U.PORTO

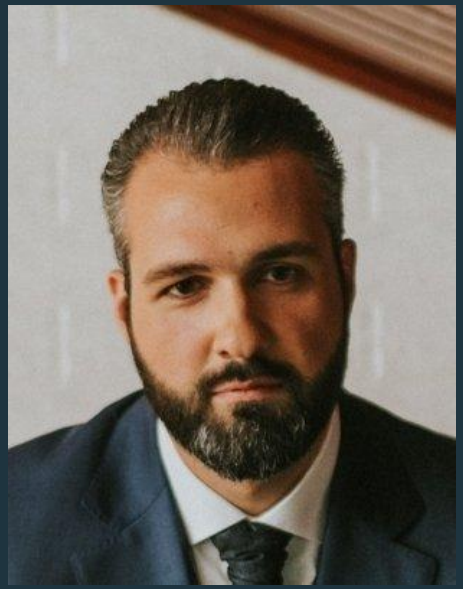
FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

IARIA

HUMAN-INSPIRED SECURITY IN SMART MANUFACTURING SYSTEMS

Speaker: **Rui Pinto**
Affiliation: **Faculty of Engineering of the University of Porto**
Email: **rpinto@fe.up.pt**

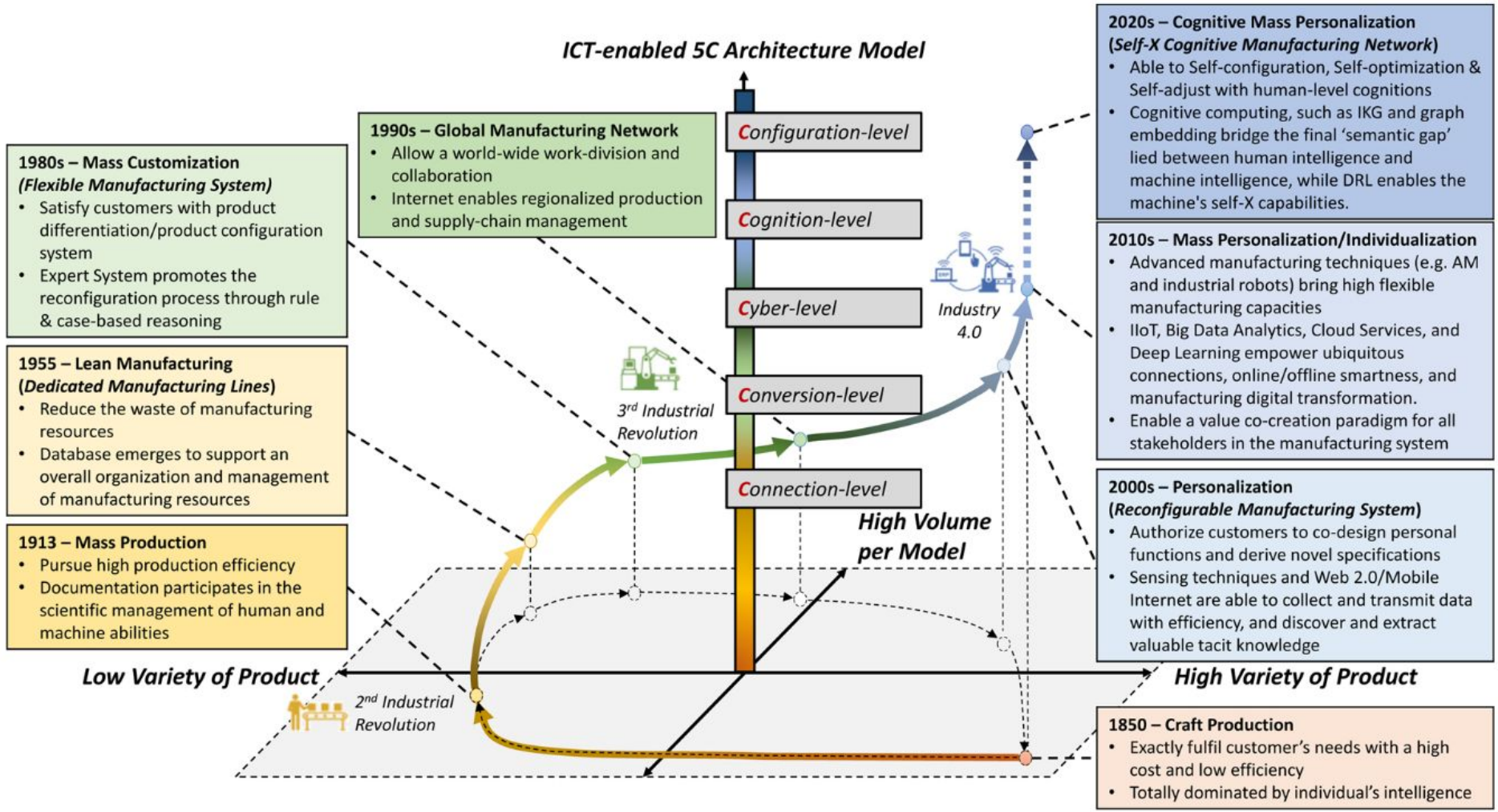
29 SEP 2023, PORTO



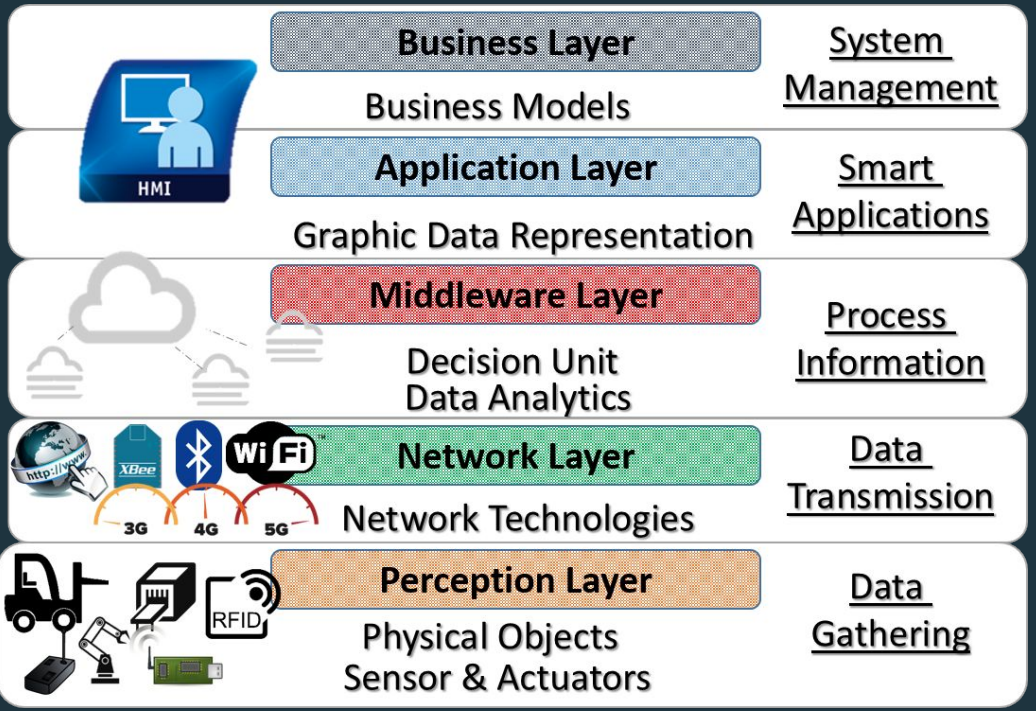
Rui Pinto received a Master's degree in Electrical and Computer Engineering from FEUP in 2013, and in 2022 a PhD in Computer Engineering from the same school. He is currently an Invited Teaching Assistant at FEUP and an Integrated Member of SYSTEC, where he has participated in multiple national and European Research and Development projects, mainly focused on the topics of digitization of industrial processes, WSAN, Edge/Cloud Computing, Smart Components, bio-inspired cybersecurity and Education 4.0. In addition, he had the opportunity to supervise and co-supervise at least 22 bachelor projects, Master's dissertations and PhD thesis, on topics related to the smart industry paradigm.

CONTEXT & PROBLEM

01


ICT-enabled 5C Architecture Model
Configuration-level
Cognition-level
Cyber-level
Conversion-level
Connection-level
2020s – Cognitive Mass Personalization
(Self-X Cognitive Manufacturing Network)
• Able to Self-configuration, Self-optimization & Self-adjust with human-level cognitions
• Cognitive computing, such as IKG and graph embedding bridge the final 'semantic gap' lied between human intelligence and machine intelligence, while DRL enables the machine's self-X capabilities.
1990s – Global Manufacturing Network
• Allow a world-wide work-division and collaboration
• Internet enables regionalized production and supply-chain management
1980s – Mass Customization
(Flexible Manufacturing System)
• Satisfy customers with product differentiation/product configuration system
• Expert System promotes the reconfiguration process through rule & case-based reasoning
2010s – Mass Personalization/Individualization
• Advanced manufacturing techniques (e.g. AM and industrial robots) bring high flexible manufacturing capacities
• IIoT, Big Data Analytics, Cloud Services, and Deep Learning empower ubiquitous connections, online/offline smartness, and manufacturing digital transformation.
• Enable a value co-creation paradigm for all stakeholders in the manufacturing system
Industry 4.0
3rd Industrial Revolution
1955 – Lean Manufacturing
(Dedicated Manufacturing Lines)
• Reduce the waste of manufacturing resources
• Database emerges to support an overall organization and management of manufacturing resources
2000s – Personalization
(Reconfigurable Manufacturing System)
• Authorize customers to co-design personal functions and derive novel specifications
• Sensing techniques and Web 2.0/Mobile Internet are able to collect and transmit data with efficiency, and discover and extract valuable tacit knowledge
1913 – Mass Production
• Pursue high production efficiency
• Documentation participates in the scientific management of human and machine abilities
High Volume per Model
Low Variety of Product
High Variety of Product
2nd Industrial Revolution
1850 – Craft Production
• Exactly fulfil customer's needs with a high cost and low efficiency
• Totally dominated by individual's intelligence

CPPS & IIOT SECURITY



Antao, L., Pinto, R., Reis, J., & Gonçalves, G. (2018, April). Requirements for testing and validating the industrial internet of things. In ICSTW (pp. 110-115). IEEE.

Pinto, R., Rossetti, R. J., & Gonçalves, G. (2016, July). Wireless sensor network simulation for fault detection in industrial processes. In SIMULTECH (pp. 1-6). IEEE.

5200

cyber attacks are launched against IoT devices each month.

$3.1 BILLION

The worldwide spending on IoT security is expected to reach this year

- The security of CPPS is crucial to the development and acceptance of the technology. As the IoT environment becomes complex, the resulting security issues present more challenges than any other existing network system.
- The limited computational power of COTS devices in CPPS restricts the usage of heavy security solutions.
- Security solution must be lightweight and Self-X* compliant.

https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/

- Prevention alone is no good, since no system can be full-prove to all attack vectors, especially considering zero-day attacks and inside threats.
- The autonomous and complex nature of CPPS does not comply with traditional IT security solutions.
- Intrusion Detection Systems may be used as a 2nd layer of protection.

70%

Organizations use and rely on a security prevention tool

47%

Since 2018, the number of security incidents involving insiders has increased by

https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/

40%

Of security technology is expected to rely on artificial intelligence by 2023

55%

of enterprises plan to increase their cybersecurity spendings this year

- By focusing on ML detection solutions, IDS is limited in model training, online detection and real-time data processing.
- Develop of security solutions in CPPS is a complex and error-prone process. Security features should be included in the CPPS already in the design stage.
- Avoid the training phase, batch data processing and offline detection.
- Follow an Model-based Engineering approach using an industrial standard, such as the IEC 61499.

https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/

VALUE PROPOSITION

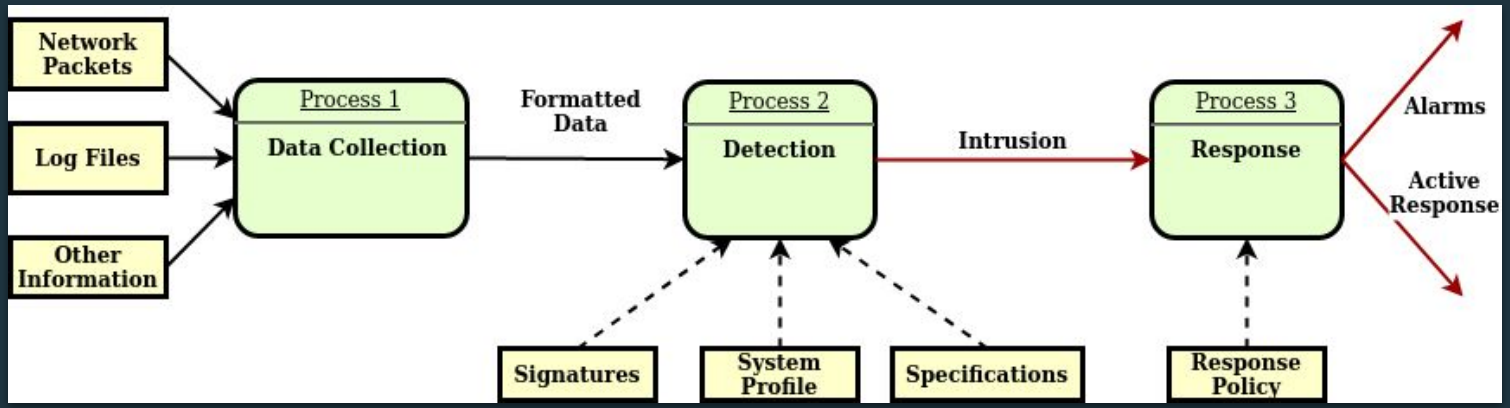
02

AN INTRUSION DETECTION SYSTEM TO PROTECT MANUFACTURING SYSTEMS, ENABLED BY BIO-INSPIRED APPROACHES, SUCH AS ARTIFICIAL IMMUNE SYSTEMS.

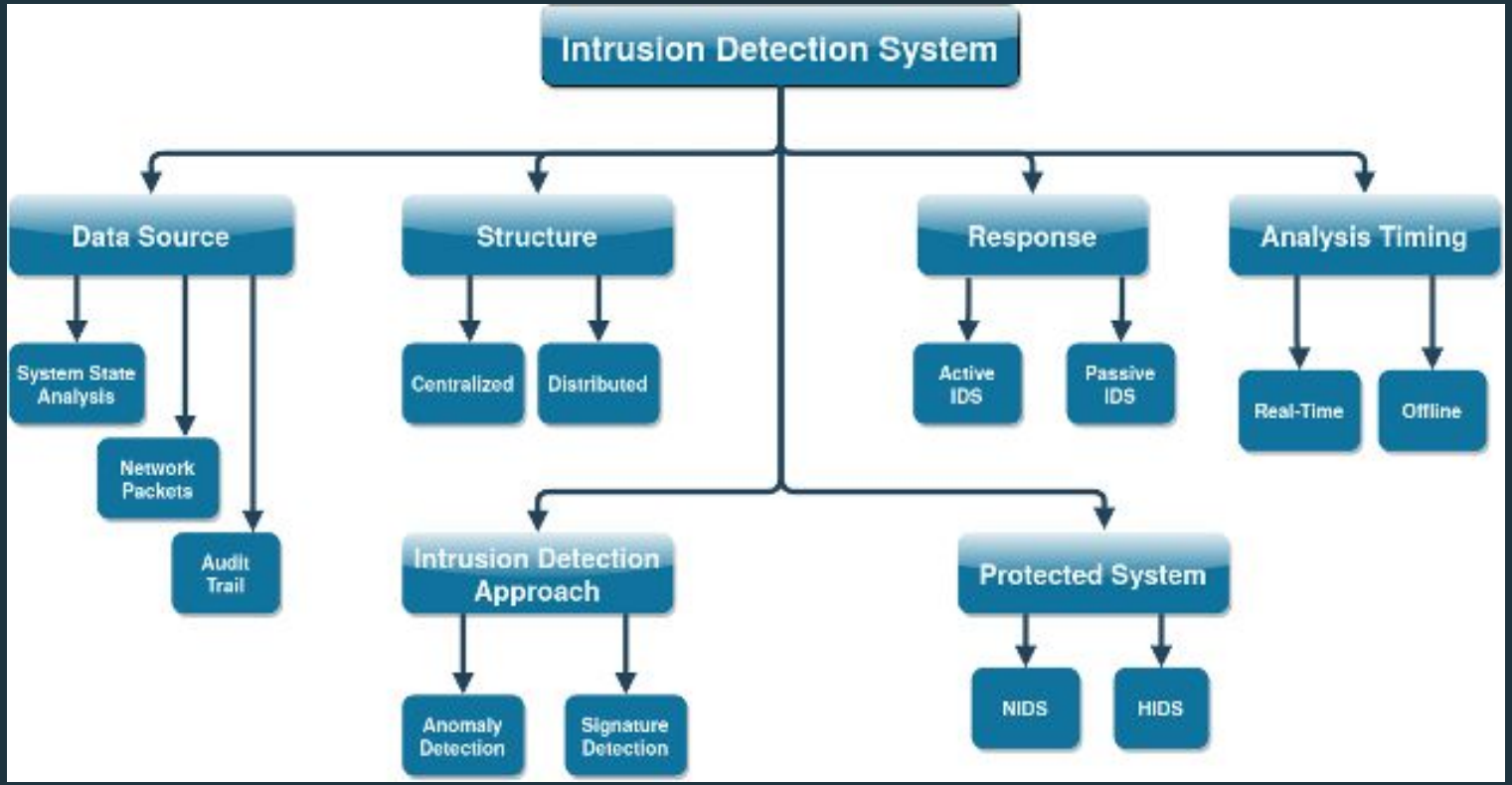
THE IDS DEVELOPMENT IS FOSTERED BY THE IEC 61499 STANDARD TO ENABLE A LOW-COST AND ERROR FREE DEPLOYMENT PROCESS.

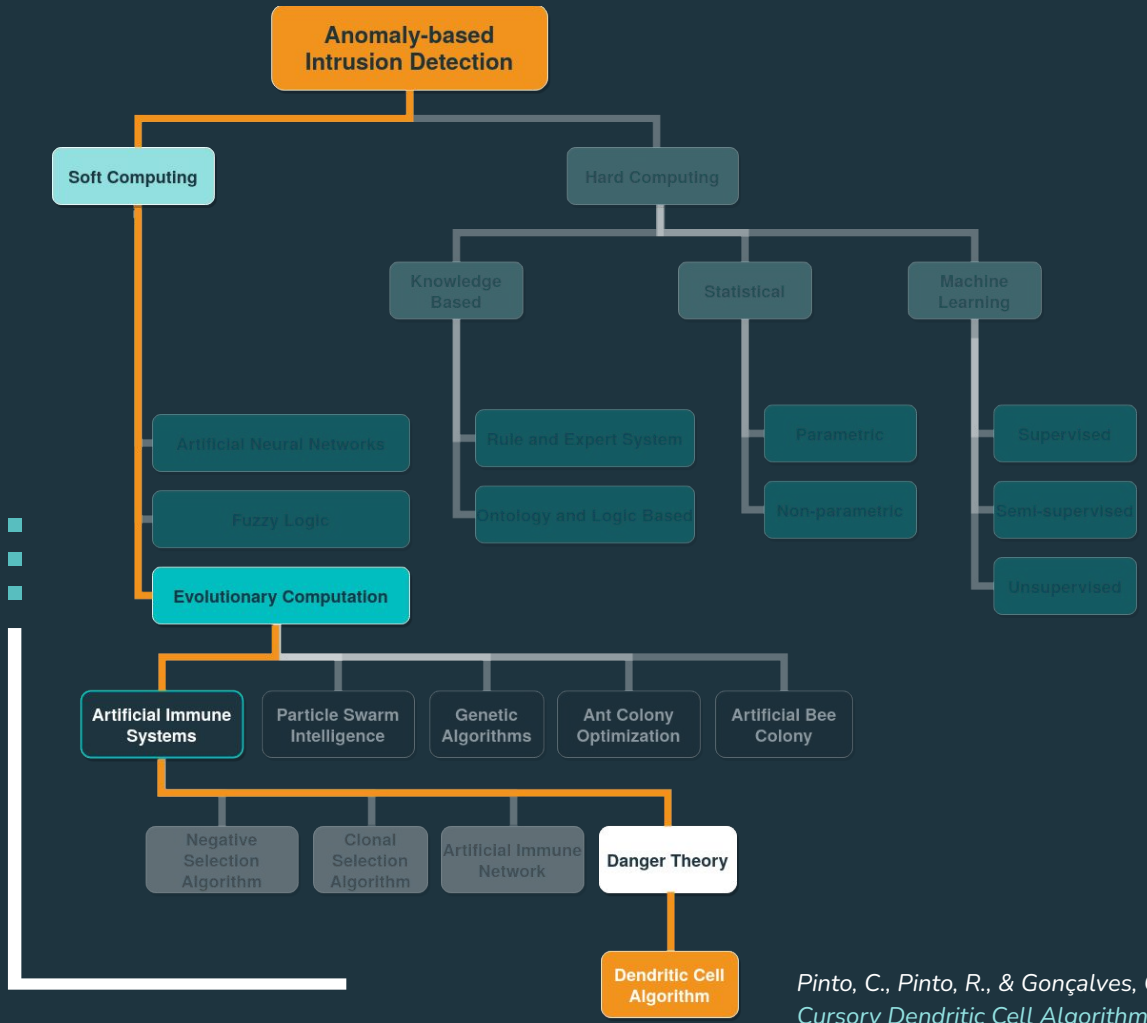
WHY IDS?

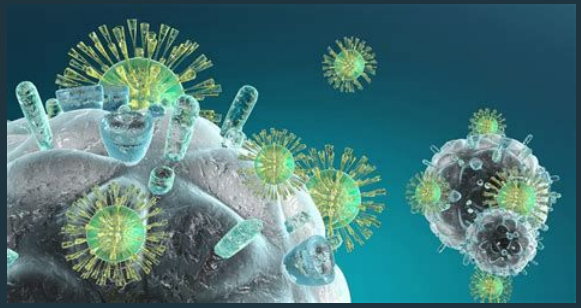
- Since attackers are becoming more and more underhand in their techniques, which are increasingly sophisticated, data breaches are inevitable.
- It is extremely difficult to fix all the possible vulnerabilities of a system and stop all intrusions/attacks to happen.
- Prevention won't stop inside attackers.

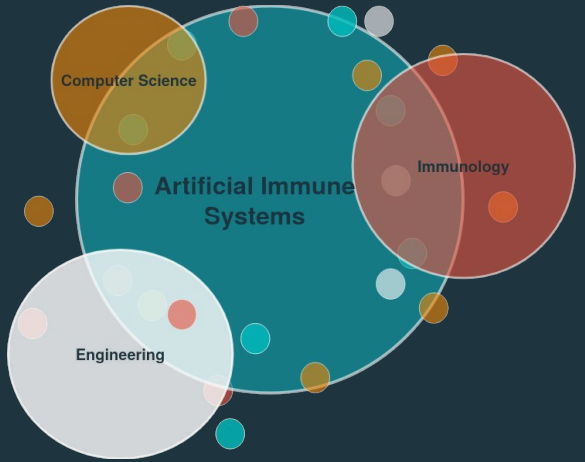


IDS TAXONOMY





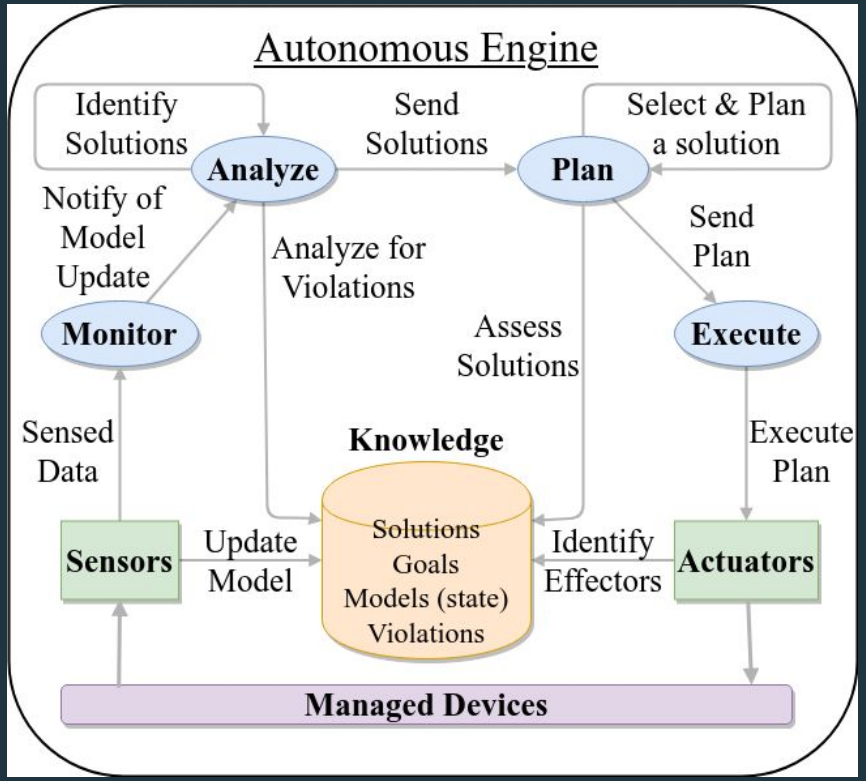




Pinto, C., Pinto, R., & Gonçalves, G. (2021). Towards Bio-inspired Anomaly Detection using the Cursory Dendritic Cell Algorithm. Algorithms.

SELF-IMMUNITY

- In the context of Autonomic Computing, a system is Self-immune when it recovers its safety properties in the face of an external (malicious) action. Ultimately, safety properties are no longer compromised when the same action occurs, acquiring tolerance over time.
- All Self-immune systems are self-healing, but the reverse is not true.



APPLICATION OF AIS IN SMS

- AIS are attracting researcher attention in ***Autonomic Systems***, *Control Systems*, *Islanding*, ***A-IDS***, ***Fault Diagnosis*** and ***Operations Research*** areas.
- The main motivations are:
  - Handle large volumes of data & manage very complex systems
  - Generate Self-behaving systems and adaptability to changes
  - MAS-oriented architecture for dynamic, heterogeneous and distributed environments
- The industry adoption of the AIS technology is very slow. The average TRL of bio-inspired solutions in industry is between 3 and 4 (**proof-of-concept** and **validation in lab**), while the LOA is between 2 and 3 (**partially/limited autonomy**). Possible reasons may be:
  - The strong stochastic nature of the solutions makes them hard to assess, explain, and use in different contexts.
  - Cost & effort of the industrial systems and infrastructure transformation.

Pinto, R., & Gonçalves, G. (2021). Application of Artificial Immune Systems in Smart Manufacturing. Array.

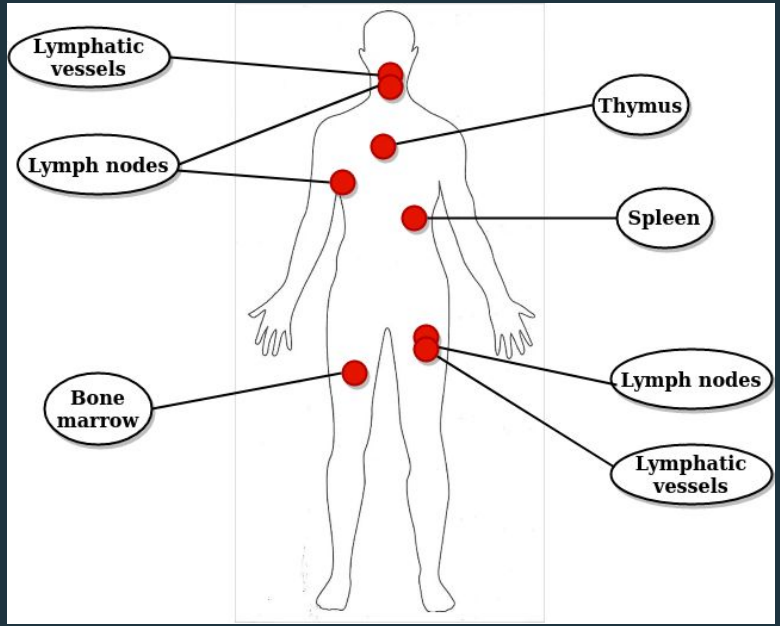
IMMUNE INSPIRED PROTECTION

03

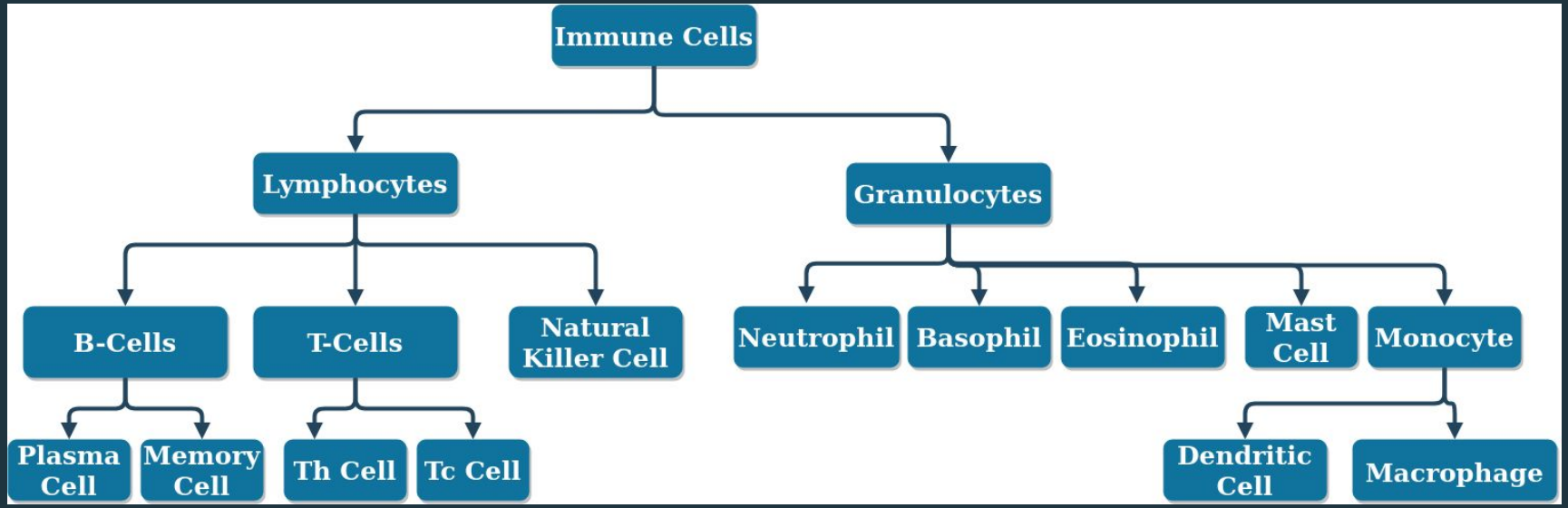
IMMUNE SYSTEM

The immune system is a network of biological processes that protects an organism from diseases. It detects and responds to a wide variety of pathogens (viruses, bacteria, cancer cells...), distinguishing them from the organism's own healthy tissue.

- There are two major subsystems of the immune system. The innate immune system provides a preconfigured response to broad groups of situations and stimuli. The adaptive immune system provides a tailored response to each stimulus by learning to recognize molecules it has previously encountered. Both use molecules and cells to perform their functions.

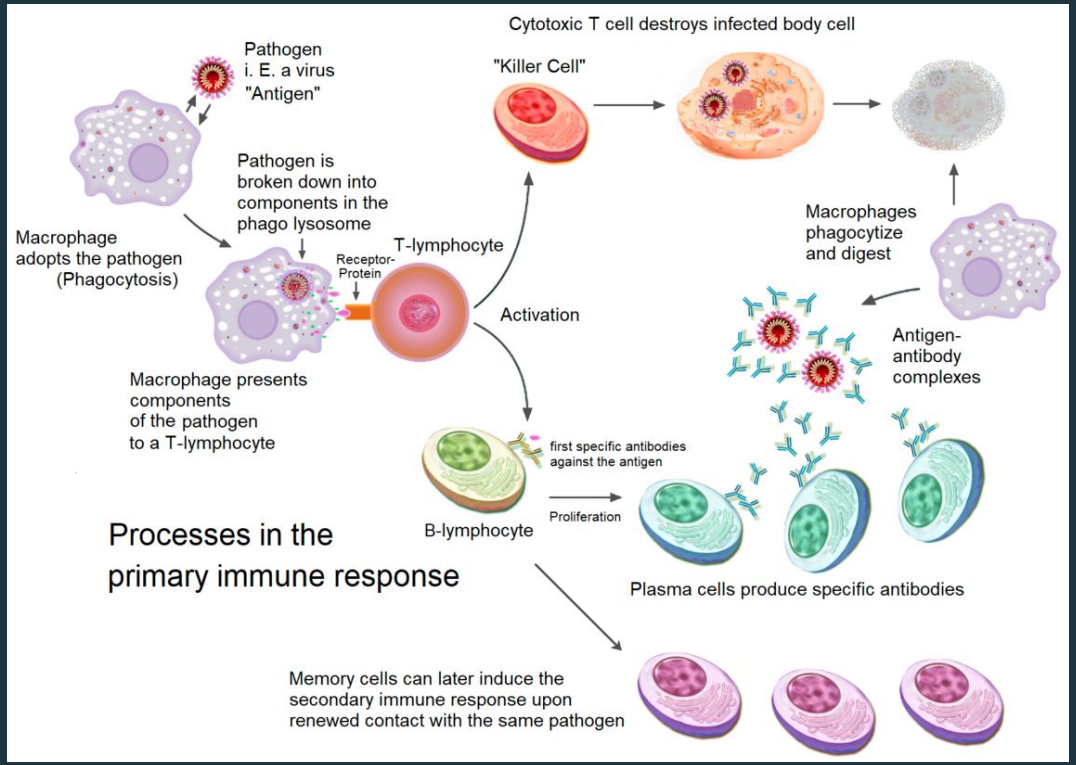


IMMUNE CELLS - LEUKOCYTES

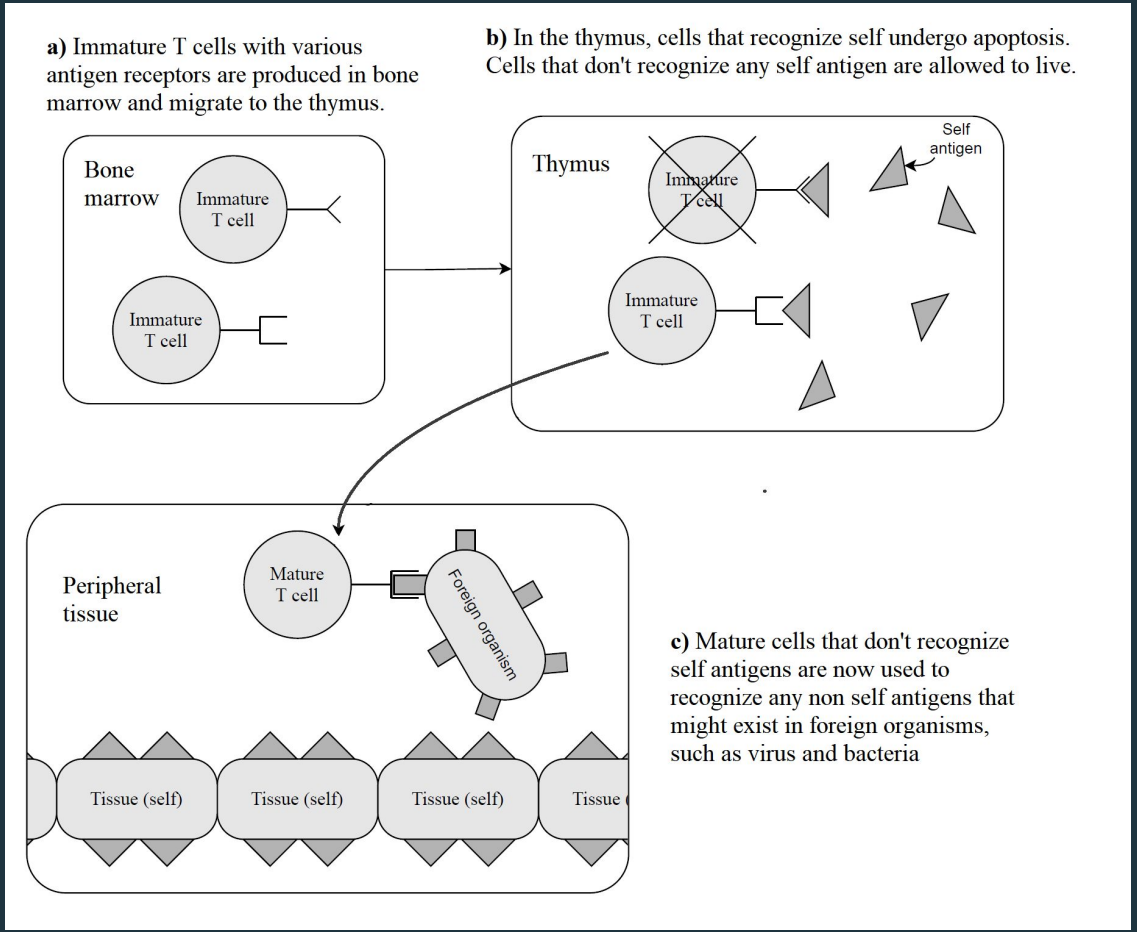


IMMUNE PROCESS OVERVIEW

- Negative Selection Algorithm
- Clonal Selection Algorithm
- Artificial Immune Network
- Danger Theory (Dendritic Cell Algorithm)



NEGATIVE SELECTION ALGORITHM



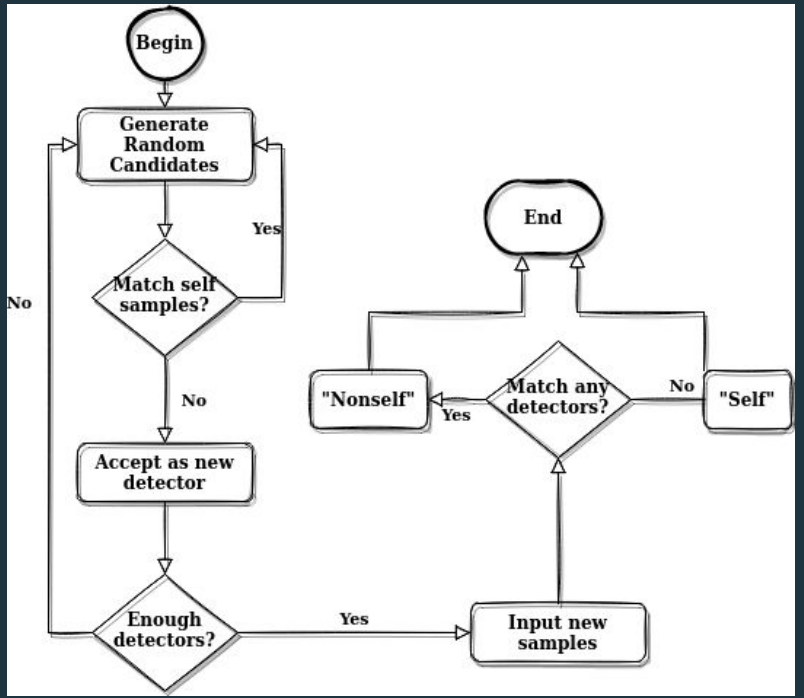
NEGATIVE SELECTION ALGORITHM

Algorithm 1: General Negative Selection Algorithm Detector Set Generation

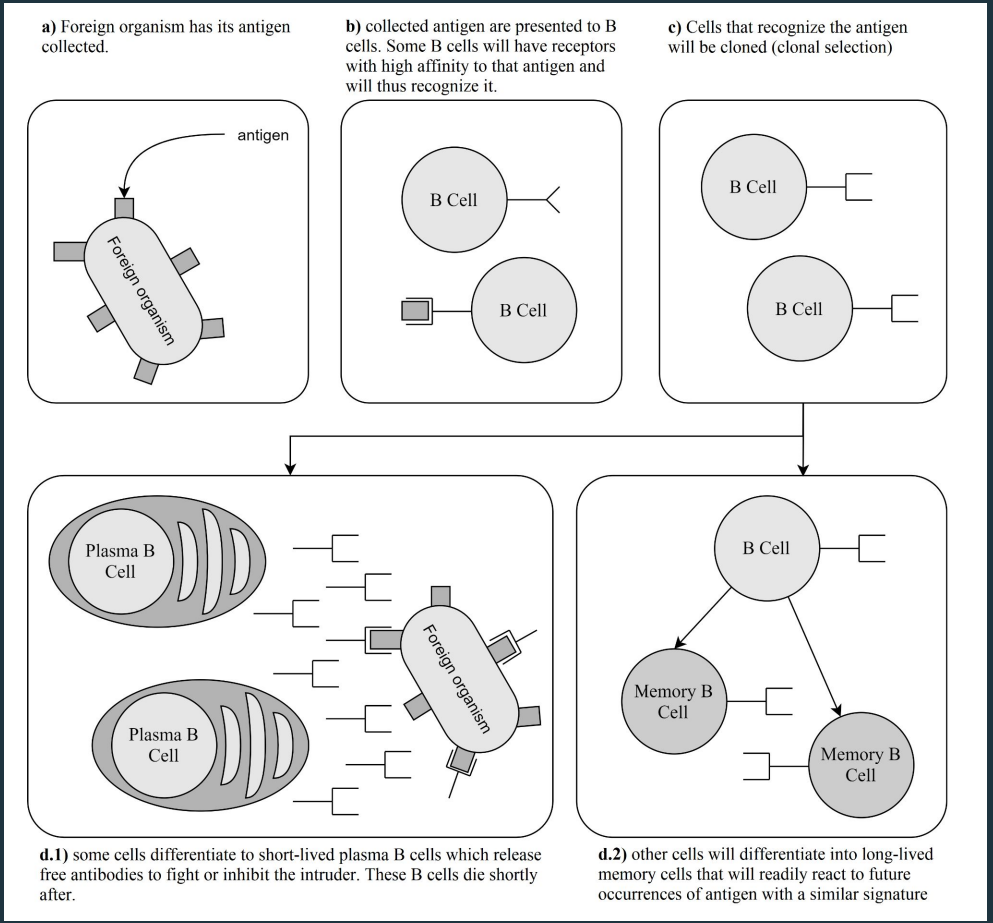
Input: S_{self} set of points that are normal

Output: D detector set

```
while not stop_condition() do
    self_detected = True;
    while self_detected do
        d = generate_new_detector();
        foreach s_i in S_self do
            if detect(d, s_i) then
                break;
            end
            self_detected = False;
        end
    end
    D ← d
end
return D
```



CLONAL SELECTION ALGORITHM

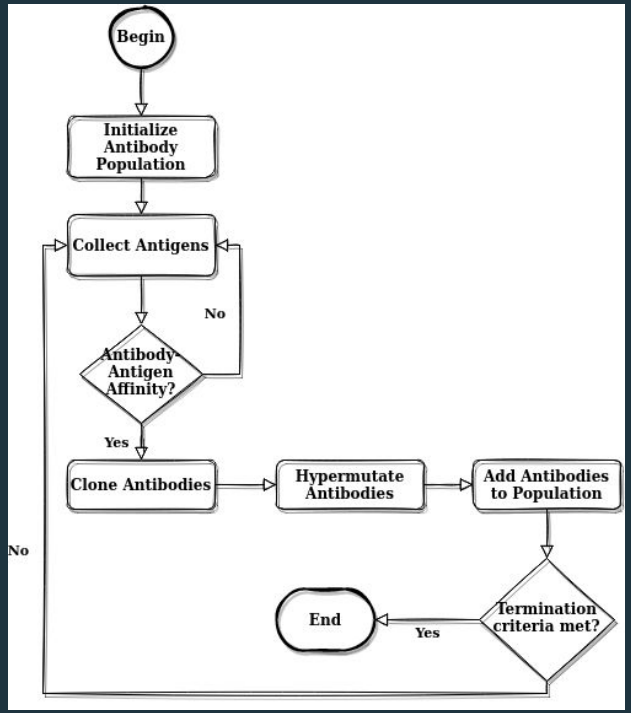


CLONAL SELECTION ALGORITHM

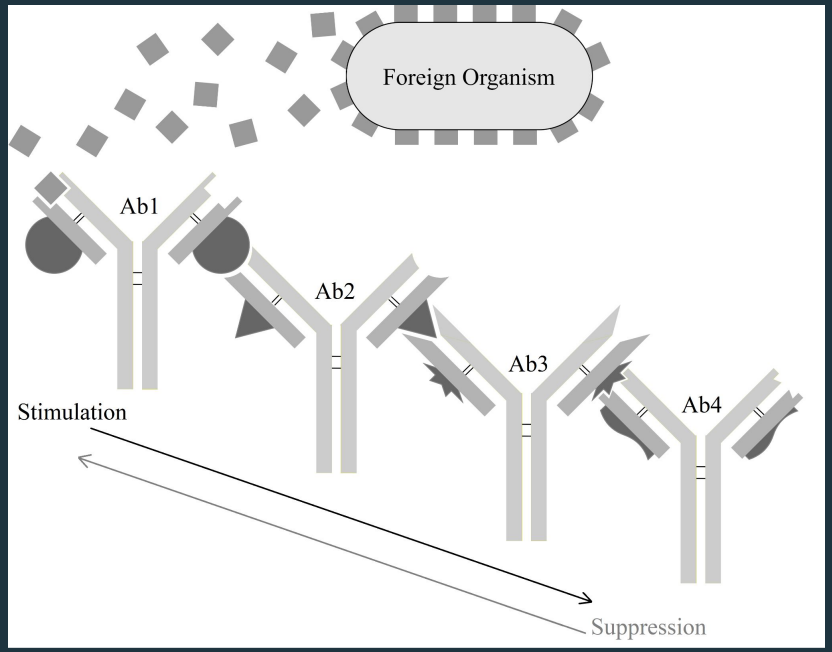
Algorithm 2: General Clonal Selection Algorithm

Input: N population size
n number of antibodies to clone
d number of new antibodies to be generated each iteration
Output: P best population

$P \leftarrow generate\_antibodies(N)$
while *not stop_condition()* **do**
  foreach p *in* P **do**
    $update\_affinity(p)$
  end
  $P' \leftarrow select(P,n)$ **foreach** p' *in* P' **do**
    $C \leftarrow clone(p')$
  end
  foreach c *in* C **do**
    $hypermutate(c)$
  end
  foreach c *in* C **do**
    $update\_affinity(c)$
  end
  $P \leftarrow insert(C,n)$
  $P_{new} \leftarrow generate\_antibodies(d)$
  $P \leftarrow replace(P,Pr)$
end



ARTIFICIAL IMMUNE NETWORK



Algorithm 3: A specific AIN implementation for generating an ARB population, based on AINE

Input: A input data (antigens)
N population size
NAT network affinity threshold
R_m mutation rate
N_c number of clones on each ARB
Output: S_{ARB} set of all ARBs

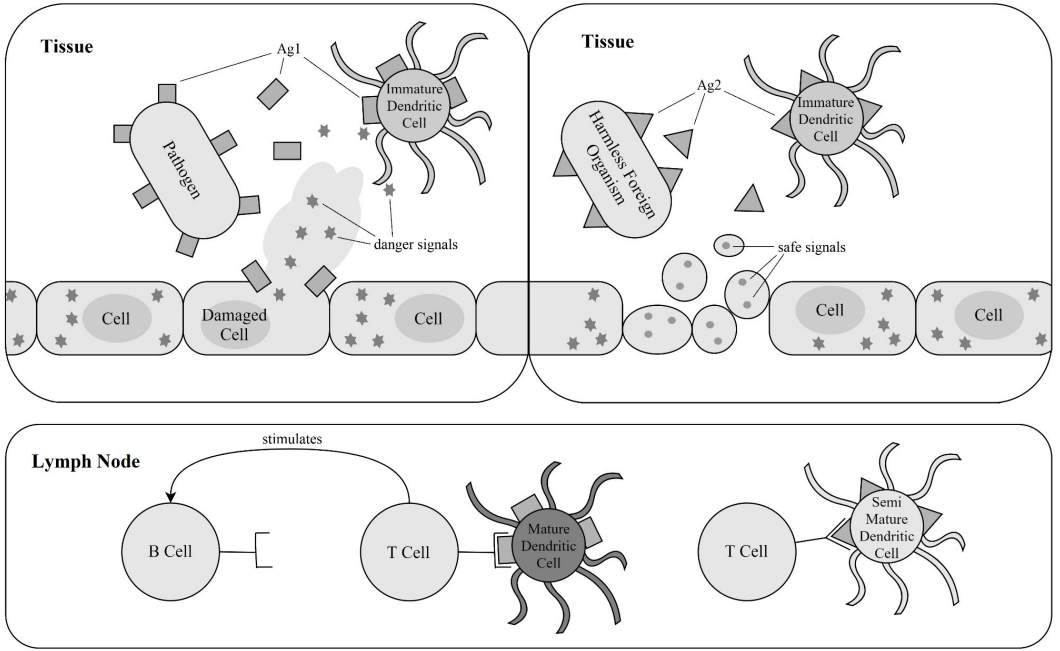
```
1  S_ARB ← initialize_population()
2  C_ARB = {}
3  while True do
4      foreach arb in S_ARB do
5          foreach a in A do
6              present_antigen(p)
7          end
8      end
9      foreach arb in S_ARB do
10         update_stimulation(arb)
11     end
12     foreach arb in S_ARB do
13         allocate_b_cells(arb)
14     end
15     if stop_condition() then
16         break
17     end
18     C_ARB = clone_and_mutate(S_ARB) foreach arb in C_ARB do
19         S_ARB ← arb
20     end
21 end
22 return S_ARB
```

DANGER THEORY

a) immature dendritic cells (iDC) navigate throughout the body, collecting antigens they encounter without descriminating whether the antigens come from self or non self.

b.1) iDCs also collect signals that originate from tissue cells. Cells that are damaged can chaotically release their contents which can be identified as danger signals by the neighboring iDC.

b.2) even if an organism doesn't harm the tissue, the iDC still collects these antigens, while also recognizing safe signals, such as those from programmed cell death (apoptosis)



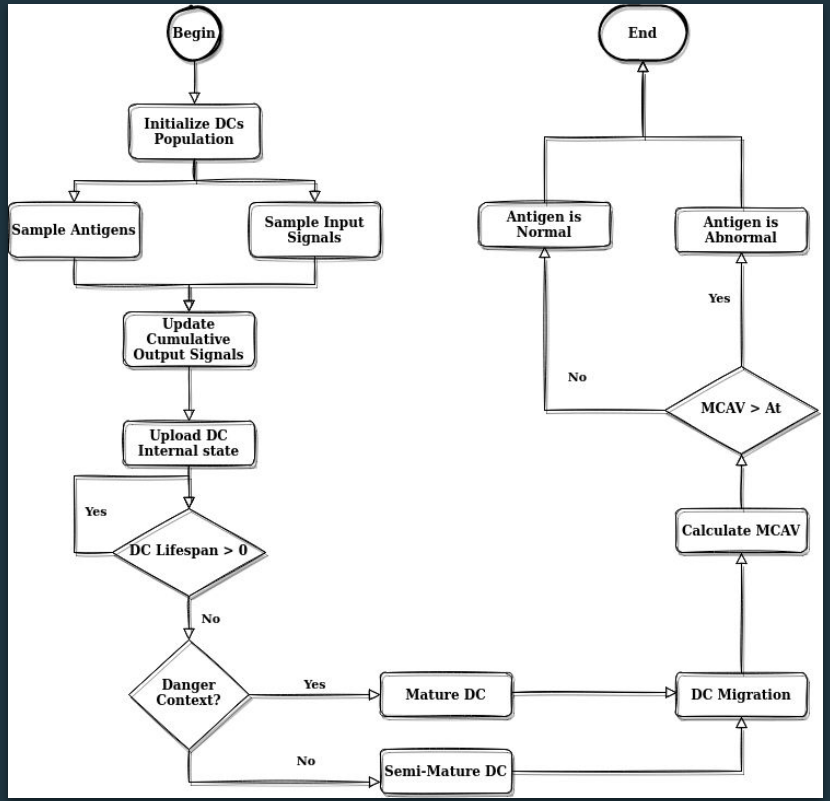
c) after collecting a sufficient amount of danger or safe signals, the iDC matures into either a mature DC (mDC) or a semi mature DC (smDC), for dangerous or safe contexts, respectively. In both cases the DCs present their collected antigen to T cells. T cells that recognize the antigens proceed to initiate an immune response for mDCs, or tolerate the presented antigens for smDC.

DENDRITIC CELL ALGORITHM

Algorithm 4: DCA algorithm implemented in this section. This algorithm is adapted from J. Greensmith

Input: Ag input data (antigens)
N DC population size
c number of times any antigen will be presented to distinct DCs
$t_{migration}$ migration threshold after which DC matures
t_{mcav} MCAV threshold above which the antigen is considered anomalous
Output: Classification of antigens as normal or anomalous

```
1  foreach ag in Ag do
2      signals = compute_signals(ag)
3      DC_sample = sample_random(c)
4      foreach dc in DC_sample do
           /* update csm and k of each cell and store the antigen in
              their repertoire                                        */
5          expose(dc, ag, signals)
6          if dc.csm > t_migration then
7              if dc.k > 0 then
                   /* this will increment the count of mDC for all
                      antigens that this cell had                     */
8                  mature(dc, MATURE)
9              else
10                 mature(dc, SEMIMATURE)
11             end
12             reset(dc)
13         end
14     end
15 end
16
17 foreach ag in Ag do
18     mcav = mDC_count(ag) / c
19     if mcav > t_mcav then
20         classify(ag, OUTLIER)
21     else
22         classify(ag, NORMAL)
23     end
24 end
```



FUTURE PERSPECTIVES

04

- **Enable Self-Immunity in industrial systems**
  - Enable automatic security features adjustment according to needs of the system to be protected.
  - Achieve autonomous reconfiguration of the industrial Edge devices in case of an attack/failure detected.

- **Enhance the detection approach & performance**
  - Relating process host-related data with network-based data for a meaningful detection approach.
  - Decentralized detection approach to enable a global self-awareness of the entire industrial system to be protected.

- **Automatic security requirement validation, solution adjustment and deployment**
  - Assess the application context and, based on the specific requirements, adjust the detection technique and deploy the solution.
  - Scalability, to be used in multiple application scenarios and business segments.

THANKS!

RUI PINTO

Do you have any questions?
rpinto@fe.up.pt