ONAP insider

amdocs

introduction

Since the creation of ONAP, the Linux Foundation has aligned some of the telecoms industry's biggest players behind a single automation and orchestration platform for virtualized networks.

This is a major step forward in terms of realising the long-term vision, which is for ONAP to become a 'Windows' for the telecom sector: a unified, standardised operating system on top of which new services and apps can be created.

Our ONAP Insider series takes you behind the scenes, offering a more in-depth look at the workings of ONAP, how it is changing business models, simplifying network design and tapping new business opportunities for service providers, content developers and end-users.

table of contents

why it makes sense to open-source ECOMP

By Dr. Eyal Felstaine
CTO & Head of Technology Office
Amdocs

From its inception, AT&T's ECOMP platform for NFV automation has attracted attention because the project has been led by a service provider rather than a vendor or a standardization body. The recent decision to convert ECOMP to an open source project and irrevocably hand the majority of its code to the Linux Foundation has put it back in the spotlight.

Well-established in the IT world, the open source model remains something of an alien concept in telecoms. You could say that its ethos of free licensing, open collaboration and fast-paced development is diametrically opposed to our industry, which is built on proprietary solutions, ring-fenced Intellectual Property and lengthy design cycles.

Yet, as cloud and virtualization technology grows its foothold in telecoms, and service providers become more like their Cloud counterparts, they – and everyone else in the industry – need to review their business models and modus operandi.

All hands on deck for standardization

AT&T realized that 'cracking' VNF orchestration and automating lifecycle processes would be crucial to reaching its target of virtualizing 75% of its network by 2020. Its decision to recruit telecom operators and blue chip vendors as founding members of ECOMP established the collaborative direction that would eventually see the project converted to an entirely open-source initiative.

Amdocs was one of the early contributors, and it was clear to us that this approach would ring in fundamental changes to how our industry works.

By involving the global open source developer community and encouraging broader industry involvement in the open source project – from other operators, system integrators and VNF vendors – work can be spread across a much wider group. Sharing the burden across an ecosystem of contributors will result in accelerated development cycles and allow organizations to reduce their individual cost base. This has the potential to move open source ECOMP closer to becoming the de-facto 'gold standard' in orchestration. It is already being recognized by service providers like Bell Canada and Orange. I have full confidence that we will see more operators joining and committing resources to developing the code base.

Speeding development

Another early insight was that it did not make sense to rely on a proprietary solution for an end-to-end MANO (Management, Automation and Network Orchestration) solution, which would have been the traditional approach.

The cost of a developing, maintaining and constantly updating the code for a proprietary solution single-handedly incurred by any given vendor – would be prohibitive. Vendors would ultimately extend the cost to their customers, and service providers would have to bear the brunt of it.

Another issue is that tweaking VNFs to work with an orchestration platform is a costly and time-intensive undertaking. When operators introduce a VNF into their network this typically involves a lot of changes and alterations to code. This means going back and forth to the vendor, discussing requirements with various teams – from tech support to product management – and initiating functional requests for the vendor's R&D department to come up with a solution.

This process can easily take several months and tie up multiple teams – equating to a huge loss of time and unnecessary labor costs. Conservative estimates put the overall impact of these iterations at around 35% of the overall project cost. This runs counter to the budget pressures service providers are under, and the fast pace of innovation required to stay competitive.

Establishing greater transparency

By tapping into the open source community, the path from designing to rolling out new services can be streamlined, resulting in dramatic reductions to the operator's cost base – and materially shorter time-to-market.

With open-source code, vendors can not only pre-configure VNFs, they can also make changes to the orchestrator itself should a technical issue arise during the test phase of a given VNF. This will avoid interminable to-ing and fro-ing between vendors and operators, as well as cutting down on the cost of customization.

Another substantial benefit is that having direct access to the VNF code reduces the operators' dependence on vendors. This has obvious time and cost implications, and will also transform the operators-vendor's relationship to become much more collaborative in nature.

More fundamentally, though, I believe that having visibility and full control of the code which powers an operator network is essential if operators are to fulfil their obligations as trustees of critical infrastructure: without this high level of transparency they cannot effectively protect their infrastructure against cyber-attacks and other risks.

Furthermore, it is only within an open source environment that you get a healthy and vibrant community of 'white hats.' White hats are ethical hackers who constantly review and test the code of open source infrastructure to fix vulnerabilities and improve the resiliency of the code. This is essential for protecting an attack-prone code base effectively.

how ONAP will transform the dynamics of the telecom marketplace

By Alla Goldner
Director of Industrial Affairs & Standardization
Amdocs

Today, the Linux Foundation announced that it would merge two concurrent projects, Open Source ECOMP and OPEN-O. Both aim to create a standardized management and automation platform for NFV/SDN networks. The new project will be called Open Network Automation Platform (ONAP).

Creating common ground for innovation

Combining two open-source initiatives targeting the same outcome seems like a no-brainer. But what concrete benefits will this bring to the telecoms sector? And how else might a standardised, open-source NFV/SDN automation platform affect our industry?

The fact that there are numerous open source projects trying to solve the issue of orchestration and automation in virtualized networks underlines the fact that operators urgently need a streamlined way to manage their networks and launch new VNFs and services at the click of a button.

In practical terms, you could say that the aim of standardizing on an automation and orchestration platform is to create a 'Windows' for telecoms: a common, widely accepted technology platform for service and app innovation.

Achieving critical mass

Getting a large share of the industry to buy into one single standard has obvious advantages. The bigger the open source community working on this, the faster ONAP can reach the level of maturity, scale and performance needed for it to run live networks. That AT&T's ECOMP is already in production within the AT&T network and is also being tested by Orange and Bell Canada will be an advantage for ONAP's evolution.

ECOMP was originally designed by AT&T and co-created with Amdocs. Over the last year, it has won the support of Orange and Bell Canada, and become an open-source project. Open-O has backing from operators like China Mobile, China Telecom and Hong Kong Telecom, along with vendors such as Ericsson and Intel. These are all large industry players with significant contingents of software developers, and as more operator and vendor partners come on board, this will boost ONAP's momentum.

Not only will joining forces up the numbers of those helping to take ONAP to maturity more quickly. The scale of the project should also give ONAP a large share in the automation and orchestration market.

This may create the critical mass needed to achieve two important goals. Firstly, it will provide a strong argument for more industry players to join ONAP. Secondly, wide industry support will convince more operators to opt for ONAP as an orchestration and automation platform. This will, in turn, contribute to it becoming the de-facto industry standard for automation and orchestration.

Giving service providers greater independence

It's also clear that a harmonized standard will make life easier, cheaper and faster for operators and vendors alike.

For example, rather than spending months tweaking the interactions between a new VNF and the service provider network, these can be pre-configured automatically.

The open source approach gives complete transparency of the platform's code, which means that operators can make adjustments at any time.

Longer-term, the standard will also affect the cost and ease of switching VNF supplier, reducing the vendor dependence and 'lock-in' typical with proprietary solutions.

A change of business model

This has significant implications for the established operator-vendor relationship. Rather than being somewhat opposing forces, ONAP will usher in a new collaborative relationship between the two.

Vendors will benefit from becoming ONAP 'insiders' ensuring that they remain attractive as integrators and co-developers for ONAP rollouts. For operators, it will mean clawing back accountability for their network, and taking on more of the responsibilities typically borne by vendors.

In conclusion, if the Linux Foundation can build on the momentum behind ECOMP and OPEN-O to push ONAP to maturity, this may drive the current business models in telecoms into a brand-new age.

code never lies

By Dr. Eyal Felstaine
CTO & Head of Technology Office
Amdocs

With telecom networks becoming increasingly virtualized, we deal less and less with 'boxes' and spend more of our time looking at code. In theory, this should make introducing a new service or network function much easier. As the saying goes, code never lies. It either works or it doesn't. And when it doesn't, you fix it.

In practice, it's not quite as straightforward, and industry take-up of network virtualization has been hampered as a consequence. The answer, I believe, lies in adopting an open source approach.

Ending the pain of VNF onboarding

Even though you now don't have hordes of engineers delivering and installing new equipment, adding a new VNF to your network (VNF onboarding) is still a time-consuming and costly exercise.

The new VNF should be 'orchestrable', and the VNF vendor will typically provide the automation scripts and artifacts, such as descriptors and relevant APIs, needed to make it compatible with the operator's orchestration platform.

Once the VNF has been 'onboarded,' the operator needs to test its compatibility with other VNFs it has to talk to, and with the network as a whole. If automation artifacts are found to be incompatible, or if the vendor simply hasn't provided them, this sets off a lengthy troubleshooting process for the operator.

Troubleshooting today

In my experience, the process of fixing errors and plugging gaps is one of the costliest aspects of NFV network deployment today.

Resolving a trouble ticket – no matter how small the error – typically involves everyone from the VNF vendor's tech support to product management, network engineering and R&D to the developers who will ultimately amend the code. In addition, staff from the service provider's organization will be tied up in this process as well.

The iterations between vendor and operator can easily eat up over a third of the overall budget. What's more, they may ultimately negate some of the benefits associated with virtualization, not least cost efficiencies and reduced time-to-market for new services.

Fixing code the open-source way

This is where the open source approach has a distinct advantage over traditional telecom business models. Open source code is in the public domain, not hidden away in a 'black box' like proprietary vendor solutions. This means that VNF onboarding can be dramatically simplified compared with the troubleshooting process described above.

If we take the ONAP orchestration and automation platform as an example, as an open source project, its code will be completely transparent to both vendors and operators.

This has two immediate benefits. The first is that vendors can now pre-configure their VNFs to work with ONAP, ahead of rollout. The second is that when onboarding throws up technical issues, they are much more straightforward to resolve by amending orchestrator and VNF code directly. This eliminates the endless to-ing and fro-ing between vendors and operators, leading to significant time and cost-savings on both sides.

Taking a collaborative approach

If you consider what open source has already done to transform operating systems (Linux), virtualization infrastructure (OpenStack) and big data (Hadoop), the benefits of taking this collaborative approach – rather than relying on proprietary solutions or standardization bodies – are clear.

As I said before: code never lies: it either works or it doesn't. The beauty of open source over proprietary approaches is that, when it doesn't, you can fix it more easily and quickly – and the wider industry benefits from your contribution.

ONAP is changing the fabric of telecoms – here's how

By Dr. Eyal Felstaine
CTO & Head of Technology Office
Amdocs

To say that the telecom sector has undergone dramatic transformation in recent years would be a gross understatement.

Designed for voice services, telecom networks have had to keep pace with the capacity needs of ever more data-hungry applications. At the same time, operators have faced intense competitive pressure. This has come not only from other service providers but also from cloud players entering the fray with more agile business models and cut-rate services.

In response, networks have evolved from the monolithic, specialized structures of old to adopting low-cost, off-the-shelf cloud infrastructure solutions, while moving intelligence and functionality into software. This network virtualization enables operators to slash costs and take new services to market in a fraction of the time it used to take. It also affects the very fabric of our industry as traditional business models are replaced with new ones, not least open source collaboration.

Joining forces

ONAP, the open-source network automation platform, is a good example of this.

To start with, any operator intending to virtualize their network needs automation and orchestration technology. This will enable them to handle previously manual tasks, such as allocating bandwidth or designing and provisioning services, automatically – at the proverbial touch of a button.

Such a platform needs to have a high level of interoperability so it can interact easily with a wide range of vendor products. The fact that adoption of NFV/SDN networks has been hampered by the lack of a standardized automation platform is testament to this.

In the past, finding that technological 'common ground' would have led to a standardization committee being set up to define a framework which individual vendor solutions must interoperate with.

In contrast, ONAP is created by members of the industry, who pool their resources and work in collaboration where they may previously have competed.

Many hands make light work

While ONAP is not the first open source initiative in telecommunications, jointly creating software code that is free for anyone to use represents a fundamental shift for an industry built on proprietary solutions and vendors' intellectual property.

One key advantage is that the more developers can work on ONAP code, the quicker it will be available to operators who want to virtualize their networks. For them, ONAP will be a major shortcut, saving them the time and expense of undertaking their own development or working with vendors to achieve the same. This is expected to speed the adoption of NFV/SDN networks significantly.

Making the switch

Having a standardized platform which works with a large range of vendor solutions will also make service providers' relationship with vendors less 'sticky'.

With a range of ONAP-ready products to choose from, it will be easier for service providers to combine 'best of breed' technology from different sources in their networks.

What is more, switching vendors will become much more straightforward. Rather than a lengthy migration from one proprietary solution to another, changing suppliers will be more like moving between different Linux distributions. While there may be some proprietary quirks to each flavour of ONAP, the underlying code will fundamentally remain the same.

Adopting the cloud model

Ultimately, ONAP will help contribute to a lower cost base and increase the scope for innovating faster around NFV and SDN services. This will make operators' strategies and business models much more akin to those of cloud service providers, such as AWS and Google, boosting the agility and efficiency with which they can respond to the market.

virtualization needs open source! – here's why

By Dr. Eyal Felstaine
CTO & Head of Technology Office
Amdocs

There's little debate in our industry that network virtualization (NFV/SDN) is the way forward for telecoms' infrastructure. So why are adoption rates of NFV/SDN architectures still low?

That's because two critical elements for realizing its benefits have been missing: a standardized way of automating NFV/SDN infrastructure (as opposed to a plethora of different solutions), and a more viable way of rolling out virtualization technology. Amdocs has long recognised this challenge and has been actively contributing through organisations like the TM Forum to find solutions.

ONAP provides the answer to both

Its introduction of an open-source approach into telecommunications – an industry traditionally steeped in proprietary solutions – is critical to the success of network virtualization. I'd go as far as to say that virtualization can't really be justified without open source – in other words, the benefits of virtualization will be hard to realize without open source.

Why can't we just do what we've always done?

In theory, virtualization is a no-brainer. Like cloud, it benefits from low-cost, off-the-shelf hardware, while gaining greater agility in network management, service creation and provisioning. But because virtualization is a fundamental shift for our sector, the reality looks quite different.

It simply doesn't make sense to deploy NFV/SDN networks in the traditional way, where operators specify their requirements and vendors provide proprietary solutions. The cost of developing, maintaining and constantly updating code for proprietary NFV/SDN products – including all customer-specific adaptations – would be prohibitive for any individual vendor. (Not to mention their operator clients, who would of course have to foot the hefty bill).

Another issue with the traditional approach is that onboarding a new virtual network function (VNF) is a lengthy and costly process for the operator. It involves developing vendor guidelines, testing, and then going back and forth with the vendor to fix bugs until the VNF can finally be deployed.

As a service provider, you don't want to go through – and pay for – this protracted process more often than you need to. It means that you're now heavily tied in with your chosen vendor, can't switch easily, and can't viably build your network with solutions from multiple suppliers.

ONAP addresses all these issues, thanks to its underlying open-source philosophy, building on industry agreements already established.

Learning from the cloud

Our industry needs to adopt much more from cloud computing than just virtualization technology – we need to learn how it works and why open source has become so fundamental to its business model. Just think of the success of OpenStack, Cloud Foundry, KVM, Hadoop and Docker, and you can see that taking a collaborative approach – rather than one marked by competitive tension – has obvious benefits.

First, many hands make light work. With ONAP, industry giants like AT&T, China Mobile, Bell, Orange, Cisco and Amdocs are putting their weight – and their software engineers – behind the project. Bringing together a large community of developers means that software can mature more quickly compared to what an individual organisation could achieve.

With a large-enough share of telecom heavyweights – operators, vendors and integrators – joining the project, it will reach the critical mass needed to make ONAP the de-facto industry standard for network automation. This will put an end to the product fragmentation that has curbed operators' appetite for NFV/SDN technology, and simplify the work of standardization projects.

What's more, onboarding can happen much faster with a standardized platform: a vendor can build and test a VNF for ONAP before it is validated and deployed by the operator. Any outstanding troubleshooting, fault finding and bug fixing will also become easier because the ONAP code is accessible to all parties.

For the same reason, ONAP will finally enable service providers to build multi-vendor networks, rather than being 'locked in.' It will also make their vendor relationships less 'sticky', enabling them to switch suppliers as they see fit.

What will it take to succeed?

Let's be clear: moving our industry from its traditional vendor-centric to the open-source model won't happen overnight. The success of projects like ONAP will be critical to making this transformation happen.

The first priority will be to unite large swathes of the industry behind ONAP in order to elevate it to an industry standard.

Secondly, membership must not just be a token gesture. Contributors must pull their weight, making sufficient resources available, both human and financial. Committing to ONAP early on will have the added benefit that they can drive and influence the development of the platform from the get-go, rather than becoming an 'also ran'.

Thirdly, the project must be well-managed – a lot will depend on ONAP's Governing Board and Technical Steering Committee. But while strong leadership is required, it mustn't become too restrictive. If members think that too few of the suggestions they're putting forward are making it onto the ONAP roadmap, this may affect their motivation to contribute.

The result could be a multiplication of side projects, which would lead us back to fragmentation and proprietary approaches. This must be avoided at all cost.

the balance of power in telecoms is shifting – you just need to take a leap of faith

By Alla Goldner
Director of Industrial Affairs & Standardization
Amdocs

The telecoms industry is at the heart of the 'Fourth Industrial Revolution'. The digital transformation has led us from TDM to IP, from fixed line to mobile, and from voice to data, in less than two decades. Yet, despite all this disruption, the way our sector operates has not changed very much.

How we design networks, select, test and commission infrastructure, and roll out services is fundamentally the same as it's always been. This also applies to the relationship between service providers and their suppliers.

Now the transformation from physical to NFV/SDN infrastructure is throwing the industry a curveball: virtualization is not only disrupting network technology, it is shaking up the operator-vendor dynamic.

Shifting the balance of power

In the past, service providers were dependent not only on vendors' proprietary network equipment, but also on their customization and integration services. Beyond some standardized APIs, equipment was essentially a 'black box' which only the vendors themselves could make changes to.

Deploying a new network element involved a virtually endless 'dance' between the vendor and the service provider to integrate and troubleshoot before the function could be commissioned.

This translated into high costs, a great level of vendor dependence, and high barriers to switching. It also discouraged service providers from selecting 'best of breed' products from a number of suppliers.

With the advent of NFV/SDN, it became clear that these dynamics could jeopardize some of the key benefits NFV promised to operators, such as cutting costs and gaining greater agility in creating and delivering services.

Do operators hold the reins?

Innovation is accelerated once a technology has been standardized and commoditized – you just have to look at the electricity grid, television and the 'cloud' for proof. Rather than building networks from a pool of proprietary solutions – and continuing the 'dance' – operators realized that it would be critical to achieve a high level of standardization.

Taking a page out of the cloud textbook, they started looking at the open source community and its track record for standardization in the IT world.

Unlike the established telecoms industry bodies, open source offers a faster, more collaborative and transparent route to developing industry standards. Not only does the transparency of open source code put an end to the operator-vendor 'dance', participating in open source projects also gives service providers greater scope to shape technologies that will eventually come onto their networks, rather than being tied to vendor roadmaps.

Are vendors getting left behind?

Clearly, this represents a big shift for technology vendors.

The need for integration will reduce dramatically as a result of standardization and transparency of code. Ongoing maintenance – another important source of vendor income – will largely be provided by the open source community. In addition, suppliers will have to wave good-bye to long tie-ins with operators as standardization will bring down the barriers to switching.

Add declining hardware sales due to virtualization, and these developments make for an explosive mix that could have a devastating effect on vendors' revenue base.

Opening the door to creativity

However, when one door closes, another opens.

Integration and maintenance have never been a source of innovation. Vendors need to embrace open source as a way of freeing themselves up from the mundane so they can put more resources behind service creation and tap new revenue streams.

What's more, creating standardized platforms does not eliminate the need for customized solutions. Open source software development is managed by a technology committee, and not all functional requests to the committee will be successful. Consequently, there will still be a sizeable market for solutions which meet those operator needs that the open source process cannot cater to.

Why should vendors get involved?

Some vendors will spot the value in these opportunities and throw themselves into open source projects like ONAP. Others will be dragged along kicking and screaming.

If you are in the latter camp, consider the following.

Service providers will want to partner with companies that drive open-source development rather than with bystanders. It's another way for them to influence the direction that a particular technology is taking.

Also, to secure a share of the NFV/SDN services pie and create differentiated services, you need to know the underlying platforms from the inside.

Finally, don't forget that NFV/SDN is still an emerging technology: industry adoption has been held back by a lack of standardization and a fragmented product landscape. If this stumbling block cannot be removed, virtualization in telecoms will remain a pipe dream and a market predicted to reach nearly $12 billion by 2019 will crumble.

So, it's a leap of faith worth taking.

network virtualization is a culture shock – we need to get over it

By Oren Marmur
Vice President, NFV
Amdocs

Much has been written about the technological change, financial benefits and increased agility that NFV/SDN technology will bring to telecoms networks. But behind the glossy shopfront of virtualization lurks a subject few commentators have dared to broach.

For a very monolithic sector like telecoms, virtualization is a huge culture shock – one so major that it could become a serious roadblock to the technology's success.

We need to get over it – and quickly.

The only constant is change

When Cloud computing and data centre companies started to adopt virtualization, theirs was a young sector with little technological baggage. With more than a hundred years of history and decades' worth of legacy infrastructure to consider, the telecoms sector faces a much bigger challenge.

Casting aside the technological implications of moving from hardware to software, there is a significant cultural component to consider.

Looking at it from the point of view of service providers, telecoms has a history of operating in silos: network operations, IT, and service creation have all been distinct functions with limited crossover. With the advent of NFV/SDN, the once solid boundaries between these functions are starting to crumble. The resulting changes and overlapping of roles and responsibilities have created uneasiness among staff which is not helped by the lack of a firm vision of what the future telecoms landscape will look like.

The cultural impact of NFV/SDN only adds to the substantial practical challenges that come with operating a 'cloud' rather than a physical network, including aligning and retraining large swathes of the workforce. Taken together, these concerns have led to delays in adopting NFV/SDN technology and may explain why many operators have settled for partial deployments rather than committing fully.

Such a halfway house may feel more comfortable culturally, but it will not enable service providers to reap the full benefits of virtualization.

Embracing the sharing culture

For vendors, the move towards open source standardization – again pioneered by the Cloud community – adds another level of complexity and unease.

Where ringfenced Intellectual Property used to be their main source of differentiation – and income – vendors are now being asked to share code with customers and competitors alike.

What's more, the way vendors develop, package and sell products will have to change substantially as a result of working in an open source setting. Instead of focusing on proprietary products, there needs to be a stronger emphasis on creating new services but also on integrating and customizing third-party applications, for example. Similarly, vendor 'lock-in' will become a thing of the past. Operators will no longer be tied to vendors eternally and will be able to swap between different vendors' solutions in their network, further affecting individual suppliers' revenues.

For network equipment manufacturers, this will be a particularly bitter pill to swallow as it will only aggravate the impact of virtualization on their hardware sales.

The fact that open source is so new to telecoms – it is still looking for direction rather than presenting a solid roadmap – further adds to the feeling of being in limbo among the vendor community.

Don't cut off the branch you're sitting on

It is easy to understand why both service providers and their suppliers struggle with these fundamental changes to the inner workings of the telecoms sector.

But burying our heads in the sand and hoping it will go away won't get us anywhere. Legacy infrastructure, processes and strategies won't keep up with the demands of an increasingly digitalized world. NFV/SDN and open source are the best approaches to meet these demands, and we need to get over our misgivings and embrace them.

As an industry, we must not cut off the branch we are sitting on but collaborate to develop this new market. Only then can we ensure that it becomes big enough for us all to get a viable slice of the pie.

We should view open source as a way of offloading some of the mundane aspects of our work – standardization for one – to free up time for more productive activities, not least of which is service creation. We also need to realise that open source means 'collaboration' but it does not mean 'free.' There will still be plenty of opportunities to develop differentiated products and carve out competitive advantage.

Democratising infrastructure

In particular, there is a major opening for smaller companies to enter the fray – companies that operators would have ruled out previously simply due to their size and maturity.

In the past, selecting a supplier for a critical piece of hardware was a risky business. Operators needed to play it safe and minimize risks by working with large, proven players. With NFV/SDN, this risk is much reduced because each system is just one of many pieces of software.

Virtualization has the potential to open many new doors for our sector, speed up innovation and make it thrive again. We should not let fear of change hold us back.

open source can protect your virtualized network – here's how

By Liron Shtraichman
NFV R&D Director
Amdocs

Virtualization has been a hot topic in telecommunications for nearly half a decade, and security concerns have remained an ever-present feature. This is not surprising given the extent to which NFV/SDN is transforming the industry and the many 'known unknowns' this entails.

As networks migrate from hardware to software, and 'walled gardens' turn into much more open cloud-like architectures, so security risks increase.

Throwing open source software development into the mix adds a further layer of complexity.

If large numbers of developers across the world can manipulate the code of a piece of software, doesn't this increase the risk of malicious code being introduced? And if code is visible to anyone, isn't it going to be much easier to find, and capitalise on, vulnerabilities?

The answer is no. Just because a software is open source it doesn't mean that it is more vulnerable. Quite the opposite, in fact.

Balancing the risks

While the risk of someone implanting a malicious piece of code is conceivable, the mechanisms of the open source community would ensure that it's not there for very long. Open source code is inspected by a lot of people. I would go as far as to say that it is reviewed and audited much more than closed source code. So, while the risk is there in principle, any rogue code would get flushed out pretty rapidly.

When it comes to attacks from the outside, there is little difference between hacking an open source or a closed source application.

In the case of a probing attack – where hackers identity software weaknesses from the way the application responds to a range of prompts – the tools and processes used are the same for both closed and open source.

Another approach, static code analysis, is ostensibly easier in open source because the code is fully visible. However, the fact that the code is closed doesn't mean that you cannot read it. There are enough tools in the market that allow you to decompile the code, so the hacker can find those soft spots without having the code itself. Hence the risk levels are no different between the two domains.

A global community to fend off threats

While this may sound counterintuitive, open source even has the potential to be more secure than a closed source application.

Why? Because in closed source settings, it is not generally in the vendor's interest to disclose vulnerabilities. Fixing them can therefore take a long time – leaving users exposed over a prolonged period of time.

The transparency which characterizes the open source environment translates into a much greater incentive to identify threats and root them out quickly.

It's also less likely for vulnerabilities to creep in inadvertently. Compared to closed source developers, the open source community tends to invest much more time in polishing code before submitting it for inspection. After all, developers are putting their professional reputation on the line with a large, global audience.

Reaching critical mass

How effectively an open source project can stay on top of security risks depends entirely on the size of its support base. Ultimately, this could create more stumbling blocks for the adoption of NFV/SDN networks.

the missing piece of the puzzle?

By Angela Logothetis
Vice President, Open Network CTO
Amdocs

Artificial Intelligence (AI) is the latest piece of the jigsaw telecom operators must put together as they evolve their networks from physical to cloud-based, virtualized infrastructures (NFV/SDN).

It's easy to get carried away by the possibilities AI and technologies such as Machine Learning offer. Customer analytics, revenue assurance and network optimization are all ripe for this new technology.

But the area where AI can make the biggest impact is operational automation: letting networks run themselves. Instead of spending substantial amounts on managing, maintaining and fixing them, networks could become "self-healing."

But carriers have been slow to commit to automating their networks.

Letting the network run itself

To date, network operations have been semi-automated at best. Though more and more functions have moved onto software platforms, it has made little sense for many operators to automate these functions, when there was still a large physical network that required manual configuration and servicing.

However, NFV/SDN virtualization converts much of the physical infrastructure into software. And within a virtualized network, there is little need for so-called truck rolls – sending out engineers to configure, repair or service equipment. This opens an unprecedented opportunity to automate networks 'end-to-end', enabling them to take care of themselves.

The costs savings and the flexibility NFV/SDN brings to creating and provisioning services ('service agility') are well documented. But the technology can only come truly into its own once network and service operations are automated. Not only that, but operational automation is so vital that the business case for NFV/SDN will crumble without it.

And yet, neither vendors, nor service providers or the standards community have paid much attention to operational automation so far, preferring to focus on service creation instead.

Artificial Intelligence could play an important part in changing this.

How AI fits into the picture

A telecoms network generates billions of data points daily. Level 3, the global carrier, registers more than 50 billion network events every day, including faults, security threats and performance alerts on issues such as latency, loss and jitter. Some events require action but much of the data is noise.

So far, it has fallen to rules engines within network assurance systems to sift through all this data before it is reviewed by network operations staff to figure out what to do. With the bulk of analysis being done by a person, these systems did not have to be very accurate; they just had to provide a first layer of analytics.

This is different in an automated NFV/SDN network, where the network orchestration platform – for example ONAP – needs a highly accurate feed of data and instructions to execute.

This is where Artificial Intelligence and Machine Learning come in. AI algorithms monitor the behaviour of the network and detect events that require action. Machine Learning then steps in to analyse the events and come up with solutions, using a database of past events. Those decisions are then implemented automatically by the orchestration platform. For example, when the AI engine detects latency or a security threat on the network, ONAP can trigger an automated 'fix' to the problem.

A process which typically takes hours – for instance allocating extra bandwidth to reduce latency – can instead be completed in a matter of minutes. And because AI also picks up issues which a human analyst might have missed, it enables carriers to provide more consistent customer service levels.

While the benefits of AI-driven automation are evident, the question is how service providers can evolve from manual to automated operations?

The route ahead

The use of AI in NFV/SDN networks is in its infancy – as is virtualization itself. How AI engines will interact with automation platforms such as ONAP is still a work in progress.

What is clear is that the industry is looking to machine learning and AI to define automation 'on the fly'. The goal is for the automation platform to learn from past events, improve continuously and respond to triggers ever more independently.

Right now, this is easier said than done. Existing machine learning systems do not meet carriers' requirements in areas such as reliability ('six nines', 99.9999%), real-time processing and scalability.

That said, no matter how much machines can learn and how quickly they can do so, there will always be situations where even the best AI engine cannot replace a 'war room' of human expertise. This is especially true for rare or first time scenarios. So, while we can automate network operations to a considerable extent, they will never run entirely without human intervention.

However, even when the last resort is a person, AI and Machine Learning can assist with troubleshooting, for example by and picking out what 'war roomers' should investigate first.

Automation, automation, automation

The biggest threat to realizing the potential of virtualization and automation is inertia.

Modern telecoms has a history of jumping on the bandwagon of new technologies and then only committing to them half-heartedly. Take the move to all-IP networks, which dominated the headlines in the early 2000s: it was never fully realised because service providers did not want to lose control of network operations, especially routing and prioritizing traffic.

Unless carriers are willing to 'let go' and commit to automation, the same could happen with NFV/SDN. Because without operational automation, virtualization is simply a sideways step. Instead of hardware the network is software – but not much else changes.

AI and machine learning can play a major part in the transition towards operational automation and help ensure that operators reap the rewards of their investment in NFV/SDN.

lessons from the cloud will help telcos get better at services – here's why

By Tzvika Naveh
NFV Solution Marketing Manager
Amdocs

Telecom network operators were nothing if not rattled when cloud computing arrived on their doorstep. In an industry where competition was already ripe and growing consolidation a certainty, the thought of more players entering the fray set alarm bells ringing. But they had little to counter cloud providers' low-cost services that could be switched on quickly and scaled flexibly.

The cloud business model appealed not only to end users but also to the telcos themselves. 'Cloudification' and virtualization technologies such as NFV (Network Function Virtualization) and SDN (Software-Defined Networking) were ushered in with much fanfare. They promised to transform the economics of telecoms and make operators more agile in creating new services.

But nearly half a decade later, few operators have virtualized their networks to any great extent. There is one area operators critically need to get to grips with for this transition to happen, and that's onboarding – the process of setting up virtual network functions (VNFs) and new services on the network.

I wouldn't start from here

In the past, telecoms networks were relatively static and there was little of what we now call service innovation. For the better part of the last century, telecom networks mainly provided fixed-line voice communications, quite often in monopoly settings.

As these started to break down in the 1990s, competitive pressures mounted, and creating new services became fundamental to winning, retaining and growing customer revenues. At this point, there was little automation. New services were created from scratch and onboarded manually – a costly, slow and cumbersome process in what was a fast-paced marketplace.

While telcos have caught up to some extent and automated some aspect of this, NFV/SDN will mean going the whole hog and automating the entire onboarding process. This will give us not only cost advantages but also a much greater agility to develop and launch new services at an unprecedented pace.

Taking the Lego approach

In moving towards cloud-based networks and automated onboarding, we can learn from the best practices established in cloud computing. DevOps (Development and Operations) is one of these.

DevOps is an approach that brings together developers who create software with operational staff who manage networks, two functions which typically have little crossover. Both take part in creating a new piece of software, a network function or service, and jointly accompany it through its lifecycle.

This means that how the service works and interacts with other parts of the network is built into the service from the start. It's not left until the service is ready to be deployed and tested. The main advantage of this is that less integration will be needed during onboarding, with obvious time and cost savings. But as an additional benefit, taking the DevOps approach also creates pre-packaged service components, which can be reused.

So, instead of building services from scratch as we used to, we can simply re-use components and put them together differently to create new services. This Lego block approach has obvious cost and time advantages and will speed up service creation markedly.

Gazing into the crystal ball

With an automated onboarding process and ready-made building blocks for services, all the time-consuming, labour-intensive tasks around service creation can be reduced to a minimum.

But for the network to manage itself in this way, functions and services need to anticipate future requirements. Many of these will be unpredictable, especially considering that one service might become the building block of another service in the future.

One consequence of this is that we need to give VNFs and services more functionality than they may strictly need at the time of their creation. But that's a small price to pay for an infrastructure that can create, scale and repair itself, with minimum human intervention.

three reasons why network virtualization won't fly – and what we can do about it

By Dr. Eyal Felstaine
CTO & Head of Technology Office
Amdocs

The honeymoon is over.

After nearly half a decade of dabbling in network virtualization, the telecoms industry is waking up to a harsh reality: it may have hitched itself to NFV/SDN, but married life is far from a bed of roses. Instead, "we find ourselves mired in an unprecedented mess," according to Steve Saunders, founder of industry portal Light Reading. His statement strikes a strong chord with me.

So far, few – if any – operators have been able to reap the much-vaunted benefits of NFV/SDN virtualization. Instead of cost-savings, they have seen mounting integration costs. Instead of building open, multi-vendor networks, they still find themselves tied to individual suppliers. And because networks aren't all that open, creating an ongoing string of innovative services has remained nothing more than a pipedream.

There's a serious risk that NFV/SDN will go the way of so many ground-breaking technologies in our industry: snuffed out by a fear of cutting off the branch we're sitting on.

There are three reasons why virtualization won't 'fly', and we've got to tackle them urgently to give our sector a new lease on life.

No commitment to open source

Some lay the blame for the 'mess' we're in at the feet of standards bodies. In over four years, they have failed to create a broad basis for interoperability, hampering the take-up of virtualization technology. To me, this suggests that you can't teach an old dog new tricks. NFV/SDN is so fundamentally different from anything we've done before in telecoms that our institutions are ill-equipped to handle it.

Cloud computing has shown us that open source development is a much more efficient route to standardization. By collaborating and pooling resources, code can be created and validated faster, and security issues and bugs resolved more quickly. There is little need for integration, either. Software can be configured to a transparent code base rather than a 'black box' with a few standardised APIs. This transparency also means that operators can 'mix' products from different vendors more easily, ending the scourge of vendor lock-in.

For these dynamics to work, you need a critical mass of industry players to throw their weight behind an open source initiative. It does not help when separate projects are set up to achieve one and the same thing. The Linux Foundation wisely brought together the Open-O and Open ECOMP initiatives under the ONAP banner. However, the Open MANO group continues alongside, not to mention proprietary initiatives.

For NFV to succeed, two things need to happen: first, the industry must commit to open source, full stop. Second, to develop a function, we need to unite behind a single open source project rather than fragmenting the support base.

Automation or bust

The importance of automation for NFV/SDN has been all but ignored to date. Everyone has been talking up cost savings and 'service agility' but forgetting to mention that these can only be realized once network and service operations are automated.

The ideal is for networks to virtually run themselves, using AI and machine learning to make decisions more and more independently, without human intervention. The potential in terms of costs, time and ease of provisioning are self-evident.

Admittedly, machine learning has a long way to go before it will give us this level of automation. But the bigger issue is that carriers have been slow to commit resources to automation. There are two reasons for this. Firstly, automation means giving up a high degree of control over the network. Secondly, it often falls into the 'too hard' basket.

If we want to make NFV/SDN investments pay off, operators will have to get over their misgivings and sign up to operational automation. We can turn all the switches and routers in the world into software, but without automation, we'll never see any real-world benefits.

Changing a culture steeped in tradition

This leads me to the third reason virtualization may never achieve its full potential: culture.

Arguably, culture is the single biggest factor holding back NFV/SDN. Our industry may be seeking a place at the heart of the Fourth Industrial Revolution, but it is steeped in tradition and set in its ways.

Virtualization is shaking things up and creating uncertainty. Traditional operator 'silos' are merging and job functions are blurring. As new roles emerge, fundamental re-training and new recruitment will be needed. As proprietary approaches give way to collaborative efforts and operators gain more freedom of choice, vendors see their established sales models crumble. All this sits rather uncomfortably with the telecoms community, and explains – at least in part – its half-hearted commitment to virtualization.

But the fact is, there is no plan B. NFV/SDN is our best bet right here, right now.

So while the cultural transformation will be the hardest and won't happen overnight, we need to get over ourselves and adapt to the changes that an increasingly digitalized world is throwing at us.

Back to Plan A

Telecoms is one of the most competitive markets in the world: carriers are not just fighting off other carriers. They also face stiff competition from OTT content providers, virtual network operators and cloud service providers, to name but a few. If we want our industry to stay competitive, we must ensure that it stays relevant and bring its technology, processes and culture 'up to scratch.'

about amdocs

Amdocs is a leading software & services provider to the world's most successful communications and media companies. As our customers reinvent themselves, we enable their digital and network transformation through innovative solutions, delivery expertise and intelligent operations.

Amdocs and its 25,000 employees serve customers in over 85 countries. Listed on the NASDAQ Global Select Market, Amdocs had revenue of $3.7 billion in fiscal 2016.

amdocs