

NISIS Brainstorming Meeting - Ideas on the vision for future IT Systems

Immune System Inspired Health Monitoring of Machinery using the Danger Theory

Jens Strackeljan, Kauko Leiviska, Esko Juuso, Sulo Lahdelma

In recent years, mechanical machinery systems have become increasingly complex and consequently the challenge of protecting these systems has become increasingly difficult. Objective of the task force is to study the potential of the Immune System philosophy to dynamically adapt and evolve a Health Monitoring System to explore, learn and absorb new machinery incipient fault detection and discovery knowledge in order to provide accurate health monitoring response in dynamic environments.

The following levels of adaptability are conceivable in conjunction with monitoring systems.

1. Level 1
An adaptive monitoring system is capable of recognising variations in the surroundings and process conditions. Modifications, such as the adaptation of limiting values, can be performed automatically by the system itself.
2. Level 2
An adaptive monitoring system can be transferred from one machine to another without the need of readjustment by an expert. Any necessary adjustment work should be reducible to an absolute minimum. However, the monitoring task itself should not be altered in this connection.
3. Level 3
An adaptive monitoring system can be employed for other monitoring tasks without the need of altering the basic structure. The necessary limiting values or control parameters of the classification algorithm are, to a large extent, specified independently. At this third level, the monitored object itself can also be varied. For allowing the system to function at this level, learning strategies are implemented, rather than pre-programmed algorithms for calculating problem-specific features, such as the effective value of the vibratory acceleration.

In its present status, the technology usually does not even attain the first of the levels just defined. This situation may at first be surprising, and perhaps also somewhat disappointing, but it is easy to understand from an engineering standpoint. The decisive external parameters causing variations in the monitoring parameters are highly diversified, and the mutual interactions among them are often unknown, consequently, a consideration of these parameters in a diagnostic model is difficult or impossible. Once trained, a system is capable of performing a monitoring task as long as the prerequisites for the training status are satisfied. If these conditions change, however, problems will occur in the monitoring system, and the system must be retrained.

The human immune system (HIS) is a robust, complex, adaptive system that defends the body from foreign pathogens. It is able to categorize all cells (or molecules) within the body as self-cells or nonself cells. There are two major branches of the immune system. The innate immune system is an unchanging mechanism that detects and destroys certain invading organisms, whilst the adaptive immune system responds to previously unknown foreign cells and builds a response to them that can remain in the body over a long period of time. Since 50 years, the central dogma of immunology has stated that the human immune system reacts to entities that are not part of the organism. Therefore the decision to react is a result of the HIS classifying its own cells as self and everything else as nonself. Most biologically inspired artificial immune systems based on the HIS have relied on the self and nonself model. Algorithms derived using this model have been largely successful. Artificial immune systems (AIS) have been developed for a wide range of applications from data mining to information security but not for monitoring complex mechanical systems. The development of low cost sensors and their distributed integration in monitoring systems will increase the demand on decentralized smart information systems. AIS fulfil this requirement.

Over the last decade, a new theory, called the Danger Theory, has become popular amongst immunologists. A number of advantages are claimed for this theory; not least that it provides a method of “grounding” the immune response. The theory is not complete, and there are some doubts about how much it actually changes behaviour and/or structure. Nevertheless, the theory contains enough potentially interesting ideas to make it worth assessing its relevance to artificial immune systems and we believe that the theory could be helpful to overcome existing problems in the definition of self and non-self states for complex machinery. In reality, the immune system actually discriminates “some self from some nonself”.

The Danger Theory introduces a way of escaping the semantic difficulties with self and nonself, and thus provides grounding for the immune response. Accepting the Danger Theory as valid we can take care of “nonself but harmless” and of “self but harmful” states in our system. The central idea in the Danger Theory is that the immune system does not respond to nonself but to danger supports, just like the self–nonself theories, the need for discrimination. However, it differs in the answer to what should be responded to. Instead of responding to foreignness, the immune system reacts to danger. This theory is borne out of the observation that there is no need to attack everything that is foreign. A change in vibratory behaviour can be due to a wide variety of factors that do not result from a fault in the machine itself. Minor conversion work may have been performed on the machine, for instance, in the course of maintenance and servicing; such measures can cause a change in behaviour without resulting in a malfunction. In this theory, danger is measured by damage to cells indicated by distress signals that are sent out when cells die an unnatural death.

And exactly the problem of defining the self or normal state is a problem for advanced monitoring systems. Anomaly detection systems rely on constructing a model of machine behaviour that is considered ‘normal’. This is achieved by using a combination of statistical or machine learning methods to examine vibrations, temperature, oil and processes. However, ‘normal’ behaviour in a large, dynamic system is not well defined and changes over time. This often results in a significant number of false alarms known as false positives and the reduction of false positives is a key challenge that the Danger Theory may be able to address. In this field of developing artificial immune systems for fault detection, Danger Theory may provide significant improvements to current detection techniques. Work is currently being performed into exactly how danger signals can be identified in the HIS. It is hoped the results of this research will yield a clearer view on what danger signals are *in vivo*, how they can be translated for detecting danger within mechanical systems.

It is clear that a task force could not cover all related problems and present solutions but we could use some existing test rigs at the University of Oulu and Magdeburg to build a demonstrator and get more reliable information. This should lead to the identification of future research need in this field and in consequence to new research projects, road map contributions and publications and at least open the door for transferring NISIS topics to industry. The task force will summarise the results in a technical report.

What is the business need that will drive sustainable change in condition monitoring in the future? In our view, the business need that is likely to dominate the industrial maintenance scene is asset effectiveness - the need to extract maximum profits from the minimum investment in plant and equipment. There are different ways to achieve this through the use of complete new condition monitoring information systems:

- By improving equipment reliability through the effective prediction (and then avoidance) of equipment failures,
- By minimising downtime through the integrated planning and scheduling of repairs indicated by condition monitoring techniques with those indicated by other techniques.
- By maximising component life by avoiding the conditions that reduce equipment life.
- By utilising condition monitoring techniques to maximise equipment performance and throughput.
- By minimising condition monitoring costs.

We believe that such a system would be a visionary example for future IT Systems in different industrial areas.