funkschau Kommunikationstechnik für Profis

datacenter

Tests, Trends und Technik für CIOs, CTOs und CSOs

funkschau.de

CeBIT 2015 • Redfish • Storage • WAN-Performance
Software-Defined-Datacenter • Network-Functions-Virtualization
Carrier-Ethernet/Third-Network • Cloud-Architekturen • Klimatisierung

NFV und SDN machen Produktionsnetze fit für Industrie 4.0

Industrie 4.0 ist laut dem Digitalverband Bitkom das Trendthema des Jahres für die Branche. Erstmals landete die intelligente, umfassend vernetzte Industrieproduktion unter den fünf meistgenannten Hightech-Stichwörtern der jährlichen Bitkom-Trendumfrage. Die Digitalisierung des produzierenden Gewerbes, so der Verband, sei für die Wettbewerbsfähigkeit der deutschen Wirtschaft von existenzieller Bedeutung.

Allerdings ist Industrie 4.0 noch lange kein Selbstläufer, im Gegenteil: Eine Reihe wirtschaftlicher, politischer und nicht zuletzt technologischer Voraussetzungen muss erfüllt sein, damit Industrie 4.0 auch für deutsche Unternehmen ein Erfolg wird. Von zentraler Bedeutung ist dabei die Entwicklung der industriellen Produktionsnetze. Bislang bilden diese „Industrial Automation and Control Systems" (IACS) meist innerhalb eines Unternehmens und eines Standorts abgeschottete Inseln – insbesondere bei kleinen und mittleren Unternehmen.

Eine Flut von Protokollen und Systemen beherrschen

Im Zuge der Verwirklichung von Industrie 4.0 werden sich diese Produktionsstrukturen in Zukunft zu umfassend standort-, firmen- und länderübergreifend vernetzten Systemen entwickeln. Damit müssen sowohl Vielzahl als auch Verschiedenartigkeit von Protokollen und Systemen in der Welt industrieller Produktionsanlagen bewältigt werden. Das wiederum hat Auswirkungen auf das Netzwerkmanagement, das dafür optimiert werden muss. Das gilt vor allem im Hinblick auf die sicherheitsspezifischen Anforderungen an industrielle Produktionsnetze: Da ist einmal die IT-Sicherheit (Security), an die in der Produktion eine ganze Reihe von Zielsetzungen geknüpft ist – vom Geschäftsprozessmanagement über die Qualitätssicherung bis zum Know-how-Schutz. Gerade in der industriellen Produktion müssen natürlich zum zweiten auch Aspekte der funktionalen Sicherheit, vor allem die Arbeitssicherheit (Safety), berücksichtigt werden.

Dass die Netzwerke als Reaktion auf die neuen Sicherheitsanforderungen zügig durch entsprechende Hardware-Komponenten vollständig neu gestaltet werden, ist aufgrund langer Investitionszyklen nicht zu erwarten. Deshalb werden Maßnahmen diskutiert, die sich auf technischer Ebene auf die Struktur der Produktionsnetze konzentrieren. Hierzu schlägt die Normenreihe IEC 62443 der International Electrotechnical Commission (IEC) vor, die Produktionsnetze in einzelne Zonen und Zellen zu segmentieren. Diese werden an den Übergängen, den so genannten Conduits, durch Security-Appliances wie Firewall und Daten-Dioden geschützt.

Virtualisierung und optimiertes Netzwerkmanagement

Vielversprechende Lösungsansätze stellen in diesem Zusammenhang Virtualisierung und optimiertes Netzwerkmanagement dar. Technologisch finden diese Konzepte ihren Niederschlag in Network-Function-Virtualization (NFV) und Software-Defined-Networks (SDN). NFV und SDN sind also Technologien, die den gestiegenen Anforderungen an die variable Bereitstellung von Netzwerkfunktionen und -ressourcen sowie an das Netzmanagement in Zeiten von Industrie 4.0 entgegenkommen.

NFV stellt die wichtigste technologische Neuerung in Kommunikationsinfrastrukturen dar. Sie ermöglicht es, unterschiedliche Netzelementefunktionen als universell verwendbare Programme (Virtual-Network-Functions, VNF) darzustellen und dadurch einheitliche Standards anzustreben. Die Technik der funktionalen Abstrahierung mittels Virtueller-Maschinen (VM) ist ein bereits seit längerem genutztes Prinzip, mit dessen konsequenter Anwendung auf IT-gestützte Produktions- und Logistikprozesse der nächste große Evolutions-Schritt unmittelbar bevorsteht. Die dynamische Bereitstellung von Netzwerkfunktionen durch VNF bei gleichbleibender Hardware bietet einerseits einen wesentlichen Vorteil, führt andererseits jedoch zu neuen Herausforderungen für das derzeit bestehende Netzwerkmanagement. Zu nennen sind hier vor allem erhöhte Ansprüche an die Kontrolle und Verteilung der virtualisierten Elemente, die zügig und zuverlässig in die Netzwerkinfrastruktur eingebunden werden müssen.

Diese VNF können schnell mit SDN verfügbar gemacht werden. Dazu werden physikalische Netzelemente abstrahiert und in eine Steuerungsebene (Control-Plane) und eine Datenebene (Data-Plane) transformiert. Die dynamische Kontrolle der Verkehrsflüsse, für die Einbindung der VNF, übernimmt der SDN-Controller. Entkoppelt von der Datenebene ist dieser als Server in einem Rechenzentrum positioniert.

SDN und NFV verfolgen dabei die gleichen gemeinsamen Ziele, nämlich eine höhere Kosten- und Betriebseffizienz zu erreichen.

Forschung prüft SDN und NFV auf funktionale Abhängigkeiten

Eine erfolgreiche Umsetzung in der Praxis setzt jedoch detaillierte wissenschaftliche Untersuchungen voraus. So beschäftigen sich die Forscher des Fraunhofer ESK etwa mit möglichen funktionalen Abhängigkeiten bei simultaner Anwendung beider Technologien, SDN und NFV, im Netz. Ansatzpunkt dafür sind die bestehenden Netzübergänge für die Übertragungs- und Sicherheitssysteme, zum Einsatz kommt die Methode der funktionalen Dekomposition: Dabei werden Systeme in ihrer Gesamtheit betrachtet und die abgrenzbaren Grundfunktionalitäten identifiziert. Die Dekomposition dieses Endsystems erlaubt die Detailanalysen der

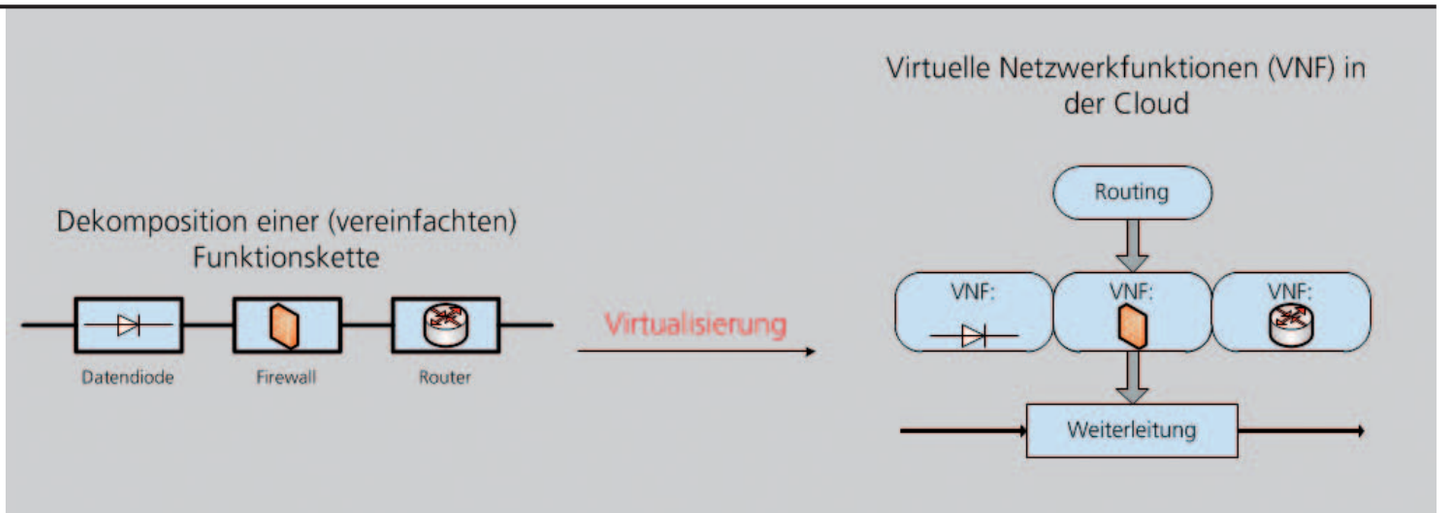

Bild: Fraunhofer ESK

Beispiel eines Virtualisierungsprozesses anhand von „Network Service Chaining", das heißt Verkettung unterschiedlicher IP-Netz-Funktionen.

SDN/NFV-Einflüsse und die Erstellung daraus resultierender Geräte- und Betriebskonzepte. Zum Beispiel kann die empfohlene Segmentierung der Netzwerke laut IEC 62443, samt festgelegten Kommunikationspfaden und -übergängen, mit dieser Analyse durch die Kombination der beiden Technologien sichergestellt werden. Die bei Industrie 4.0 erforderliche Flexibilität und Skalierbarkeit der Netzwerkarchitekturen wird durch VNF zur Verfügung gestellt. Mit SDN können die komplexen Netzwerkstrukturen administriert und im laufenden Betrieb den sich ändernden Rahmenbedingungen angepasst werden.

Anwendungsszenario: Flexible Anpassungen im Netz

Die Open Networking Foundation (ONF) und das European Telecommunications Standards Institute (ETSI) haben innovative Anwendungsfälle für die Kombination von SDN und NFV erarbeitet, die sich auf das Industrie-4.0-Umfeld erweitern lassen. Als Beispiele dienen Fertigungsumstellungen bei großen Herstellern samt deren Auswirkungen auf externe Prozesse. Bezogen auf logistische Abläufe und Bevorratung könnten in Zukunft verzugslos Informationen aus der Produktion, wie geänderter Materialbedarf und Auslieferungszustände, mit Lieferanten und Abnehmern ausgetauscht und die jeweiligen Kommunikationsbeziehungen durch die neuen Technologien angepasst werden.

Die NFV-basierte so genannte. „Infrastructure as a Service" als konsequente Weiterentwicklung von Netzwerkdiensten bietet für solche verteilten und hochflexiblen Produktionsprozesse mit komplexen Abhängigkeitsbeziehungen innerhalb der gesamten Wertschöpfungskette neue Möglichkeiten. Auf aktuelle Anforderungen an die Vernetzung kann kurzfristig reagiert und die notwendigen Ressourcen zur Verfügung gestellt werden. Die Infrastruktur dafür lässt sich auch von unabhängigen Dienst- und Netzwerkanbietern bereitstellen, die spezielle Anforderungen von Industriebetrieben erfüllen. Die beteiligten Unternehmen müssen die darunterliegende kostenintensive Infrastruktur nicht mehr selbst verwalten; dem Service-Gedanken für Datacenter entsprechend ist es möglich, benötigte Netzwerkressourcen hochverfügbar in zentrale Rechen- und Betriebszentren, also in die Cloud, auszulagern. Die Netzwerkfunktionen und Kommunikationsinfrastrukturen für Industrie 4.0 könnten also zukünftig bedarfsgerecht zentral und virtualisiert vorhanden sein.

Virtualisierte Sicherheitsfunktionen schützen Netze

In Produktionsnetzen bestehen höchste Anforderungen an die IT-Sicherheit mit unterschiedlichsten Ausprägungen wie Verfügbarkeit, Vertraulichkeit und Know-how-Schutz. Allerdings muss dabei zielgerichteter Informationsaustausch immer gewährleistet sein. Besonders im Industrie-Umfeld werden derzeitige Sicherheitsanforderungen oft mit teuren Hardwarelösungen umgesetzt oder durch abgeschottete Inselanwendungen erreicht. Deren Einsatzgebiet ist nicht nur örtlich beschränkt, sie sind zusätzlich unflexibel in der Aufnahme externer Ressourcen und Informationsschnittstellen. Ein erfolgsversprechender Ansatz basiert auf der Virtualisierung verketteter unabhängiger Hardware-Ressourcen. In einem ersten Schritt können logisch zusammengehörende Netz-Elemente, die Sicherheitsmaßnahmen umsetzen, mittels funktionaler Dekomposition in ihre virtualisierbaren Grundfunktionen zerlegt werden. Anschließend lassen sich diese per Service-Chaining im Netzwerk logisch gruppieren und stehen als virtualisierte Sicherheitsapplikationen bereit. Darüber hinaus ist es möglich, weitere Betrachtungen zu wichtigen Verfahren wie etwa Lastverteilung, Netzwerküberwachung oder Sicherheitsgateways anzustellen.

In zukünftigen Szenarien der angewandten Forschung sind sowohl einzelne Objekte im Sinne von adressierbaren Sensoren und Aktoren – Stichwort Internet of Things – betroffen, als auch deren Zusammenfassung zu komplexen und in Produktionsflüsse eingebetteten Systeme. Damit kann durch die konsequente Anwendung der Virtualisierung in den Industrienetzen die weiterführende integrale Einführung der SDN/NFV-Prinzipien auf die Produktions- und Logistikprozesse als der nächste große Evolutionsschritt angegangen werden. Um das zu ermöglichen, müssen im Rahmen von Industrie 4.0 neue Steuerungsarchitekturen für Produktionssysteme noch entwickelt werden – als Voraussetzung eines ganzheitlichen Ansatzes für die Automatisierungstechnik auf der Prozesssteuerungsebene. *(AP)*

Florian Krojer, M. Sc.,
Dipl. Ing. (FH) Ivan Furjanic,

Wissenschaftler am Fraunhofer-Institut für eingebettete Systeme und Kommunikationstechnik ESK in München