Glossary

Access control The means of ensuring that users access only those resources and services that they are entitled to access; ensuring also that qualified users are not denied access to services that they legitimately expect to receive.

Accessibility Preventing detention of information or resources to the detriment of others.

Adaptation Process leading to a modification of a system for it to better respond to its environment.

Adaptive Immune System The adaptive immunity provides specificity and memory capabilities to the system involving a particular type of cell, called a lymphocyte, of which there are two kinds: the B-cell and the T-cell.

Adequacy between a system and its environment State reached when a system flawlessly interacts with its environment. Every action/reaction is relevant.

Antibody Antibodies (also known as immunoglobulins) are gamma globulin proteins that are found in blood or other bodily fluids of vertebrates, and are used by the immune system to identify and neutralize foreign objects, such as bacteria and viruses.\(^1\) In our case, antibodies represent specific behaviours with associated preconditions and affinities with other antibodies.

Antigen An antigen (from antibody generator) originally defined as any molecule that binds specifically to an antibody.\(^2\) In our case, it refers to any external stimulation that can influence the system of interest.

Authentication Ensuring that users (or the entities) are the persons they claim to be.

Availability Ensuring that a system is operational and functional at any given moment usually provided through redundancy. Loss of availability is often referred to as Denial of Service (DoS).

Chemical-Based Middleware Middleware—e.g. the chemical extension of the TuCSoN (Tuple Centres Spread over the Network) infrastructure—where data and processes can be seen as reactants or molecules whose reactions are managed via

---

laws resembling those governing actual biochemical systems. As a result, agents are coordinated through chemical-like coordination laws that specify how data items have to be manipulated based on patterns such as data transformation and aggregation.

**Collective weaving** Activity exhibited by social spiders consisting in building spiderweb through coordinated actions.

**Completeness** An algorithm is complete if it *is able* to find a solution if one exists and if not, to inform that no solution is possible. This characteristic is desired but often costly to implement, depending on the complexity of the problem itself.

**Confidentiality** Preventing access to information by unauthorised persons.

**Cooperation** The act or attitude of interacting in whatever the means with another for mutual benefit. It usually involves sharing of information or competences.

**Decentralisation** In artificial and natural systems, decentralisation means that the decision-making process is spread among the entities composing the system. A process is decentralised when there is no central entity responsible for the implementation of the whole process.

**Emergence** Pattern or function at the global level of a system appears solely from local interactions among the lower-level components of the system.

**Encapsulation** In computer science, encapsulation is a principle for software architecture in order to reduce the interdependencies between components. This is a main idea in object-oriented design, which is extended in the MAS domain in order to use the same public interface between agents in protecting their internal components and facilitating their reuse.

**End-to-End Trust** End-to-end trust emphasises that the trust in the technical infrastructure must be taken into account when the trust in the virtual identity is computed.

**Evolution** in the sense of natural evolution mixes the natural selection process with the DNA mutations upon several generations of a population. At each generation, some individual presenting some phenotypical traits are favoured, and so are more slightly able to propagate those “good” trait in next generation.

**False negative** A false negative occurs when the system fails to detect that an activity is intrusive.

**False positive** A false positive occurs when the system identifies an intrusion, but the activity is not actually intrusive.

**Field-Based Middleware** Middleware—e.g. the TOTA (Tuples On The Air) middleware—where data structures are created and managed via mechanisms resembling the physical concept of field. Agents in distributed computing environments are then coordinated via abstract virtual fields that drive agents’ activities, in the same way as gravitational field drive mass particles in the universe. To this end, the role of middleware is that of effectively supporting creation and representation of such virtual fields, taking into account dynamic environmental conditions so as to allow agents to base their actions on the locally sensed fields.

**Holarchy** A holarchy is a hierarchy defined by the composition relationship between holons.

**Holon** A holon is an entity that can be composed of other (sub-)holons or that can be part of (super-)holons.
**Human Immune System** The human biological system that protects the body against diseases, infections and foreign agents.

**Idiotypic network** N.K. Jerne proposed a model for immune system regulation based on communications between antibodies. These communications take the form of stimulation and inhibition.

**Immune System** The immune system protects organisms from infection with layered defences of increasing specificity. Most simply, physical barriers prevent pathogens such as bacteria and viruses from entering the organism. If a pathogen breaches these barriers, the innate immune system provides an immediate but non-specific response. Innate immune systems are found in all plants and animals. However, if pathogens successfully evade the innate response, vertebrates possess a third layer of protection, the adaptive immune system, which is activated by the innate response. Here, the immune system adapts its response during an infection to improve its recognition of the pathogen. This improved response is then retained after the pathogen has been eliminated, in the form of an immunological memory, and allows the adaptive immune system to mount faster and stronger attacks each time this pathogen is encountered.³

**Innate Immune System** Specialised cells whose self- and non-self-recognition abilities are built-in from birth.

**Integrity** Preventing the alteration of information by unauthorised persons in a way that is not detectable by authorised users.

**Intruder** Any entity, such as a person, a group, or an organisation responsible for the intrusion. An attacker is any entity responsible for an attack.

**Intrusion** A deliberate or accidental unauthorised access to and/or activity against a communication and information system. It is also a deliberate or accidental abuse of privileges by legitimate users. An intrusion is always relative to the security policy built for the system it is intended to protect because the security policy defines what is allowed and what is denied on the system. An attack is a deliberate intrusion.

**Intrusion detection** The process of identifying that an intrusion has been attempted, is occurring, will occur or has occurred.

**Intrusion Detection System** A tool to detect intrusions. Its main goal is to alert the appropriate authority (system administrator or system security officer) before the intruder does any damage.

**Intrusion response** The counteractive measures taken after an intrusion is detected and/or at best, the corrective measures taken to undo the damage that was done or even suspected to be imminent.

**MAS Environment** Space shared by the agents which can be modified by the actions of the agents.

**Mobile Agent** A software agent that is able to autonomously move from one computer to another via the network and can continue its execution on the destination computer.

Monte Carlo method  As to simulate a decision-making process over a set of possible actions with an associated probability distribution, one can sort a randomly generated action depending on this distribution. This technique is called the Monte Carlo method.

Mutation (DNA)  are defined by some physical and chemical alteration of the genome on an individual. Mutations spans from single base change to gene duplication or deletion. In monocellular individual, mutation will propagate in the next generation each time the cell divides. In multi-cellular sexuated individual, the mutation will propagate in the following generation only if concerns sexual cells.

Natural Selection  is the process by which a population of individuals under the pressure of environment will be modified. Less fitted individual will die or at least become less performant in their reproductive behaviour.

Non repudiation  Ensuring that the originators of messages cannot deny that they sent the messages.

Non-self  Harmful entity of the human body.

NP-Complexity  A decision problem is in the class P if it can be solved in polynomial time on a deterministic Turing machine. The P-class problems are considered to be easy to solve. The NP class contains problems solvable in a polynomial time by a non-deterministic Turing machine. Unfortunately, there exist a huge amount of real hard problems (NP-complete problems) for which we do not know polynomial-time algorithms (P = NP is an open question).

Pathogen  An agent or a microorganism capable of causing disease.

Pervasive Display System  A system composed of a network of digital displays pervading the physical world, showing advertisements and/or information in urban and working environments. Traditionally, such displays are exploited via manual configuration so that they are insensitive to their operating context, resulting in a low infrastructure effectiveness. The adoption of the service ecosystem metaphor can promote context-awareness for the infrastructure, so that information can be displayed based on the current state of the physical environment and actions among displays can be coordinated depending on their spatial distribution, e.g. their physical proximity.

Pervasive Service Infrastructure  The growing deployment of pervasive computing technologies has led to an increased availability of devices carrying digital information as well as able to perform actuating/sensing actions in the physical world. This results in a huge amount of data available, regarding personal, social and professional activities as well as the physical world. Accordingly, a pervasive service infrastructure is aimed at providing digital services allowing users to perceive, interact and act on the surrounding physical world so as to open to emerging application scenarios, such as real-time traffic information systems and urban networks.

Phagocytes  Eating cells of the innate immune system.

Pheromonal gradient  The amount of pheromone that a colony of insects dispatches in its environment.

Pheromone  A volatile chemical substance used by insects to mark their environment.
Rationality Ideally an agent having all the useful data, the relevant heuristics and algorithms, and sufficient time to process on, it could make the more optimal decisions. This is not the case in real multi-agent systems, and consequently an agent has only a bounded rationality; nevertheless, this situation cannot prevent the MAS to find a relevant collective solution.

Privacy Ensuring that individuals maintain the right to control what information is collected about them, how it is used, who uses it, who maintains it and for what purpose it is used.

Reactive agent Simple behaving individual that reacts according to stimulus response rules based on its own state and to the state of its surrounding environment.

Region In image analysis, it is a set of pixels with the properties of connexity (each pair of pixels can be connected by a path of pixels belonging to the region) and homogeneity (all the pixels of the region share some radiometric properties).

Region segmentation Task in image analysis consisting in providing from an image a partition of regions (which by definition cannot overlap and whose union reconstitute the whole image).

Search space Given $p$ the number of parameters being estimated to define a problem, and having a set of constraints to satisfy, the domain (typically a subset of $R^p$) where each parameter verifies its constraints is called the search space.

Security In the context of a computer system, security is the prevention of, or protection against, an illicit action against this computer. These illicit actions are access to information resources by unauthorised entities or intentional but unauthorised destruction or alteration of that information.

Self Harmless entity of the human body.

Self-adaptation The property of a system to automatically adapt at runtime to dynamic evolution of the surrounding environment, with no need for external control.

Self-organisation Process where a system changes its internal organisation to adapt to changes in its goals and the environment without explicit external control.

Self-organisation According to Prigogine, self-organisation involves four essential properties: (a) Mutual interaction: the existence of multiple interactions involving a large number of interacting constituents. (b) Positive feedback: individuals reinforce the organising effect attracting new individuals which will in turn reinforce the effect. (c) Negative feedback: conversely, some variations or phenomena tend to reduce themselves and progressively disappear. (d) Amplification of fluctuations: the randomness in the behaviour of some constituents allows the system to escape difficult situations that could compromise self-organisation. Self-organisation can then take part at another moment and/or at another location.

Self-organizing Middleware Middleware that support the construction of systems through architectural models inherently promoting self-organisation at the application level.

Senescence is the natural eldering process that leads some cell to loose their repairing potentialities.

Service Ecosystem A system where service and data components are conceived as individuals of a sort of virtual ecosystem, in which they interact to serve their own purposes according to a set of “ecological laws”, resulting in self-adaptation and
eternity coming as inherent properties of the system rather than peculiar features of the individuals.

**Social spider** Spider species whose individuals have a tendency to live in colonies and to exhibit collective behaviour.

**Stigmergy** Stigmergy is a kind of coordination with indirect communication. The etymology of “stigmergy” is from “stigma” (cue, sign) and “ergon” (work): the work of individuals is controlled by previous works, done by itself or by conspecifics. *Sematectonic stigmergy* denotes communication via a modification of the physical environment. *Sign-based stigmergy* denotes communication via a signaling mechanism.

**Stigmergy** Paradigm that describes the way social insect communities, such as ants, termites and bees, interact through their environment.

**Trust** Trust is a subjective assessment of another’s influence in terms of the extent of one’s perceptions about the quality and significance of another’s impact over one’s outcomes in a given situation, such that one’s expectation of, openness to, and inclination towards such influence provide a sense of control over the potential outcomes of the situation.

**Trust Value** A trust value, that is the digital representation of the trustworthiness or level of trust in the entity under consideration, is seen as a non-enforceable estimate of the entity’s future behaviour in a given context based on past evidence.

**Virtual Organisation** A temporary alliance of autonomous and separately owned groups (companies, individuals, ...) where the participants pool resources, information, capabilities and knowledge in order to meet common objectives.

**Methodologies**

- Self-organisation—see Chap. 2.
- Self-organising system—see Chap. 2.
- Development methodology—in software engineering, a development methodology formally defines the process that is used to express requirements, analyse them, design an application that meets these requirements before implementing and testing this application. A methodology is usually made up of a process, some notations and tools to support these notations and/or help the developer.
- Development process/lifecycle—in software engineering, the software development process/lifecycle is a logical model followed by designers in order to create and/or alter a software system. Different models have been proposed such as “waterfall”, “spiral”, “incremental”, “agile” and some others.
- Unified Process—UP is an iterative software development process.
- Rational Unified Process—RUP is an implementation by Rational Software (IBM) of the Unified Process.
- Modelling language—a modelling language is a graphical or textual language which defines a precise notation to express abstract concepts. Such a language enables designers to have a common basis for understanding each other during the design of a system by sharing a common language.
- Unified Modelling Language—UML is the OMG’s modelling language that enables designers to express the abstract artefacts that are involved in the object-oriented design of a system (such as use cases, classes, activities and so on).
• Requirement analysis—this phase defines the requirements of the system and the problem the customer wants to solve.
• Functional/Non-functional requirements—in software engineering, a collection of requirements describes the features of the system to be designed. These requirements may be functional (what the system has to do) or not (with which quality of service). According to [4], a functional requirement specifies an action that a system must be able to perform, without considering physical constraints, and is a requirement that specifies input/output behaviours of a system. A non-functional requirement specifies system properties, such as environmental and implementation constraints, performance, platform dependencies, maintainability, extensibility and reliability. It is a requirement that specifies physical constraints on a functional requirement [1–3].
• Analysis—considering the requirements previously gathered, what the system does is specified and expressed considering existing constraints. Problems are abstracted and separated, and a conceptual model is established.
• Design—this phase answers how the system has to be done. A modular decomposition is done, and the software architecture is defined to provide a logical model.
• Implementation—the models previously defined are implemented using a specific programming language. The different modules written are validated.
• Test and verification—software testing aims at evaluating features of a program and proving that this program behaves as expected by meeting its requirements.
• Deployment—the software system previously implemented and tested is made available for use. This is a general process which is usually customised depending on the context.
• Software Process Engineering Metamodel—OMG’s SPEM is a metamodel used to describe a concrete software development process or a family of related software development processes.
• WorkDefinition—in SPEM (1.0), a WorkDefinition describes a work performed in a process. Its main subclass is Activity, but Phase, Iteration and Lifecycle are also subclasses of WorkDefinition. A WorkDefinition can be composed of other WorkDefinitions. A WorkDefinition is related to the work products it uses (as input or output) and is owned by the primary role that performs that WorkDefinition in the process.
• Activity—an Activity is a subclass of a WorkDefinition. It is a discrete task, relatively short which can be assigned to one individual playing role. It has input and output work products and can be decomposed into smaller atomic elements called Steps.
• Step—a Step is the atomic unit of an Activity and can be described in terms of the workproducts it uses and roles it depends on.

References


Index

A
A service providing MAS, 212
ABT, see Asynchronous Backtracking
ACO, see Ant Colony Optimisation
Acropora millepora, 90
Adaptation, 372
Adaptive trust, 381, 393
Adaptivity, 381
ADELFE, 290
ADOPT, see Asynchronous distributed constraint optimization
Affinity, 232–236, 242, 244, 245
Agent, 106, 349, 350
Agent & Artefact metamodel, 289
Aggregation, 151
AMAS, see Adaptive Multi-Agent Systems
AMAS-Modelling Language, 302
Ambiguity, 207
Ant Colony Optimisation, 352, 360, 364–366, 375
Ant foraging, 10
shortest path, 10
Antibody, 88, 228–239, 241–245
Antigen, 228–236, 239, 241–244
APO, see Asynchronous Partial Overlay, 354–356, 360
dynamic, 355
optimisation, 355
Apoptosis, 85
Aptitudes, 300
Artificial evolution, 81
Artificial self-organising systems, 14
Astrolabe, 157
Asynchronous Backtracking, 352–354, 357, 358, 360, 364–366, 374

Asynchronous Weak-Commitment Search, 352, 353, 355, 357, 358, 360, 365–367, 375
dynamic, 355
Autonomic Entity Recognition, 391
Autonomy, 107
AWCS, see Asynchronous Weak-Commitment Search

B
B-lymphocyte, 87
Bucket brigades, 20

C
Cell communication, 85
Cellular systems, 85
Chaotic dynamics, 78
Cloud computing, 151
Collective weaving, 429
Completeness
algorithm completeness, 352, 355, 368
Complex adaptive systems, 9
Complex systems, 200
Complexity, 78, 105
Computer security, 98
Concentration, 230, 233, 234, 236
Concurrency, 207
min-conflict heuristic, 356, 358, 366, 368
nogood, 353, 366, 374
Constraint optimisation
DCOP, 354, 355
Constraint satisfaction
complete assignment, 349, 350, 352, 356
constructive algorithms, 349

G. Di Marzo Serugendo et al. (eds.), Self-organising Software, Natural Computing Series,
DOI 10.1007/978-3-642-17348-6, © Springer-Verlag Berlin Heidelberg 2011
Constraint satisfaction (cont.)
domain, 352
variable, 352
Context-aware Authentication, 398, 399
Context-aware Security, 381
Context-awareness, 382
Convergence, 153
speed, 153
Cooperation, 365, 369, 375
Critical level, see criticality
Criticality, 366, 369
Customised Unified Process (CUP), 285
Cytoskeleton, 11

Data aggregation, see aggregation
DBA, see Distributed Breakout Algorithm
Death certificates, 150
Decentralisation, 349, 351, 355, 357, 359, 363, 364, 368
Dictyostelium discoideum, 84
Distributed Breakout Algorithm, 352, 357–359, 364, 365, 367, 374
Distribution, 351, 352, 355, 357, 361, 363, 364, 367
Drosophila melanogaster, 84
Dynamics, 364
DynAPO, see Asynchronous Partial Overlay, dynamic
DynAWCS, see Asynchronous Weak-Commitment Search, dynamic

Ecology, 82
Ecosystem adaptation, 82
Ecosystems, 77
Embryology, 85
Emergent phenomena, 9
Entities, 293
Environment, 8, 113, 294
Environment, Reactive rules and Agents, 352, 357–359, 364–367, 375
Epidemics, 94, 140
ERA, see Environment, Reactive rules and Agents
Eukaryotic cells, 11
Evolutionary programming, 82
Evolutionary strategies, 82

Fitness function, 81
Foraging, 89

GA, see Genetic Algorithms
General Methodology, 288
Genetic Algorithms, 82, 360, 362, 364–366, 375
Genetic programming, 82
Gossip, 95, 139
push averaging, 155
push-pull averaging, 152
push-pull gossip algorithm skeleton, 159
SI Model, 143
SIR model, 146
Grassé, 7
Groups, 89

HMAS, 252, 253, 258
Holarchy, 254, 255, 268, 271, 276
Holon destruction, 261
Holon satisfaction, 266, 273, 274, 276
accumulative, 267, 273
collaborative, 267, 273, 274
instant, 268, 273
necessary, 268, 273
self, 267, 273
Holonic role
head, 258–266, 268, 272–274, 276
multi-part, 258, 260, 261, 263, 264, 266–268, 272, 273
part, 258, 260, 262–264, 266, 268, 269, 272–274
stand-alone, 258, 264–266, 268, 273
Human behaviours, 92

Image analysis, 426
Immune system, 87, 409
Incompetence, 207
Incomprehension, 207
Information dissemination, 141
Intrusion, 407
Intrusion detection, 406, 412
Intrusion response, 406, 412

Local search, 349, 350, 352, 356, 357, 359, 361, 365, 366, 368
distributed, 356
tabu search, 356
Locality, 349, 355, 364, 365
principle of locality, 349
Location-based Authentication, 396
U
Unproductiveness, 207
Uselessness, 207

V
Variable, 348–351
Vision-based Entity Recognition, 393