THE CASE FOR MEDICAL ELECTRONICS SUPPLY CHAIN TRANSPARENCY

A number of factors are putting medical electronics supply chains at risk. It is urgent that device companies act on them now. What are they and what can be done about them?

BY ERIK SWAIN

There are a number of pressures on the electronics supply chain today, and they are affecting medical device companies like never before. Environmental regulations, business decisions caused by the volatile economy, political turmoil, and natural disasters are among the factors creating supply problems for electronic components.

This can have a tremendous impact on a device company's revenues and reputation. If a component or material is not available or restricted and a firm does not have a backup plan in place, it cannot fulfill its manufacturing goals or keep up with customer demand. It also makes itself vulnerable to price spikes, fines and other consequences of noncompliance, and counterfeiting.

> "THE MORE REGULATIONS WE HAVE, THE MORE SHORTAGES WE HAVE. THE MORE SHORTAGES WE HAVE, THE MORE COUNTERFEIT PARTS WE WILL SEE."

These issues are already having a monetary impact. For example, in the second quarter of 2010, General Electric Co. attributed $50 million in lost sales for its GE Healthcare division to "supply constraints for its electronic components," according to the *Wall Street Journal*.

In order to prevent those kinds of scenarios from coming to pass, medical device companies must tightly monitor all phases of their electronics supply chains – or have a partner do it. A finished medical device

can't ship until it has 100% of its parts installed, so the supply chain for every part must be tracked and accounted for, and any potential part shortages must be anticipated and worked around. The days of medical device companies dealing only with their immediate suppliers and immediate customers are over. They must be aware of what is going on at all steps of the supply chain.

"Medical device OEMs have to make decisions differently than they did in the past," says Scott Wilson, content solution strategist for IHS, a firm that provides data, analysis, market intelligence, and other services. "They can't just consider what parts they need; they have to ask if their parts are compliant, and if they can get detailed compliance, design, and life cycle information for those parts."

The urgency of the situation was reinforced in March, when an earthquake and tsunami in Japan shut down a number of electronics manufacturing plants. According to IHS iSuppli, over half of the world's electronic component manufacturing takes place in Japan, and the disaster is causing some supplies to be disrupted. Companies that have visibility into their supply chains will be able to find alternative solutions to alleviate shortages and the problems that stem from them. Companies that do not have visibility into their supply chains may not be able to react until it is too late. They may get stuck with higher prices for components, lost sales, and decreased profits. Worse, they may end up using counterfeit parts that could impact product performance and harm patients.

Medical device companies can no longer afford to be ignorant of electronics supply chain issues, all the way down to raw materials. There are too many factors in play right now that have the potential to cause shortages, which may bring about a number of disastrous consequences. What follows is a breakdown of the major factors that are causing shortages of electronic components and materials, and a discussion of how supply chain transparency can prevent or mitigate the problems that stem from shortages.

REGULATORY CHALLENGES

One of the largest contributors to disruptions in the electronics supply chain is the growing number of regulations being promulgated around the world, much of them dealing with environmental issues. In some cases, medical devices are exempt, but device OEMs need to understand these issues anyway, because their electronics suppliers are also selling to industries that are affected and might discontinue parts for their entire client base because of new regulations.

Device companies must pay attention not only to governments that are restricting or banning the use of some chemicals and substances for environmental reasons but also to non-governmental organizations (NGOs) that are raising awareness about toxic substances, and to customers who are basing contracts and purchasing decisions on environmental compliance.

"Compliance and sustainability are topline issues," says Jim Brown, president of Tech-Clarity, a research firm that analyzes the business value of software technology. "It is not just a way to save legal fees. The potential consequences include being locked out of markets entirely. Regulations add a tremendous amount of challenge."

One trend is regulation of "conflict minerals," Paul E. Hagen, principal of Beveridge and Diamond, P.C. said at a recent IHS Focus Group. The idea is to clamp down on the use of minerals obtained from mines that are being used to fund wars and repressive regimes, most notably in the Democratic Republic of Congo (DRC).

In the United States, the Dodd-Frank Act, which brought reforms on the financial sector, requires the Securities and Exchange Commission (SEC) to promulgate rules on how it will make firms disclose whether their products contain minerals mined from the DRC. As of this writing, the rules had not been published, but the SEC is expected to require firms to file an annual report stating whether they are using conflict minerals, and if so, whether they are necessary for functionality or production, says Hagen. Third-party auditing will likely be required. The minerals in question are columbite-tantalite (coltan), cassiterite, wolframite and gold. The derivatives are the more commonly known tantalum, tin, tungsten, and gold used in electronics and other industries.

"Companies may also label their products DRC-conflict-free," says Hagen about products that don't contain conflict minerals believed to finance armed groups in the DRC. "We expect that will drive some changes in the market."

A significant fallout from the regulation is that OEMs are going to have to reach all the way to the beginning of their supply chains to determine where smelters are getting their minerals, Hagen says. International organizations have just begun to certify smelters who are not using minerals from the DRC. Encouragingly, firms all along the supply chain appear to be aware of this issue, which was not the case at the outset of many other regulations.

Another regulation device manufacturers must heed is the recast of the European Union's Restriction of Hazardous Substances (RoHS) Directive. RoHS from its inception has declared that no product sold in the EU shall contain more than 0.1% of lead, mercury, hexvalent chromium, or two types of polybrominated flame retardants. It also prohibits sale in the EU of products with more than 0.01% of cadmium.

RoHS recast, which will become legally binding in late 2012 after it is transposed by member states, removes the exemption for the medical device industry and compels mandatory disclosure for non compliance, Hagen says. In most cases, medical devices will need to comply by 2014.

"THE TIMELINES TO COMPLY WITH RoHS RECAST SOUNDS LIKE A LOT OF TIME, BUT WHEN YOU THINK ABOUT THE QUALIFICATION PROCESSES REQUIRED WHEN CHANGES ARE MADE TO A MEDICAL DEVICE, THAT TIME GETS EATEN UP QUICKLY"

"The timelines to comply with RoHS recast sound like a lot of time, but when you think about the qualification processes required when changes are made to a medical device, that time gets eaten up quickly." say Wilson. "In reality, it's very little time."

Another major development is that compliance with RoHS is now a requirement for a CE Mark, which allows a product to be sold in the European Union. Companies that aim to comply must keep detailed technical records on their compliance, and in some cases may need to perform or obtain compliance testing. As has always been the case with RoHS, companies that do not comply could find their products banned from being sold there, which puts them at a tremendous disadvantage globally.

While RoHS is an EU regulation, it has become the template for other regulations around the world, including in some U.S. states, and in particular has inspired a number of regulations on batteries. For example, a proposed U.S. Department of Transportation

rule would impose substantial new constraints on the transport of lithium batteries, especially by air.

Even more far-reaching is the EU's Registration, Evaluation, Authorisation, and Restriction of Chemicals (REACH) regulation, which classifies chemicals and substances according to their toxicity, singling out the worst offenders for banning and aiming to restrict the use of Substances of Very High Concern (SVHC). Any material that appears on the SVHC list is likely going to be hard to come by in the future, having a dramatic impact on the medical device supply chain, perhaps even in cases where medical devices have exemptions.

By November 30, 2010, the most widely used and most dangerous chemicals had to be registered, regardless of whether they were on the SVHC list. Manufacturers who failed to register them can no longer use them.

Separately, by June 1, 2011, any products that contain more than 0.1% of any SVHC had to be reported to the European Chemicals Agency (ECHA).

There may be some exemptions for medical devices, but that might not matter if suppliers, most of whom serve other industries as well, find it unprofitable to make one version of a component for medical devices and another version for everything else.

"Some companies are focusing on exemptions, but that may not be the best long-term strategy," says Rory King, director of global product marketing at IHS. "In reality, if your suppliers provide materials to medical customers and other customers, and their other customers need them to get rid of a substance, either they are going to provide two substances, or end the version with SVHC. It is not the best strategy to assume the former. For example, a lot of suppliers have decided to get out of the lead parts business altogether, simply because part of their customer base can no longer use lead-based parts due to RoHS."

Device companies that fail to keep up with REACH requirements may also be bogged down with major redesign costs, since they are prohibited from switching out parts without performing revalidation and getting the FDA to sign off on it.

There are 46 substances on the SVHC list, 15 of which have been proposed for authorization. If put on the authorization list, they can only be used with the permission of the ECHA. That is the first step toward phasing them out altogether.

"RoHS was very costly, but REACH is expected to be even more costly," Wilson told an IHS Focus Group. "We have to understand what SVHCs are in the parts we produce, and we may be required to warn end users of SVHCs."

Also being recast is the EU's Waste Electrical and Electronic Equipment (WEEE) Directive. It aims to reduce the amount of electrical and electronic waste that is disposed of, and sets targets for the recovery of medical devices.

That, Hagen says, has inspired numerous "take-back" laws around the world, including in 24 U.S. states and a number of Latin American countries.

"A common element is linking compliance with a take-back plan to market access," Hagen notes. That is, firms who are not addressing this issue could find themselves banned from selling their products in certain jurisdictions.

Device firms also must be aware of the tenets of the Basel Convention, a worldwide treaty that restricts the movement of hazardous wastes between nations. More used and end-of-life products are being classified as hazardous wastes for the treaty's purposes, including end-of-life medical and electronic equipment, Hagen says.

An unintended consequence of WEEE is that in less developed countries, some parts that fall under the WEEE purview are being "recycled"

into counterfeit parts, Wilson says. So vigilance against counterfeiting should become an even bigger priority for OEMs doing business in developing markets.

Keeping track of all these regulations is very important to supply chain risk mitigation, Hagen emphasizes. One way to accomplish that is to use EIATRACK, an online tool found at *www.eiatrack.org* that was established by members of the Telecommunications Industry Association (TIA) in order to quickly and cost-effectively navigate the maze of global environmental regulations and legislations.

With REACH, the recasts of RoHS and WEEE, and other regulations all coming online at around the same time, not only do firms have to make sure that all their new products comply, but they have to go back through the supply chains for every existing product to ensure that they are compliant, Wilson says.

"We are at a unique point in time," he says. "This represents a great deal of work. You may have to find alternate sources, and to redesign products with compliant parts. It is mind-boggling, the rate of change that is going on with environmental regulations. There has been a 46% increase in environmental regulations in the last two years. There are 300 new laws slated to come into effect in 2011."

An appropriate action plan has four main tenets, Wilson says:

- Track environmental regulations around the world using tools such as EIATRACK and understand how they impact the products your firm makes.
- Make sure the parts and materials used in your firm's products are compliant.
- Track your suppliers' decisions to change or discontinue materials.
- Track parts and materials that have been or are at risk to be counterfeited.

"DEVICE MANUFACTURERS AND OTHER COMPANIES PARTICIPATING IN A RECENT BEST PRACTICES CONFERENCE SAID THAT ABOUT ONE-THIRD OF THEIR CONTRACTS OR RFP'S HAVE REQUIREMENTS AROUND ENVIRONMENTAL COMPLIANCE OR SUSTAINABILITY MANDATES TO RESTRICT HAZARDOUS SUBSTANCES."

There is no one right way to organize these efforts. About 50% of device companies surveyed by IHS give the responsibility to their quality team, while about 25% give it to their environmental health and safety team; about 25% give it to their procurement and/or supply chain groups. Similarly, there are different technologies that can be used to keep track of everything, from dedicated compliance-management systems to product life cycle management systems to expanding existing systems. The larger and more global the company, the more likely it is to need a system that covers everything.

Regardless of who gets put in charge of the tasks, personnel from a number of different functions should be in the loop, Wilson says. This also includes IT personnel, ERP personnel, design engineers, and lawyers.

It is also important that device companies do not adopt an attitude that doing the minimum to comply with the regulations will suffice. More healthcare customers are demanding that their suppliers not only comply with measures like RoHS and REACH, but in some cases, that they exceed them, for instance by requiring information for additional substances that are not currently regulated.

"Device manufacturers and other companies participating in a recent best practices conference said that about one-third of their contracts or RFP's have requirements around environmental compliance or sustainability mandates to restrict hazardous substances,"

Wilson says. "It's not enough just to comply with the law. Client requirements are applying additional pressures. It really has stepped up." Notably, Kaiser Permanente, one of the largest healthcare organizations in the United States, has an extensive set of environmental requirements that it uses to differentiate among potential suppliers.

OBSOLESCENCE CHALLENGES

Any time use of a material or component is dissuaded, there is a risk that suppliers will decide that it is no longer worth the aggravation to stock it, and discontinue it.

"Regulations that lead to chemical restrictions always lead to obsolescence issues with parts and materials," Wilson told an IHS Focus Group. "So you have to take appropriate measures to ensure continuity of supply. You have to make sure you have a way to track your components. Even if a regulation does not apply to your industry, it could force parts you rely on to become obsolete."

> EVEN IF A REGULATION DOES NOT APPLY TO YOUR INDUSTRY, IT COULD FORCE PARTS YOU RELY ON TO BECOME OBSOLETE."

Obsolescence is usually a concept thought of when new technology displaces old, but suppliers also make obsolescence decisions when scarcity occurs. This can be because of environmental considerations, because of political upheaval as in the DRC, because of a natural disaster as in Japan, or because of an economic downturn anywhere in the world. Therefore, it is critical not only to track parts that have gone obsolete but also to anticipate the ones that will.

"You must have flexible and responsive supply chains that understand and track these pressures, and that have the tools to respond to them," Wilson told the group.

Firms like IHS are able to do such tracking on behalf of medical device companies. Among other things, a partner can catalog end-of-life (EOL) notices and determine why particular parts are being discontinued. That can help predict which parts are likely to be made obsolete in the near future. For example, a spike in EOL notices in 2006 correlated with the implementation of the first version of RoHS. A spike in product change notices (PCNs) correlated with the run-up to RoHS taking effect.

If vendors of a part whose supply has become constrained do not decide to discontinue it, they are likely to begin charging much more for it. This, too, is a trend device companies want to spot before it happens, Wilson says.

This is why device firms need to practice predictive obsolescence, or partner with others that do, Daniel Bronstein, a solutions engineer for IHS, told an IHS Focus Group. He defines predictive obsolescence as "steps taken to mitigate effects of obsolescence by applying predictive forecasters to component production and sales decisions."

At its core, the practice involves assigning a part a spot on a life cycle continuum. One way, based on the EIA 724 standard, is to give a part one of five designations:

- Code 1. The part has been newly introduced. Little sales data is available, and it's not known if it will succeed well enough to be continued. The price is high because R&D costs must still be recouped. Manufacturing may be in low volumes.
- Code 2. Sales and demand are growing, cost is coming down. Manufacturing is in higher volumes.
- Code 3. Demand and price have stabilized. Manufacturing and profit are as high as they will get.
- Code 4. Demand is in decline and phase-

out may have begun. Manufacturing is returning to lower volumes.

- Code 5. Production has stopped completely, or nearly so. The product's price is high and it may only be available in the aftermarket. It is susceptible to counterfeit.

For optimal results, products should have as many Code 2 and Code 3 parts as possible, and OEMs need to have a good idea when parts will shift to Code 4 and Code 5.

Another aspect of predicting obsolescence is calculating Years to End of Life (YTEOL), says Bronstein. That is, the number of years until a part is no longer available. Factors include the specific marketplace, how many and what type of manufacturers are making a part, sales data, and any disruption that impacts availability.

Having YTEOL data at their disposal will enable medical device OEMs to anticipate which components might not outlive the expected life cycle of a product, and enable them to effect changes to it as quickly as possible. Advance knowledge is especially crucial in medical technology, where regulations often make changes to a product difficult once it is on the market.

The best way to incorporate predictive obsolescence into your operations, says Bronstein, is to "work with internal or external sources to get accurate, complete, and up-to-date part lists. It is very critical that this information be available. You may need a contract in order to get that data, so additional funding may be required in your product planning."

Failure to perform predictive obsolescence

Component Obsolescence Forecast

Years-to-End-of-Life (YTEOL)

Current Availability	1 – 2 Years	3 – 4 Years	5 – 6 Years	7 – 8 Years
Available	Available	Available	Available	Available
Available	Available	Available	Available	Available
Discontinued	Discontinued	Discontinued	Discontinued	Discontinued
EOL	Discontinued	Discontinued	Discontinued	Discontinued
Available	Available	Discontinued	Discontinued	Discontinued
Available	Available	Available	Discontinued	Discontinued
Available	Available	Available	Available	Discontinued
Available	Available	Available	Available	Discontinued
Available	Available	Available	Available	Discontinued

End Item ***Parts***

End Item ***Requirement***

Source: IHS Inc. 2011

means a firm is increasingly likely to have to go outside its normal supply chain to obtain parts. And that makes it susceptible to price spikes (up to 2000% in some cases) and counterfeits. As an example, IHS had a client that was using so many outdated materials on a product that it cost $5,000 to produce a device that sold for $1,500. As another example, says Bronstein, an electronics manufacturer found that in one year it spent $14 million more than it should have on end-of-life and discontinued parts because it was unaware of changes in availability until they happened. By implementing a predictive obsolescence program, they would have saved significant funds.

The consequences can be particularly disastrous in the medical device industry, says Brown. "If a component is EOL'd or has a shortage because of something like a conflict minerals issue or a natural disaster, there's the normal impact such as finding alternate supplies and engaging in costly redesigns," he says. "Then when you add in the fact that changes cannot be made rapidly in the medical device industry because of issues like revalidation and process realignments, the impact can be extensive. Especially when there are no pure substitutes, as happens in a lot of cases."

COUNTERFEITING CHALLENGES

Another reason that device companies must do everything they can to avoid using parts that are obsolete or in short supply is that the scarcer a part is, the more likely counterfeits will flood the marketplace.

"As soon as a part becomes in short supply or obsolete, we see opportunistic individuals and companies popping up and reporting materials as something they are not," Wilson says. "The more regulations we have, the more shortages we have. And the more shortages we have, the more counterfeit parts we will see. Make sure to have the resources in place to deal with these and other supply chain issues."

Counterfeiting is pervasive. An investigation by the Senate Armed Services Committee revealed that as much as 40% of the U.S. Department of Defense's electronics supply chain has been impacted in some way by counterfeit parts. [1] The Pentagon is one of the nation's largest purchasers of medical equipment, so this finding could have far-reaching implications for the medical device industry.

"Counterfeiting has very severe repercussions," Wilson says. "It means you can run into reliability issues – and the terrible things that can go along with that."

Allowing a product to be shipped with counterfeit electronic parts can do immense damage to a device OEM's relationship with its customers. "It is often considered a contractual obligation that all parts of a product be authentic and compliant," says King. "It is assumed you will ship that, and there will be consequences if you don't. In that way, your customers are really another set of regulators."

There are two things device OEMs must do in light of this, Wilson says. "First, they must track their parts, understand which are likely to be counterfeited, and be aware of when incidents are reported," he says. "If they understand supply constraints and obsolescence issues, that will put them in a position to understand what type of parts they should keep a close eye on. Second, they need to perform stringent incoming inspections to identify any suspect parts. There's always a chance they could be affected by parts that are not known to have been counterfeited before."

The highest risk of buying counterfeit parts occurs when a firm has to go outside its normal supply chain to find parts that it cannot get (either temporarily or permanently) from its authorized suppliers.

"Buying from unauthorized suppliers means you could spend quite some time need-

ing to verify the authenticity of a part," says Bronstein. "Special tests can be needed, and the purchasing process can take longer."

The only surefire way to know you are not getting a counterfeit part is to buy directly from the manufacturer, Mark Snider, ERAI's founder and president, told an IHS Focus Group. "At every stage beyond that, you are exposing yourself to at least some element of risk," he said. "A blanket policy banning open-market sourcing will eliminate some risk, but not all of it." ERAI is an international information services organization that monitors, investigates and reports issues that are affecting the global electronics. It has an exclusive partnership with IHS to report on and track worldwide counterfeit incidents and supplier risk throughout the supply chain.

But if other sources must be explored, some ways to do it are better than others. The worst is to search Google or another general Internet search engine because they will lead you to all kinds of shady operators who are not only selling fake goods but whose numerous illegitimate claims of access to stock can inflate false expectations of inventory available in the supply chain. "Searching on Google should be your last resort," Snider says.

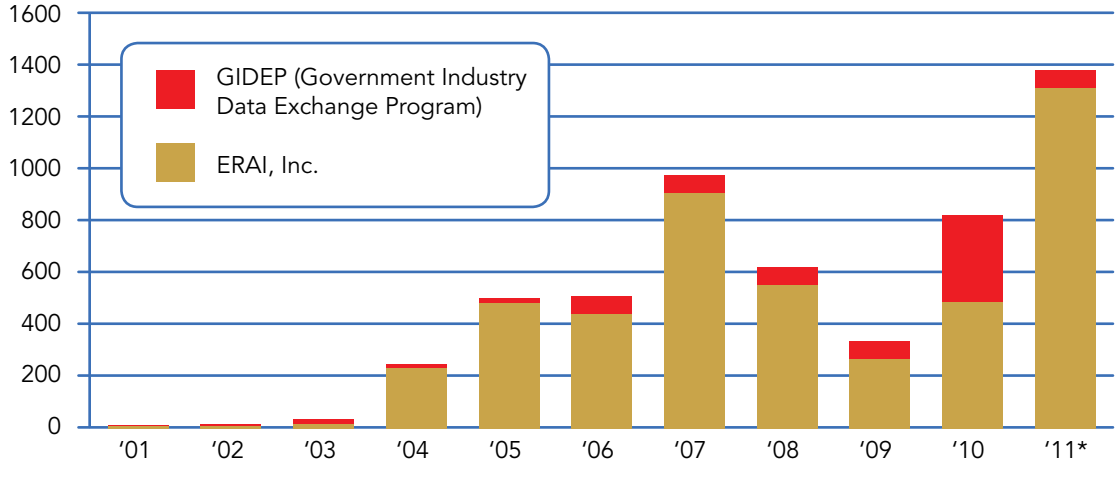
Instead, firms should have a small number of independent supply partners to tap in case a part is not available through the regular channels, and they should be properly vetted. "Contractually define your obligations and test accordingly," Snider says. "Do not deviate from your quality procedures."

Part of the vetting process should be checking if the vendor is in ERAI's database and how long it has been a member. ERAI has a zero-tolerance policy regarding counterfeiting, so being listed in the database means the vendor has never had a counterfeiting complaint lodged against it. On the flip side, OEMs can also check the Reported Companies Database to see if the vendor has been accused of selling fake parts.

It is imperative that OEMs be aware of what parts have been counterfeited and what parts are at risk to be counterfeited.

Counterfeit Incidents Reported, 2001 to 2011

GIDEP and ERAI



Source: IHS Inc. 2011
Note: 2011 figures asterisk (*) denotes projected estimate based on YTD reports

One way to track the former is with the Reported Parts Database at ERAI. Every electronics counterfeiting incident that gets reported to ERAI gets put in the Reported Parts Database, where a notification immediately warns other subscribers of the potential new threat to their products, Snider says.

ERAI also has a parts search database into which member vendors have posted their inventory, so OEMs can get an idea of which parts are readily available (and thus unlikely to be counterfeited) and which ones are not.

The U.S. government has its own database of reported counterfeit parts, the Government Industry Data Exchange Program (GIDEP), which is another tool medical device OEMs can use to keep ahead of the counterfeiters.

ERAI and IHS also offer a service whereby an OEM can input the bill of material for a product and receive a report as to whether any of the electronic components have been counterfeited or are at risk to be. In one case, four of the 94 electronic parts of a respirator were found to be counterfeit.

IN ONE CASE, FOUR OF THE 94 ELECTRONIC PARTS OF A RESPIRATOR WERE FOUND TO BE COUNTERFEIT.

Also, medical device OEMs who partner with market-intelligence firms can get a leg up on where in the world it needs to be extra vigilant about problems with counterfeiting, conflict minerals, and other hot-button issues.

"If, say, you try to enter the Colombian market and set up a supply chain there, you might need extra help in figuring out whether they use conflict minerals there," says Gustav Ando, director of healthcare and pharmaceuticals for IHS Global Insight. "Whereas that might not be as much of an issue in Venezuela, but there could be other challenges there."

It is also imperative that device firms weed out potential sources of counterfeit and other problematic parts during the earliest stages of product development, because the farther along in the development process a problem is caught, the more expensive it is to fix, says Brown of Tech-Clarity.

"Your design flexibility starts to rapidly decrease the farther you go," he says. "The cost and impact of changes start to ramp up. As you move down the design path, you make decisions that lock in certain aspects of the product. Once you source components and validate suppliers and their parts, you add costs, and all the decisions you make are interrelated. And medical device companies can't just swap out a component like automotive or electronics companies can. Any time they make a change, there is a validation issue."

A serious supply chain problem that forces a redesign can cost an OEM valuable time and money. An IHS survey in 2010 found that 88% of medical device OEMs say a redesign takes more than six months, and almost one-third say it takes more than 18 months. In today's highly competitive global market, that produces a huge disadvantage.

One example highlights this problem starkly. IHS found that 33% of one client's parts were out of compliance to various regulations; 79% of those noncompliant parts had a supplier-recommended replacement, but 21% did not. What would be the impact of an unscheduled redesign and certification of those 21% of noncompliant parts? Tremendous, regardless of the product.

Therefore, during development, all potential supply chain issues, from sustainability to SVHCs to counterfeits, should be brought together in a thorough analysis process. Firms must consider not only the current issues but also issues that could have an impact over the entire life cycle of the product. That means, for example, that an OEM cannot wait for an environmental regulation to be enacted before

taking steps to comply with it. It must account as well as it can for any regulations likely to make an impact at any point during a product's life cycle. Partners like IHS and ERAI can help with this.

"This kind of product stewardship has become a market necessity," says King.

Given the structure of the medical device industry, failure to take these kinds of steps has grave consequences, Brown says.

"In medical devices, which often have long life cycles, there is a tight relationship between customers and producers," Brown says. "In order to sell a medical device, you have to service it and keep it working throughout the product life cycle. That's a tremendous amount of investment. At the same time, there is a tremendous amount of innovation, with new products coming out all the time. That creates a dual risk if there is a problem with the supply chain. For products already on the market, a problem like using obsolete or counterfeit parts means you have missed customer requirements, and your costs to fix them will not be supported by the market. But it also delays your ability to enter new markets with new products and to get things approved."

88% OF MEDICAL DEVICE OEMS SAY A REDESIGN TAKES MORE THAN SIX MONTHS, AND ALMOST ONE-THIRD SAY IT TAKES MORE THAN 18 MONTHS. IN TODAY'S HIGHLY COMPETITIVE GLOBAL MARKET, THAT PRODUCES A HUGE DISADVANTAGE.

IMPACT OF JAPAN CRISIS

At no time has the value of transparency and communication throughout the supply chain been more apparent than now, as a result of the earthquake and tsunami that struck Japan in March 2011 and crippled some of its electronics manufacturing plants.

Even the plants that were not impacted directly by the disaster have been affected, because government-imposed blackouts and brownouts necessitated by disaster-related energy problems have left plants throughout the country without power at times, interrupting production.

"This has impacted a wide array of the electronics supply chain, from manufacturing to packaging to inventory and shipping," Dale Ford, senior vice president for market intelligence services for IHS told an IHS Focus Group. "This is the biggest impact on the electronics supply chain in the history of the semiconductor industry." Japan produces 60% of the world's silicon wafers and 20% of the world's industrial electronics.

The plants suffering direct damage may not be back to full capacity until the summer or fall of 2011, while those suffering indirect effects from the disaster have lost anywhere from a few weeks to a few months of full production. There have been reports of supply crises in medical electronics already, Ford says.

Device OEMs who know where their electronics supplies come from and either already had non-Japan sources or quickly lined ones up are less likely to be impacted by the disaster than those who don't know much about their own supply chains, or know only enough to panic.

"Days after the Japan crisis unfolded, through examination of manufacturers providing IHS full disclosure of substances that make up certain component commodities, we could

pinpoint 91% of the parts containing silicon potentially at risk and link those to the relevant plants and manufacturers," King says. "If someone in your supply chain has been completely compromised by a disaster like this, or there becomes a counterfeiting concern, having this kind of intelligence can show you the alternatives that can mitigate risks. The need for visibility is critical."

And the risks are becoming apparent. "We are seeing an increase in activity on the open market, especially with the problem in Japan," Snider says.

Compounding the problem, when a disaster strikes, OEMs concerned about a parts shortage may unwittingly create a frenzy that leads to more of a shortage than there would have otherwise been, as well as price spikes and maybe even counterfeits. Multiple buyers from the same organization might panic and order extra parts in anticipation of a shortage. That kind of spike in demand creates price spikes and intensifies the prospect of an actual shortage down the road. A number of supply chain experts say they are seeing this kind of behavior in the wake of the Japan disaster.

"We are already seeing evidence that the Japan crisis has made matters worse," says King. "In addition to component shortages, we see evidence of price increases and buyers accumulating materials. We also see companies purchasing materials from lesser-known open market suppliers, which is commonly viewed as where counterfeit parts are more prevalent."

THE IMPORTANCE OF TRANSPARENCY

Given the increasing challenges facing the electronic components supply chain, it has never been more important that medical device companies understand what is going on throughout their entire supply chains. That means they have to, among other things, manage obsolescence issues, track parts availability, account for all EOL and PCN notices, check for counterfeit parts and be on top of which ones are at risk for counterfeiting, be aware of any regulations that have the potential to limit part or material supplies, and get a handle on any other constraints that may present themselves.

For starters, OEMs need to set up a standard for how to communicate with suppliers and customers in order to maintain supply chain continuity. A couple of good templates are JEDEC Standard No. 46C, which covers PCNs, and JEDEC Standard No. 48, which covers EOL and discontinuance notices. JEDEC standards govern the semiconductor industry but can be adapted anywhere.

Then, for best results, OEMs should have a tool at their disposal that tracks and analyzes individual life cycle change events and aggregates them to help make key decisions. Companies like IHS offer such tools, which can monitor when EOLs or PCNs are sent, and notify the OEM immediately through a closed-loop system.

If the OEM has at its disposal the primary reasons why EOL notices on electronic parts were given, it can use that data to anticipate what other parts might become obsolete soon, and be sure not to include them when designing new products or redesigning existing ones. This is in keeping with FDA's mandate that device OEMs use real-world information in order to make improvements on subsequent designs.

For example, the data show that environmental compliance-related EOLs spiked in 2006 and 2007 because of RoHS, and demand-related EOLs spiked in 2009 because of the worldwide economic slowdown.

"Everyone has been focusing on compliance, but in reality, you have to focus on the

supply chain," says King. "If you don't look at the larger picture, you might shoot yourself in the foot." In the long run, addressing issues with one-off compliance projects is much more expensive than addressing them with a revamp of the supply chain to make it more efficient and transparent.

It is equally important to be able to see PCN data. Changes are made to parts all the time, especially in terms of material composition, and OEMs who aren't aware of this may find themselves with a product that is significantly different from what they thought they had. For example, one IHS client had a change in material status over a 12-month period for 38.5% of 2000 parts it used. "If you're not paying attention to something like that, such a change in material status can be the difference between being in and out of scope with a compliance regime, notwithstanding it being a fundamental change in the materials used in your supply chain, product, or manufacturing process," says King.

The bottom line is that paying attention to EOL and PCN data enables OEMs and their partners to predict shortages, and as has been discussed, one of the worst things that can happen to a product's profitability is a parts shortage, as those lead to obsolescence, price spikes, and counterfeiting.

"Access to part and material insight can mitigate disruption," says King. "The market now demands sustainability and transparency, and the supply chain is where risks emerge or benefits can be derived by applying resources appropriately. Now, more than ever, manufacturers must empower people to do just that."

[1] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf