



this issue

Powder Injection Moulding	P.1
Detecting Hacking Attacks	P.2
Plans for next Quarter	P.3
What is ... pre-processing?	P.3
Upcoming Events	P.4

Supervised learning to differentiate good from bad

Learning by example is the most common form of learning for humans. We are shown what to do by someone who already knows. Computers learn best in the same way. If we compile a list of examples for "good" and a list of examples for "bad", then a computer can correctly distinguish new examples that it has not seen before.

The number of categories does not play a major role. We can distinguish between two types (good vs. bad) or between a large number of system states, such as in the powder injection case on the right of this page.

This method of learning is called supervised learning as opposed to unsupervised learning that trains a computer to recognise similar events but is inherently not capable of interpreting the results because the information "good" or "bad" is missing. The human equivalent is learning-by-doing and this is generally less effective.

Minimizing Powder Injection Moulding Scrap

The powder injection moulding process can produce as much as 20% scrap whether the material is ceramic, metal or plastic. Often the scrap part cannot be identified as scrap before it does not pass through one or more follow-on process steps such as binder removal or sintering (see diagram below), steps that are much more expensive than moulding itself.

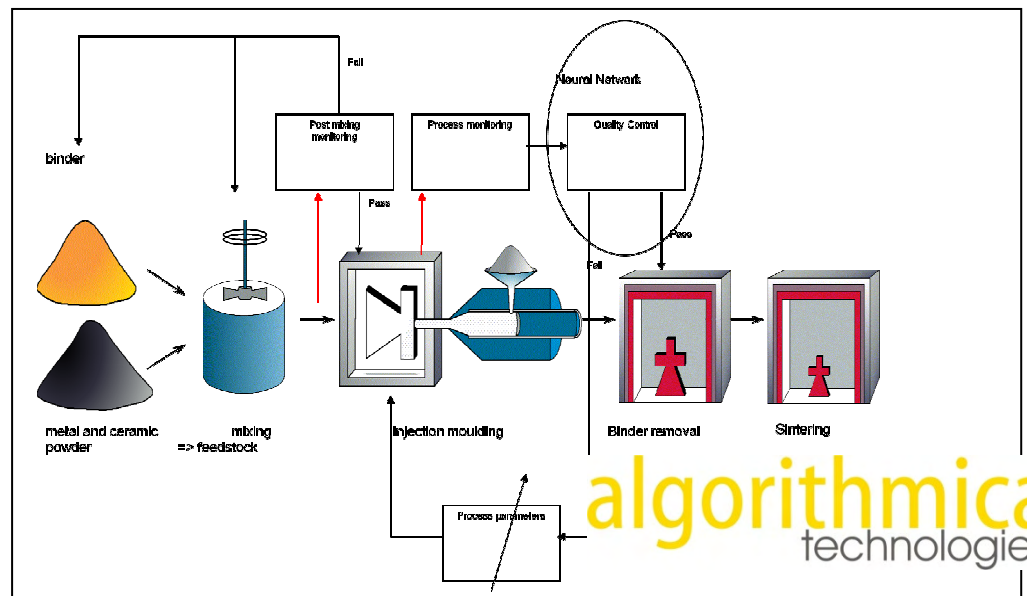
By recognizing if a part is scrap *before* it is passed through the rest of the process, significant amounts of electricity and material can be saved, the efficacy of the production rises and quality level rises. This is an essential feature in any Six-Sigma production.

To create such a recognizer, we have teamed up with materials science and moulding experts from the Fraunhofer Institute for production technology and applied materials science.

The materials know-how and experimental data will be delivered by Fraunhofer, we will provide the machine learning. Together, we will create a system capable of saying whether a part is scrap or not *while* it is being moulded based on measurements coming from the moulding machine (various temperatures, pressures and flow rates) and material properties.

This system would run on an ordinary PC attached to the moulding machine and will be able to communicate with a sorter, so that scrap can immediately be sorted into the re-cycle process and used another time.

It will be possible, after some experience, to use the same model to adjust the machine parameters in order to reduce the produced scrap at the source. This project will be tackled in the future.



Active Applications

AT is constantly pushing the envelope in the development of state-of-the-art technologies to solve practical problems. Applications for public funding and prizes occupy an essential place in this endeavour.

We have teamed up with a variety of high profile organisations to get sponsored R&D projects.

Factory Planning

A factory is essentially a building with machines in it. These machines are connected in some fashion and people have space in which to work. Where the machines go, where the people work, how the building is constructed and how the material flows through the process must be planned before the factory is built.

This planning is typically done manually over one or two years by a team of people and thus quite costly. By specifying the boundary conditions and a desired output (e.g. maximal throughput), a computer model can be created and thus an automatic optimization run on this model.

The result is an automatically planned factory that is better than any manually planned one. The process to accomplish such a plan would take only 3 – 6 months and so save considerable costs.



Hacking attacks, especially on corporate networks, are increasing both in number and in the damage they cause. This project is designed to detect when a hacking attack takes place.

Many software packages leave loopholes that can be exploited by knowledgeable persons. These persons can then gain control over the computer. They can retrieve files, listen and look into the room via the microphone and webcam.

Hacking has changed from the days in which it was the digital frontier made up of a few people in search of a challenge and recognition. Nowadays, hacking is a commercial value proposition featuring large in industrial espionage. Billions of Euros per year are lost due to deliberately stolen information via hacking.

A hacking attack usually starts by sending the user an email with specially crafted attachment or link to click on. This event brings software onto the user's computer that executes some actions on its own. For example, it can activate a remote administration program that allows a human far away to work with the user's system as if he were the user.

Hacking takes place not only in personal computers for acts like credit card fraud but also for

corporate networks where significant amounts of data can be retrieved. This is being promoted by companies and governments working on industrial espionage.

It is the purpose of this project to detect patterns among normal user activity and abnormal hacking activity such that hacking activity can be flagged to the administrator while it is on-going.

We have teamed up with several large corporations like Deutsche Telecom and ZF in order to provide the data and the TZI at the University of Bremen to analyze this data.

In order not to access confidential information ourselves, we are restricted to analyzing only the headers of the packets of information transferred via the network. This should contain enough information to distinguish normal and abnormal use of the system.

Because the data volume is so large, we cannot use supervised learning (see page 1 of this report) as the human effort to label the data is too large. We must use Data-Mining to group the data into automatically discovered patterns of use prior to human categorization.

Detecting Hacking Attacks

Your IT Systems are vulnerable to hacking. To combat this problem you must recognize that someone is hacking you ...

Due to the subtle nature of the problem and the huge volume of data, this presents a formidable problem to the data analyst and data miner. However, the user is in the forefront.

“Someone is
hacking you
right now!”

The user of this new system is supposed to be the network administrator of a corporate network. This person should be told that a hacker attack is under way and should be told what to do about it.

One difficulty is the sheer number of attacks. Networks are under almost constant bombardment of attacks from various sources. It is difficult to find a time when a particular network is not under attack.

Thus, attacks must be grouped also by their threat level. Common attacks that can be dealt with by the system itself need not be brought to the attention of the administrator. Only serious attacks that pose a real threat should be alarmed.

This is a three year project and should allow a reasonable level of advance warning to the user. Most importantly it will be a learning system and so improve over time as the system sees new attacks and provide better and better detection services.



Plans for Next Quarter

1. A crisis has hit the industry world-wide. Production in chemical plants is down to 20 – 30% of normal levels. This crisis has been caused the USA real estate market bubble and has hit the industry via the collapse on the financial markets. This crisis impacts the sale of our flagship products NEMO and OMEN as these are primarily intended for the process industry with an emphasis on chemistry. Thus, we foresee a substantial slowing down in our business as a result.

To mitigate this effect, we will heavily go into process industry areas not so affected by the crisis, such as power generation, in order to promote our products.

While the decrease of the oil price in the crisis is good for consumers, it is bad for many remaining process industry participants. The whole energy related side is hit by this energy-crisis.

Thus the plan for the next quarter is to re-group our forces for a new type of client and to develop our products further to meet their needs. This crisis is a major one that is likely to last for considerable time and so survival is the foremost strategic aim.

The advantage is that many people will have much more time to think and plan during this time but unfortunately be lacking the financial means to start projects.

2. Demo applications of NEMO and OMEN are underway at various clients' sites. Improving these installations and delivering maximum gains is our top priority.

We are always extending the pool of machines that we can model based on our clients' needs.

3. We are due to become members of the Houston Technology Center giving us access to the USA energy industry. At an event in February, we will present ourselves and generate interest there. The goal is to deliver some demo applications to the USA during 2009.

What is ... pre-processing ?

As data analysts, we are constantly confronted with data that contains corrupted data. Data can be missing entirely, be corrupted by malfunctioning sensors, have spikes due to sensor problem, contain noise from external sources or be exposed to drift from temperature ranges.

These sources of noise must be cleaned up before a proper analysis is possible. This stage of cleaning is referred to as pre-processing. Often it is a very time consuming stage that requires lots of manual work and difficult discretionary choices to be made about what structures in the data stay and which leave.

We have methods to filter outliers, to smooth data, to delete spikes, to fill gaps and a variety of other patching tasks. Any result of such a task needs to be examined by hand though to make sure that the cleaning process did not damage the signal that we want to emphasize.

Whenever data is obtained, this pre-processing stage is executed and only the clean data is used to train a mathematical model which can then be used to predict or to optimize processes.

Because of the manual work, it is often here that the project costs are generated to a large extent.

EYE ON IT

Clients / Partners :

- Aluminium Norf GmbH
- Bayer Technology Services GmbH
- EADS N.V.
- EVONIK degussa GmbH
- Fraunhofer-Institut für Fertigungstechnik und Angewandte Materialforschung
- Infracor GmbH
- Institut für Internet-Sicherheit
- METRO Cash&Carry Deutschland
- mobile solution group GmbH
- Momentive Performance Materials Inc.
- National Aeronautics and Space Administration
- nicos AG
- Rhenus Lub GmbH & Co KG
- Rieter Automatik GmbH
- RWE AG ^{NEW}
- Ryanair Ltd.
- SASOL Solvents Germany GmbH
- Tchibo direct GmbH
- Technologie-Zentrum Informatik
- ZF Friedrichshafen AG
- T-Systems Enterprise Services GmbH
- TUI AG
- TÜV Rheinland Group
- UNI Dai-Ichi Shoji Co. Ltd.
- VESTOLIT GmbH & Co. KG
- VHV Vereinigte Hannoversche Versicherung a.G.
- Volkswagen AG
- Volkswagen Plant Salzgitter



Professional Development

Do you want a challenge?
We constantly seek bright people to add to our team of expert problem solvers. We offer internships, trainee programs, part-time & full-time professional employment. Contact us and experience working on state-of-the-art solutions within a friendly team.

Upcoming Events

• Houston Technology Center

07.-13.02.2009

This event brings together leading process industry decision makers to Houston, Texas. algorithmica will be present to make its value offering known. Please get in touch with us for a private meeting during the forum.

algoTimes Q4 2008

algorithmica
technologies

algorithmica technologies GmbH
Außer der Schleifmühle 67
28203 Bremen
Germany

Tel.: ++49 (0) 421 337 46 46
Fax: ++49 (0) 421 337 46 22
Mobile: ++49 (0) 176 2073 3149

info@algorithmica-technologies.com
www.algorithmica-technologies.com

algorithmica technologies Corporation
1900 West Loop South, Suite 880
Houston, TX 77027
USA

Tel.: ++1 (713) 629 43 43
Fax: ++1 (713) 629 87 99
Mobile: ++49 (0) 176 2073 3149