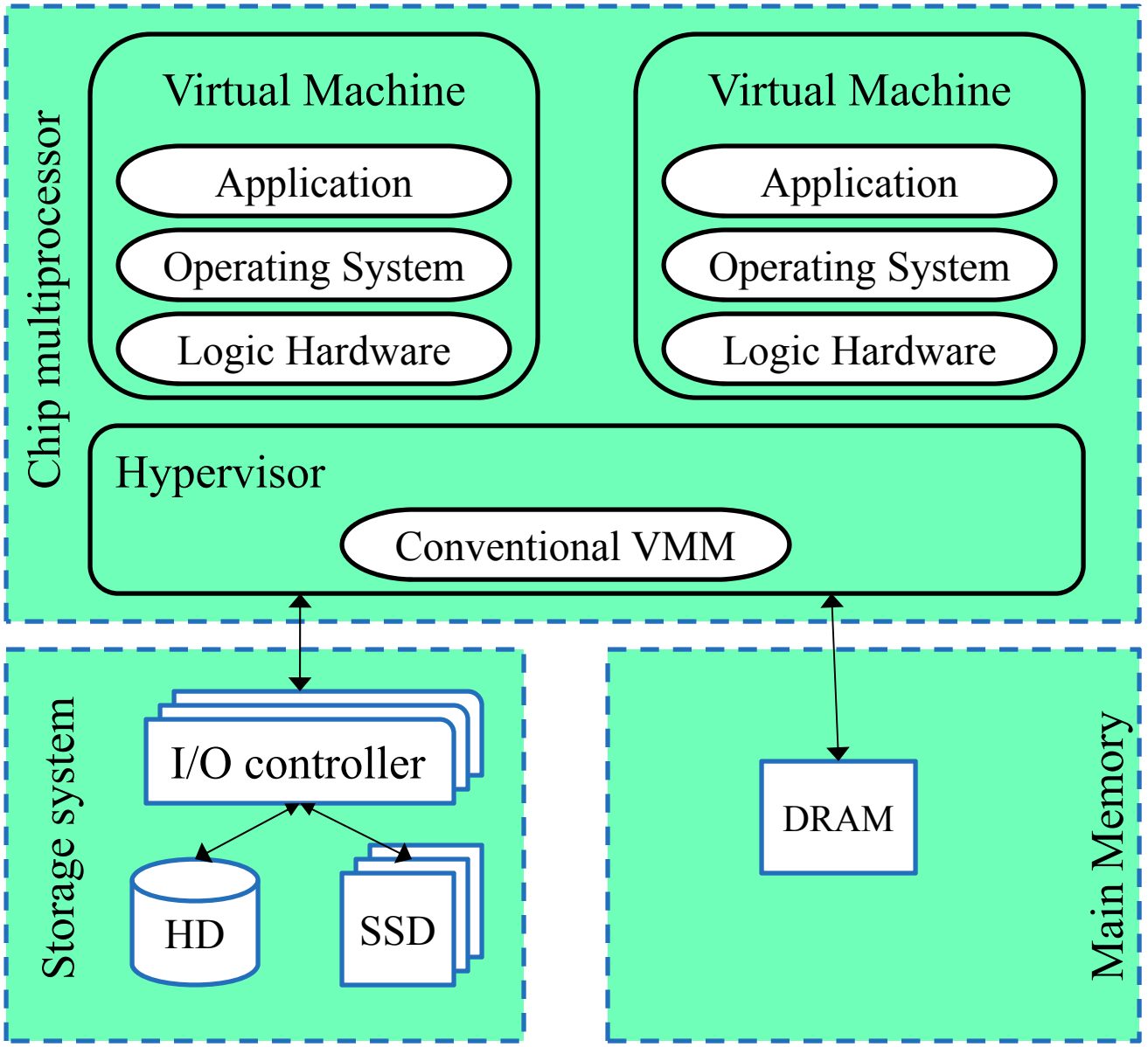
Traditional architecture



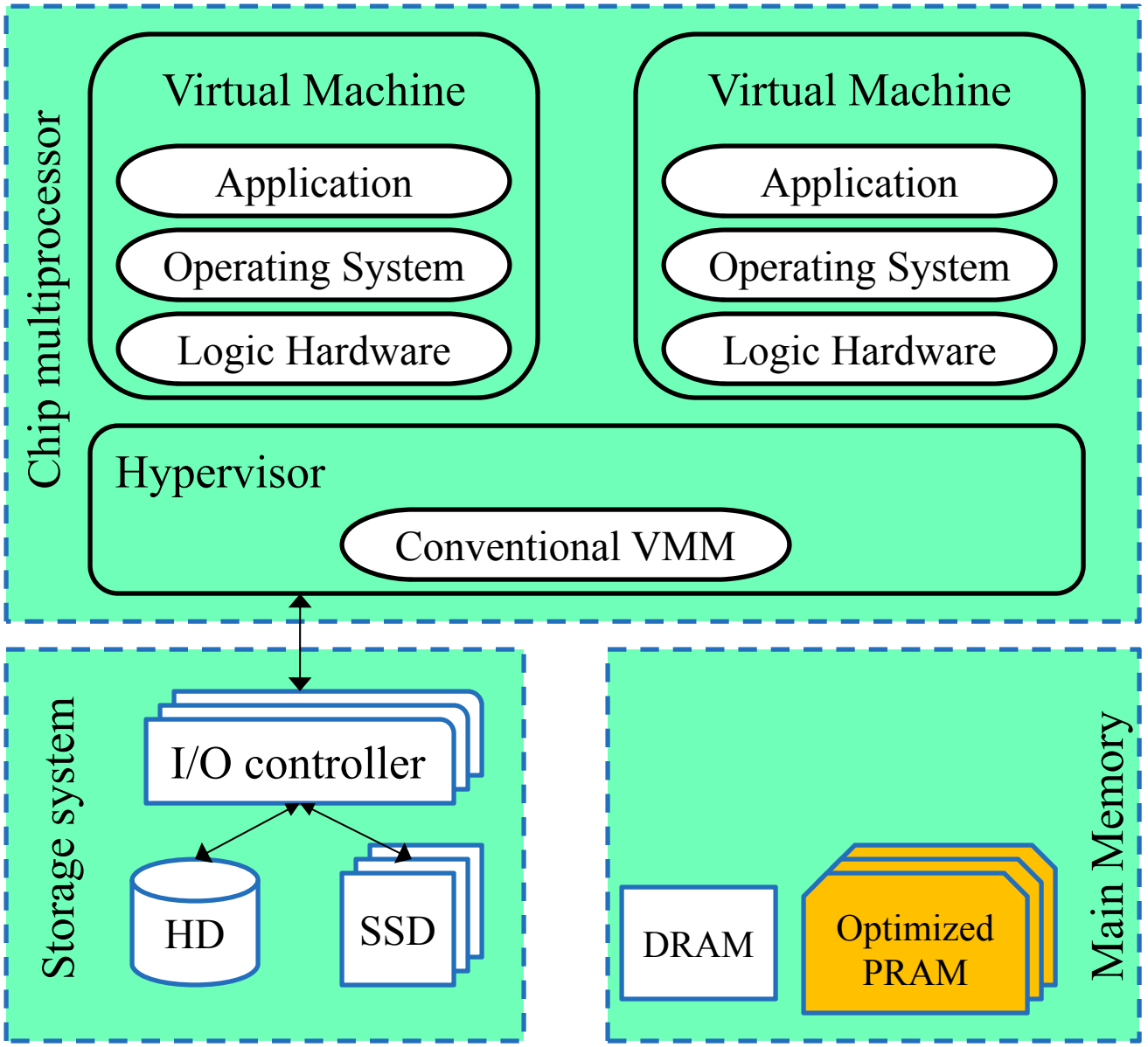
Hybrid architecture

Advantages: cheaper + denser + lower power consumption
Challenges: endurance, asymmetry, delay

A cross-layer approach

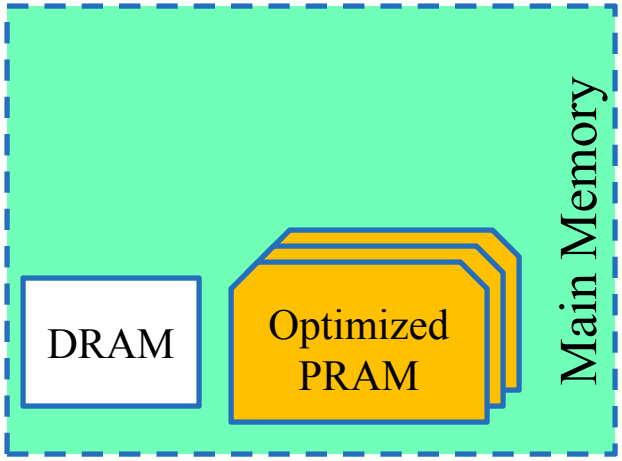


1) OPRAM (optimized PRAM)

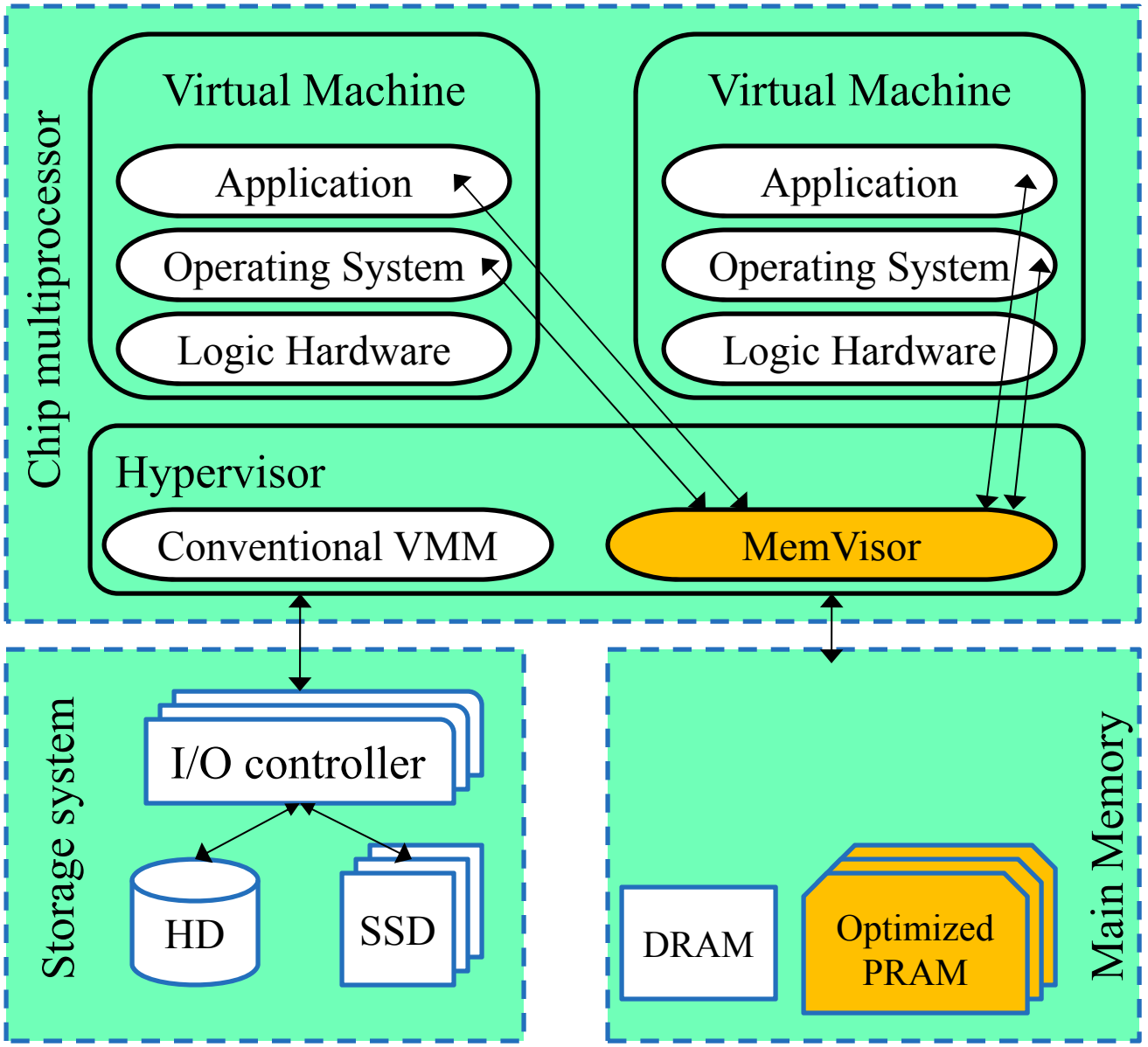


1) OPRAM (optimized PRAM)

- Optimization of PCM for main memory
  - Manage reliability (faults and wear)
  - Manage write latency
  - Manage asymmetric read/write power
- Novel interfaces with controller
- Run-time monitoring

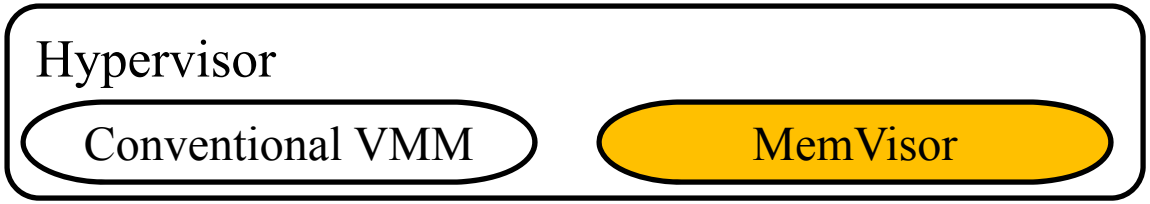


2) MemVisor


Chip multiprocessor
Virtual Machine
Application
Operating System
Logic Hardware
Virtual Machine
Application
Operating System
Logic Hardware
Hypervisor
Conventional VMM
MemVisor
Storage system
I/O controller
HD
SSD
Main Memory
DRAM
Optimized PRAM

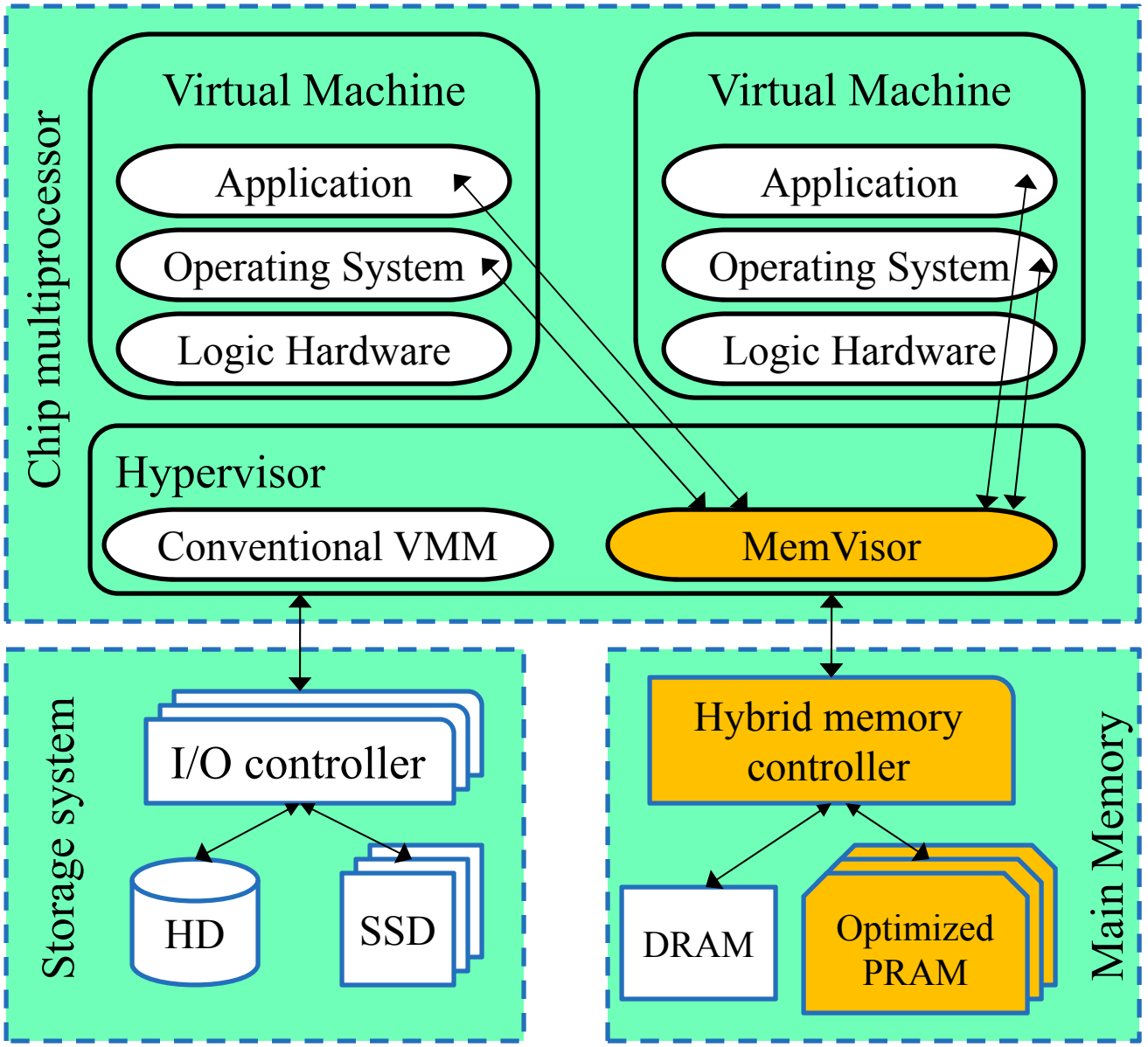
2) MemVisor

- The Memory Resource Advisor to the Hypervisor
- Allocates memory resources to virtual machines
- Maps data and code to the components of main memory
- Considers performance, energy, safety and endurance



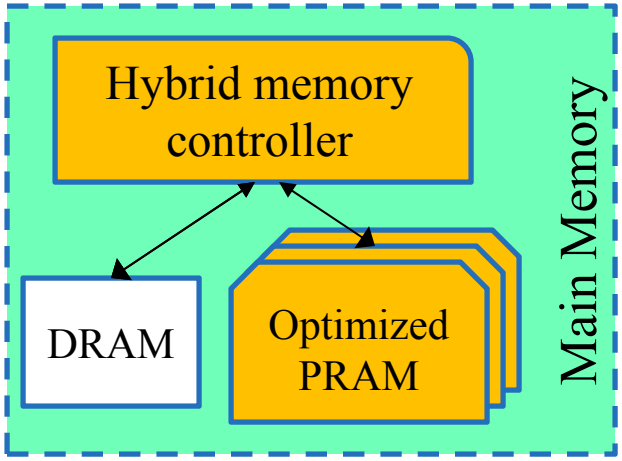
- Each VM will be managed differently based on Service Level Agreements as well a system wide goals.

3) Intelligent Hybrid controller

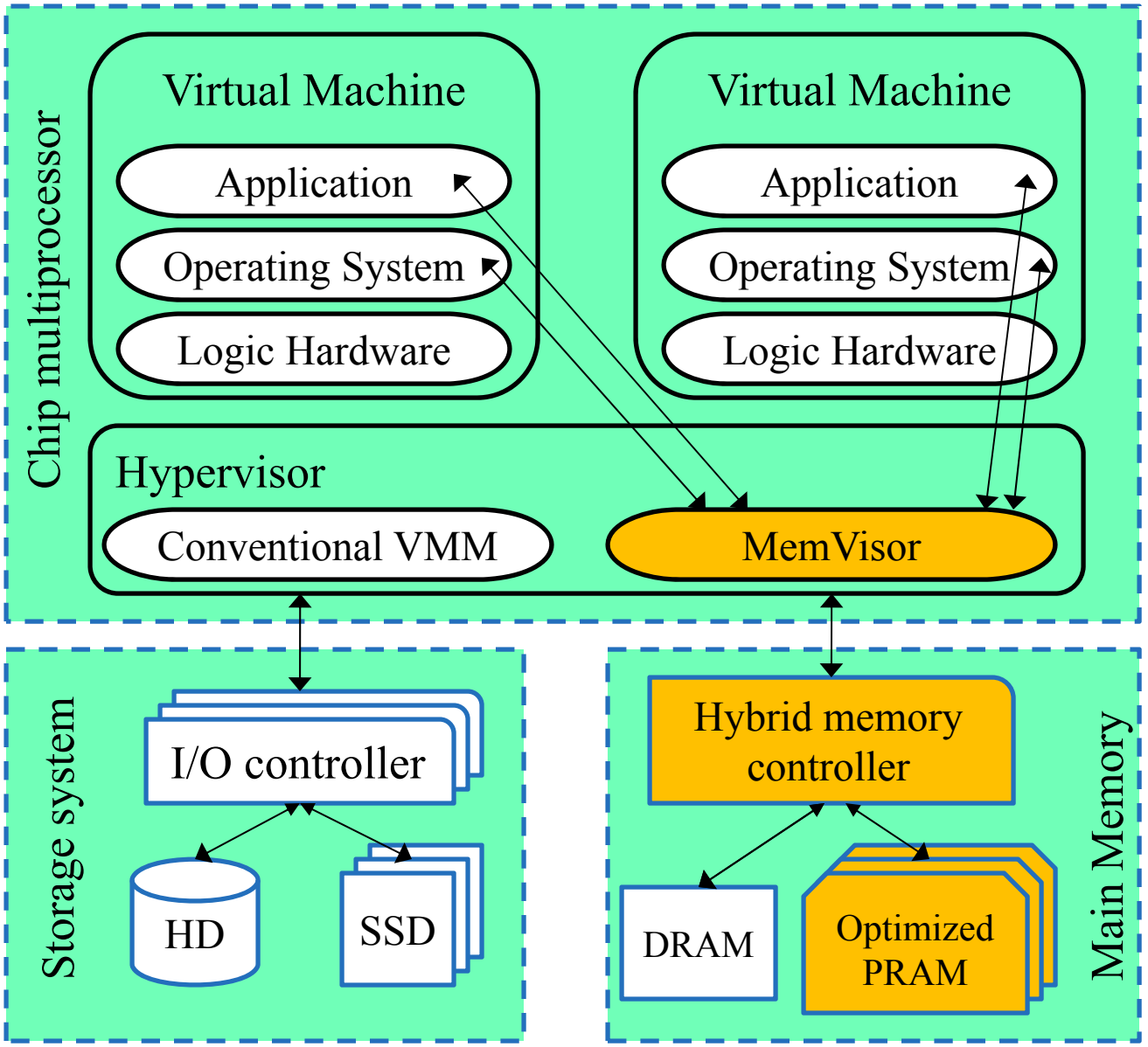


3) Intelligent Hybrid controller

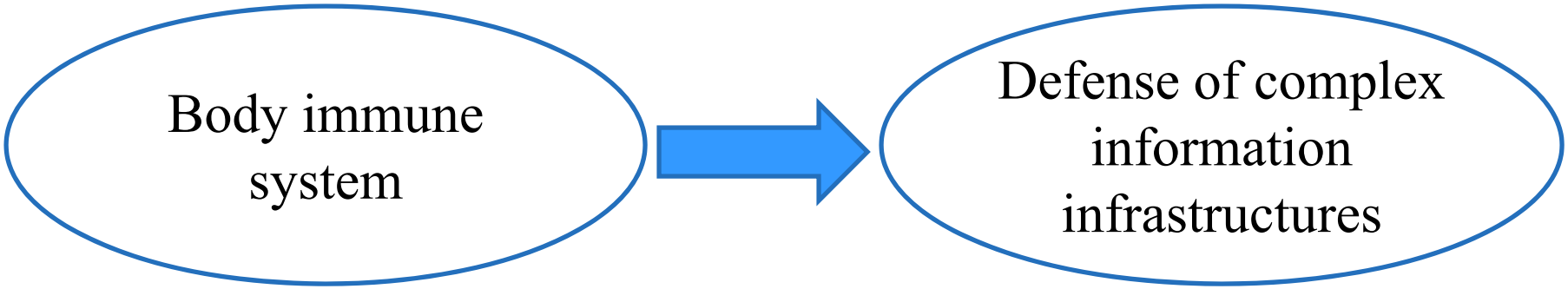
- Dynamically allocates PRAM and DRAM resources
- Accepts commands and hints from MemVisor
- Monitors usage of memory resources and performance
- Provides feedback to MemVisor
- Collaborates with MemVisor to improve PRAM endurance
  - Example: endurance aware cache replacement



SCMA (a cross-layer approach)



3. Immunity Inspired Cyber Security



- Highly distributed information processing system
- Self protecting
- Dynamic
- Diverse
- Error tolerant

Desirable properties to mimic

- Learn and retain information for future actions
- Local components that interact globally
- Individual components are continually created to improve the system's defense
- dangerous components are destroyed and eliminated from the body

Is it a good idea to mimic natural systems??
-- planes do no fly by flapping wings
-- cameras??

Concepts already borrowed from biology:

- Anomaly detection
- Neural networks
- Autonomic computing

Is research on protecting critical infrastructures adequate?

Is the human factor the "weakest point" in high-assurance systems?

Fostering collaboration?

Research on critical infrastructures without having access to real systems?

Is research on protecting critical infrastructures adequate?

- Threat is over-stated?
- Preparation is inadequate?

- Opportunity to advance knowledge is always a good thing
  -- no research is useless (putting a man on the moon??)
  -- new discoveries are made unexpectedly
  -- revolutionary Vs evolutionary research