



### What is your data centres' biggest weakness?

Growing up, Superman has been one of my favourite superhero in the DC universe. Simply because he is the most powerful superhero in the universe. He is not from this planet, yet he is human, saving millions of lives and bringing order in a chaotic world. His strength is equated to that of a planet! How cool is that!

Even Superman has a weakness, kryptonite! his home planet's radioactive material that renders him weak and vulnerable. In Zack Snyder's Batman v/s Superman, Batman weaponized kryptonite into a burst of gas that weakens Superman and brings him down to his knees.

While watching this movie with my son, it made me wonder if our data centres could be equated to Superman. Just like Superman, data centres are the guardians of the world bringing order to chaos by managing our data 24/7 and protecting our privacy. Since the dot-com bubble of 1997-2000, dependability on data centres increased and more and more IT companies invested in the data centre infrastructure. As the data centre technology grew bigger, the components used in the data centres became smaller, making it more compact and used less space.

### Energy usage

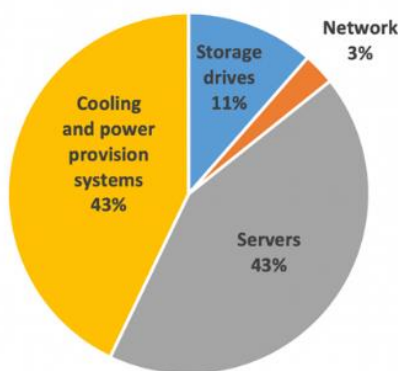


Figure 1. Fraction of U.S. data center electricity use in 2014, by end use. Source: Shehabi 2016.

Modern data centres take a lot of precautions in information security. In terms of protecting the information itself and physical security to avoid data theft. Firewalls, IDSs, layer 2 security (Port security, ARP inspection, Private LANS) and so on.

A lot of emphases is also given to the energy efficiency of the data centres since these data centres utilize a large amount of energy for their operations. The USA alone utilizes 3% of all its electricity in powering the data centres. Out of this up to 43% of electricity is used for cooling and power provision systems. Some of the world's largest data



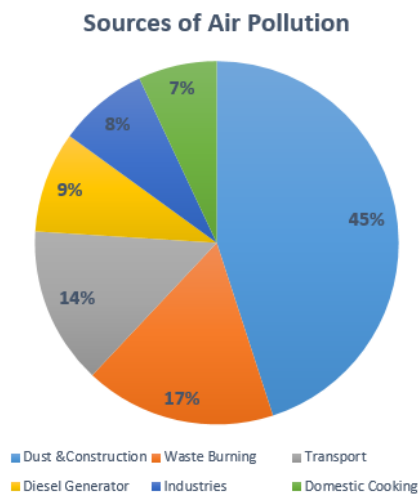
centres can each contain many tens of thousands of IT devices and require more than 100 megawatts (MW) of power capacity—enough to power around 80,000 U.S. households (U.S. DOE 2020).

### The problem

All these implementations have now given modern data centres the power to govern the information highway more securely. But just like Superman, data centres around the world have a common weakness, **Corrosion!** This is mainly attributed to the ever increasing global air pollution.

Air pollution is one of the world’s largest health and environmental problems and is also detrimental to data centres across the globe. Sources of air pollution in India are multiple and context-specific. The major outdoor pollution sources are industries waste burning, transport vehicles, diesel generators and construction.

As per WHO, major air pollutants include particulate matter, nitrogen oxide (NOx), Sulphur oxide (SOx) and Carbon monoxide. These pollutants find their way into the



facilities since most of the data centres use outdoor fresh air as a source for cooling. Although the particulate matter (PMs), PM2.5 and PM 10 are taken care of by pre and fine filters, gases are not filtered since the size of these gases are extremely well below 0.1 microns. These escape the filters and enter the facility undetected and saturate the indoor space and cause corrosion of hardware.

Since the advent of data centres, the major components in the hardware circuit boards was Lead up until 2003. RoHS (Restriction of Hazardous Substances), implemented in the European Union in 2003 under EU Directive 2002/95/EC, set limit values for Lead, cadmium, and several other chemicals in specified types of electrical and electronic equipment, including a Lead maximum of 0.1%. Since then Lead was replaced by Copper and Immersion silver in circuit boards majorly. This is when the industry realised that Copper and Silver corroded more frequently than its Lead counterpart. The IT industry was facing a huge problem in hardware failure because of corrosion.

Since the advent of data centres, the major components in the hardware circuit boards was Lead up until 2003. RoHS (Restriction of Hazardous Substances), implemented in the European Union in 2003 under EU Directive 2002/95/EC, set limit values for Lead, cadmium, and several other chemicals in specified types of electrical and electronic equipment, including a Lead maximum of 0.1%. Since then Lead was replaced by Copper and Immersion silver in circuit boards majorly. This is when the industry realised that Copper and Silver corroded more frequently than its Lead counterpart. The IT industry was facing a huge problem in hardware failure because of corrosion.

Classification of Reactive Environments				
Class	G1	G2	G3	GX
Severity Level	Mild	Moderate	Harsh	Severe
Copper Reactivity	<300Å	<1,000Å	<2,000Å	≥2,000Å
Silver Reactivity	<200Å	<1,000Å	<2,000Å	≥2,000Å
Comments	Corrosion not a factor in determining equipment reliability.	Corrosion effects are measurable and corrosion may be a factor.	High probability that corrosive attack will occur.	Only specially designed and packaged equipment will survive.

## How does corrosion occur?

The presence of SO<sub>x</sub>, NO<sub>x</sub>, H<sub>2</sub>S (Hydrogen sulphide), chlorides in indoor air are major contributors to corrosion in the electronic components. These gases, in a long run, react with the components and form oxides, halides of copper and nitrogen and cause creep corrosion. These sever the fine connections in the circuits and cause hardware failures. To address this issue, ANSI (American National Standards Institute) and ISA (Industry Standard Architecture) came up with ANSI/ISA 71.04-2013 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants guidelines. This standard covers airborne contaminants and biological influences that affect industrial process measurement and control equipment, electronic office equipment, and data centre and network equipment. The classification of the reactive environment is as follows:

The OEMs such as Honeywell, Dell, IBM and so on mention the severity level of the environment around their components to G1 and insist their customers maintain these levels so that warranty on the components is not affected.

## The solution

Detection of these corrosive gases is the most important step in mitigating corrosion. Specialised corrosion detection and monitoring devices ([OnGuard series](#)) by [Purafil](#) help to detect corrosive gases as low as 1 Angstrom. These systems have copper and silver sensors that employ metal-plated quartz crystal microbalances (QCM) for real-time reactivity monitoring. For short term passive monitoring, [Corrosion classification coupons](#) (Copper and silver plates) are installed for 30 days after which they are analysed for the corrosion film composition. The cumulative corrosion is calculated and a comprehensive report is generated.

Once these corrosive gases are detected, filtration of these gases can be done with the help of [Purafil](#)'s patented chemical media. [Purafil](#) offers a range of chemical media and filtration solutions to filter out the corrosive gases at any concentration. The chemical media are impregnated in pellets and works on the principle of chemisorption, where the gases are adsorbed and neutralised and fresh filtered air is allowed in the facility. [Ripple Effect](#) in partnership with provides end-to-end solutions in this regard.

Detection, monitoring and filtration of corrosive gases in the data centre facility are as important as setting up the facility itself. The cause and effect: extend the life of components in data centres, reduces breakdown and maintenance schedules, increases energy efficiency and reduces massive cost implications.

**Imagine if Superman was immune to kryptonite!**

*Follow us*

