

HERAUSFORDERUNGEN IM LEBENSZYKLUS EINES DIGITALEN SCHUTZGERÄTS ALS FOLGE VON DIGITALISIERUNG UND NIS

Oliver SKRBINJEK¹, Horst PAAR²

Einleitung

Die Sekundärtechnik wird bereits seit Jahrzehnten in der Schutz-, Leit- und Fernwirktechnik von zunehmender Digitalisierung getrieben und steht auch heute ständig vor neuen Anforderungen und den damit verbundenen Herausforderungen. Waren Sekundärsysteme in der Vergangenheit nur in ihrem funktionalen Prozess digital, so sind sie heute zunehmend kommunikationstechnisch vernetzt. So erfüllen sie heute neben der ursprünglichen Funktion, nämlich z.B. dem Schutz eines Transformators, viele zusätzliche Aufgaben, die durch den technologischen Fortschritt der digitalen Use-Cases und der Kommunikationstechnik erst möglich wurden.

Herausforderung

Durch den zunehmenden Bedarf von neuen Schutz-, Überwachungs-, Steuerungs- und Automatisierungsfunktionen im Betrieb elektrischer Verteilernetze, aber auch durch gesetzliche Vorgaben (z.B. NIS-G) im Bereich des Betriebs von kritischer Infrastruktur, ist der Netzbetreiber nicht nur Anwender sekundärtechnischer Komponenten während deren operativen Betrieb, sondern der Prozess des Lebenszyklus beginnt auch für ihn bereits bei der Bedarfsdefinition, gemeinsam mit Geräteherstellern, in der Entwicklungsphase. Nachdem die Anforderungen im Einsatz bei jedem Netzbetreiber, entsprechend dessen Betriebsphilosophie und dem dahinter liegenden Systemdesign, etwas anders sind muss hier von Herstellerseite ein breites Spektrum bedient werden können.

Dieses Zusammenwirken zwischen dem Systemhersteller und dem -betreiber muss sich in weiterer Folge, neben der gesamten operativen Betriebsdauer, auch in den Phasen der Pre-Qualifikation und Akzeptanz-Tests weitergeführt werden.



Abb 1: Beispiel für einen Lebenszyklus der Sekundärtechnik



Abb. 2: Mapping: IEC63060→Schutztechnik

Die Längste und auch aufwendigste Phase ist im operativen Betrieb der Systeme zu finden. In dieser Phase liegt eine wesentlich Herausforderung in der Anforderung den Betriebs der Systeme am anerkannten Stand der Technik, aus Sicht der Informationssicherheit, aufrecht zu erhalten und die dafür erforderlichen neuen Prozesse, die nicht im bisherigen Fokus liegen, zu etablierenden. Ebenso fehlen den einzelnen elektrotechnischen Fachbereichen oftmals die erforderlichen Kompetenzen der Informationssicherheit. Daher dürfen zukünftige Wartungsprozesse nicht mehr mit fachlich isolierter Kompetenz, sondern in einem Multi-Domain-Ansatz, der alle involvierten Kompetenzträger (erforderliche Disziplinen der Sekundärtechnik, Netzwerktechnik, Informationssicherheit) mit einbindet, umgesetzt werden. Diese Prozesse sind neu zu definieren und aufzubauen.

¹ Energienetze Steiermark GmbH, +43 664 6163805, oliver.skrbinjek@e-netze.at

² Energienetze Steiermark GmbH, +43 664 6167256, horst.paar@e-netze.at

Lösungsansatz

Wartungsaufgaben werden, neben weiteren Definitionen, in IEC63060:2019 (Allgemeine Aspekte zur Wartung von Anlagen und Geräten) definiert. In der Sekundärtechnik kommen, neben Herstellerempfehlungen, auch technische Hinweise und Leitfäden zur Anwendung, die von Fachexperten und Gremien von Basis Österreichs Energie, VDE/FNN und VSE erstellt wurden. Unabhängig muss jeder Anwender für sich, entsprechend der zuvor angeführten Rahmenbedingungen, festlegen, welche Art der Systemwartung zu welchem Zeitpunkt zum Einsatz kommt. Am Beispiel der Schutztechnik lauten die Fragen zum Beispiel:

- Wann ist es sinnvoll zu prüfen?
- Was (Umfang) ist sinnvoll zu prüfen?
- Wann ist eine Verbesserung (Firmware Update/Patch) auszurollen?

Oftmals können Synergien genutzt und Effizienzen geschaffen werden, wenn nicht nur eine fachliche Entkopplung, sondern auch eine zeitliche Entkopplung von Prozessschritten in einem Wartungsintervall durchgeführt werden. Ebenso verursacht oftmals nur „eine“ vollständige Standardisierung unnötige Aufwendungen, sodass eine z.B. Technologie basierte Standardisierung in einige wenige Standardprozesse eine zusätzliche Effizienzsteigerung bringt. Neben den finanziellen Aspekten muss in diesem Zusammenhang heute vermehrt auf die Ressourcen der notwendigen Fachkräfte geachtet werden.

Zusammenfassung

Im Beitrag werden, am Beispiel eines Netzschutzgeräts, die unterschiedlichen Lebensphasen und deren Herausforderungen, bis hin zur informationstechnisch konformen Entsorgung, sowie deren Wechselwirkungen zueinander, aufgezeigt. Mit Referenz zu IEC63060:2019 sowie zum Branchendokument „Leitfaden für die Inbetriebnahme und den Betrieb digitaler Netzschutzsysteme“ werden unterschiedliche Wartungsanforderungen im operativen Lebenszyklus der Netzschutzkomponente dargestellt und jeweils eine Herangehensweise für eine praktikable und bei einem Netzbetreiber umgesetzte Lösung vorgestellt. Final wird ein mehrstufiger, risikobasierter Multi-Domain-Ansatz zur Erfüllung der Anforderung, Systeme aktuell zu halten, präsentiert. Dieser kann gezielt zur Erfüllung von Patch- und Update/Upgrade-Anforderungen mit Blickrichtung Informationssicherheit (Cyber-Security) angewendet werden.

Referenzen

- [1] IEC TS 63060:2019 (VDE 0109:2020)
- [2] „Leitfaden für die Inbetriebnahme und den Betrieb von digitalen Netzschutzsystemen“, Veröffentlicht unter Österreichs Energie (OE), Verband der Elektrotechnik Elektronik Informationstechnik (VDE/FNN) und Verband Schweizerischer Elektrizitätsunternehmen (VSE) – 2022
- [3] „Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste – NIS Fact Sheet 9/2022“, Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste (nis.gv.at)